ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย

โดย

นางสาวเบญญาภา ช่างประดิษฐ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขาการค้าระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2560

ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย

โดย

นางสาวเบญญาภา ช่างประดิษฐ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขาการค้าระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2560
ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

CLOUD COMPUTING: RECOMMENDATIONS FOR THAI PERSONAL DATA PROTECTION ACT

BY

MISS BENYAPA CHANGPRADIT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF LAWS

INTERNATIONAL TRADE REGULATION

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2017

มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์

วิทยานิพนธ์

ของ

นางสาวเบญญาภา ช่างประดิษฐ์

เรื่อง

ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เมื่อ วันที่ 10 สิงหาคม พ.ศ. 2561

ประธานกรรมการสอบวิทยานิพนธ์ _____
(ศาสตราจารย์พิเศษ วิชัย อริยะนันทกะ)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(ศาสตราจารย์ ดร. กำชัย จงจักรพันธ์)

กรรมการสอบวิทยานิพนธ์ _____
(อาจารย์เสรี วัฒนวารางศิกูร)

กรรมการสอบวิทยานิพนธ์ _____
(ศาสตรจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช)

คณบดี _____
(ศาสตราจารย์ ดร. อุดม รัฐอมฤต)

หัวข้อวิทยานิพนธ์	ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย
ชื่อผู้เขียน	นางสาวเบญญาภา ช่างประดิษฐ์
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	กฎหมายการค้าระหว่างประเทศ นิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ศาสตราจารย์ ดร.กำชัย จงจักรพันธ์
ปีการศึกษา	2560

บทคัดย่อ

ระบบการประมวลผลแบบคลาวด์เป็นเทคโนโลยีที่มีความสำคัญต่อผู้ประกอบการและบุคคลทั่วไปซึ่งจะช่วยให้สามารถประกอบธุรกิจหรือดำรงชีวิตได้อย่างสะดวกสบายและประหยัดค่าใช้จ่ายมากยิ่งขึ้น และเป็นเทคโนโลยีที่เกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคล เนื่องจากมีข้อมูลส่วนบุคคลจำนวนไม่น้อยที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ กรณีจึงมีความเสี่ยงที่ข้อมูลดังกล่าวจะรั่วไหลและก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล ดังนั้น องค์กรระหว่างประเทศและนานาประเทศจึงออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์ได้มาบังคับใช้

เมื่อพิจารณาประเทศไทยจะพบว่าประเทศไทยมีกฎหมายกลางที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และมีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... หลายฉบับ แต่ร่างกฎหมายดังกล่าวก็ยังไม่มีผลใช้บังคับแม้ระยะเวลาจะผ่านล่วงเลยมากว่า 20 ปี ดังนั้น วิทยานิพนธ์ฉบับนี้จึงมุ่งศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งเป็นฉบับล่าสุด ณ ตอนนี้ ต่อการให้บริการระบบการประมวลผลแบบคลาวด์ โดยศึกษาเปรียบเทียบกับกฎเกณฑ์หรือแนวปฏิบัติระหว่างประเทศ ได้แก่ OECD Guidelines on the Protection o Privacy and Transborder Flows of Personal Data, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, Direcitve 95/46/EC และ The General Data Protection (GDPR) ตลอดจน

กฎหมายของประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์ที่มีระบบกฎหมายใกล้เคียงกับประเทศไทยและประเทศที่มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับระบบการประมวลผลแบบคลาวด์โดยเฉพาะ เพื่อพิจารณาปัญหาที่อาจเกิดขึ้นจากการใช้กฎหมายข้างต้นของไทยต่อการให้บริการระบบการประมวลผลแบบคลาวด์ และนำเสนอข้อเสนอแนะต่อการปรับปรุงแก้ไขกฎหมายหรือร่างกฎหมายดังกล่าวต่อไป

จากการศึกษาพบว่า ปัจจุบันประเทศไทยประสบปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์ใน 2 ระยะด้วยกัน คือ

ระยะที่ 1 ปัญหาการขาดแคลนกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ประการหนึ่ง และ

ระยะที่ 2 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ยังขาดหลักการสำคัญหลายประการเพื่อให้สอดรับกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับสากลและร่างพระราชบัญญัติดังกล่าวยังมีความไม่เหมาะสมหลายประการในการที่จะบังคับใช้ข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์

ซึ่งผู้ที่สนใจสามารถศึกษาสภาพปัญหาข้างต้นพร้อมทั้งข้อเสนอแนะได้ในวิทยานิพนธ์ฉบับนี้

คำสำคัญ: ข้อมูลส่วนบุคคล, ระบบการประมวลผลแบบคลาวด์, Cloud Computing, การคุ้มครองข้อมูลส่วนบุคคลในการให้บริการระบบการประมวลผลแบบคลาวด์, Directive 95/46/EC, GDPR

Thesis Title	CLOUD COMPUTING: RECOMMENDATIONS FOR THAI PERSONAL DATA PROTECTION ACT
Author	Miss Benyapa Changpradit
Degree	Master of Laws
Major Field/Faculty/University	International Trade Regulation Law Thammasat University
Thesis Advisor	Professor Kumchai Jongjakapun, Ph.D.
Academic Years	2017

ABSTRACT

Cloud computing is a valuable technology for both business operators and individuals as it assists the businesses in IT cost reduction as well as facilitates individuals to access and manage data over the Internet everywhere. Cloud computing is also relevant to personal data due to the fact that there are a great number of personal data stored in cloud computing and, as a consequence, there is possibility and risk of cloud data leaks. To deal with this issue, various international organizations and many countries have legislated personal data protection laws and enforced such laws and regulations with cloud computing services.

In Thailand, there has been only one effective data protection law so far which is “the Official Information Act 1997” applied with data in possession of the government sector. For private sector, there have been a number of drafted personal data protection laws over a long period of time. Unfortunately, such laws have never been enforced. Hence, the purpose of this thesis is to study the Official Information Act 1997 and the latest drafted personal data protection law of Thailand in respect of cloud computing comparative with the following laws:

- An international data protection guidelines including OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Asia-Pacific

Economic Cooperation (APEC) Privacy Framework, Direcitve 95/46/EC and The General Data Protection (GDPR);

- Personal data protection laws of cloud computing readiness countries with similar legal system to Thailand;

- Personal data protection laws specifically concerning cloud computing services

Apart from the study as previously mentioned, this thesis also demonstrates issues arise from enforcement of abovementioned laws regarding cloud computing in Thailand as well as presents recommendation on the revision of Thailand drafted personal data protection.

After thorough study on this matter, it has come to my attention that Thailand is now facing with problems regarding cloud computing data protection which can be separately considered as 2 phases listed below.

Phase 1: Thailand has no data protection law applying with the personal data stored in cloud computing and

Phase 2: The latest drafted personal data protection of Thailand is not consistent with international standard guideline and in appropriate to apply with the context of cloud computing.

Further information on this regard can be found throughout this thesis.

Keywords: Personal Data, Cloud Computing, Personal Data Protection and Cloud Computing, Directive 95/46/EC, GDPR

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้เนื่องด้วยความช่วยเหลือและความกรุณาอย่างยิ่งจากผู้มีอุปการคุณหลายท่าน ดังต่อต่อไปนี้

ศาสตราจารย์ ดร.กำชัย จงจักรพันธ์ ในฐานะอาจารย์ที่ปรึกษา ผู้ประสิทธิ์ประสาทความรู้ ชี้แนะแนวทางในการนำเสนอผลงานทางวิชาการที่มีคุณภาพและเป็นประโยชน์ต่อผู้อื่นและสังคมให้แก่ข้าพเจ้าจนกระทั่งผลงานทางวิชาการนี้สำเร็จลุล่วงไปด้วยดี ข้าพเจ้ากราบขอบพระคุณ

ศาสตราจารย์ วิชัย อริยะนันทกะ ซึ่งให้เกียรติในการเป็นประธานสอบวิทยานิพนธ์ของข้าพเจ้า และให้ความรู้ชี้แนะแนวทางที่เป็นประโยชน์ต่อการนำเสนอผลงานทางวิชาการ ตลอดจนถ่ายทอดประสบการณ์ที่เกี่ยวข้องกับผลงานทางวิชาการของข้าพเจ้า ข้าพเจ้ากราบขอบพระคุณ

ศาสตราจารย์ ดร.ประสิทธิ์ ปิวาวัฒนพานิช และอาจารย์เสรี วัฒนวารางศิกูร ซึ่งให้เกียรติเป็นกรรมการในการสอบวิทยานิพนธ์ของข้าพเจ้า และชี้แนะแนวทางให้ข้าพเจ้าพิจารณาข้อมูลต่างๆ อย่างรอบด้าน ตลอดจนแนะนำแนวทางแก้ไขพัฒนาผลงานทางวิชาการของข้าพเจ้าเป็นอย่างดีเสมอมา ข้าพเจ้ากราบขอบพระคุณ

นอกจากนี้ ข้าพเจ้าขอขอบพระคุณบิดา มารดา น้องชายของข้าพเจ้าที่ให้การสนับสนุนและเป็นกำลังที่ดีในระหว่างการศึกษาค้นคว้าผลงานทางวิชาการของข้าพเจ้า

ข้าพเจ้าขอขอบพระคุณ คุณพงศ์พันธุ์ เพชรยอดศรี ที่ให้ความช่วยเหลือ ให้กำลังใจและเป็นที่ปรึกษาที่ดีในการแก้ไขปัญหาฝ่าฝันอุปสรรคที่เกิดขึ้นในระหว่างการศึกษาวิทยานิพนธ์ฉบับนี้จนสำเร็จลุล่วงไปได้ด้วยดี

ข้าพเจ้าขอขอบพระคุณ คุณกิตติ ตั้งจิตรมณีศักดา คุณชัชวาล จันทร์แสงสุก คุณประสงค์และคุณมณีรัตน์ พูนสินชูสกุล ตลอดจนผู้จัดการทุกท่านในบริษัท กฎหมายเอสซีจี จำกัด ที่ให้ความช่วยเหลือ ชี้แนะแนวทางในการนำเสนอผลงานทางวิชาการแก่ข้าพเจ้า

ข้าพเจ้าขอขอบพระคุณ คุณดลหทัย จิรวิวรรธน์ คุณปิยาพร ยะโสธร คุณกมลชัย เวทีบูรณะ คุณทุติยา โล่ห์สุวรรณ คุณภัทราพรรณ วิสิทธิวงศ์ คุณรดาพร ไทยมงคล และเพื่อนร่วมงานในบริษัท กฎหมายเอสซีจี จำกัด ทุกท่านที่ให้ความช่วยเหลือ แบ่งปันความรู้ที่เกี่ยวข้องกับการศึกษาค้นคว้าวิจัยในครั้งนี้ของข้าพเจ้า จนสำเร็จลุล่วงไปด้วยดี สุดท้ายนี้ ข้าพเจ้าขอขอบพระคุณ คุณให้ความช่วยเหลือจนวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี

นางสาวเบญญาภา ช่างประดิษฐ์

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ในปัจจุบันประเทศไทยกำลังเข้าสู่รูปแบบของการพัฒนาประเทศที่เรียกว่า “ประเทศไทย 4.0” ซึ่งจะเน้นการพัฒนาเศรษฐกิจโดยอาศัยการขับเคลื่อนของนวัตกรรมเพื่อปรับเปลี่ยนโครงสร้างของเศรษฐกิจไปสู่เศรษฐกิจรูปแบบใหม่ที่มีลักษณะเป็นเศรษฐกิจรูปแบบ “Value-Based Economy” เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของโลกปัจจุบันที่กำลังเข้าสู่ยุคดิจิตอล ทั้งนี้ ธุรกิจที่จะสามารถเติบโตและพัฒนาไปพร้อมกับนโยบายพัฒนาประเทศไทย 4.0 จะต้องมีเทคโนโลยีที่เรียกว่า โมบายเทคโนโลยี (Mobile Technology) ซึ่งจัดเป็นเทคโนโลยีที่ใกล้ชิดกับผู้บริโภคมากที่สุด โดยเฉพาะอย่างยิ่งกลุ่มผู้บริโภคที่นิยมใช้สมาร์ทโฟน แท็บเล็ตและอุปกรณ์เชื่อมต่อสัญญาณอินเทอร์เน็ตอื่นๆ นอกจากมุมมองของผู้ประกอบการแล้ว ในด้านของผู้บริโภคเองก็จะต้องพัฒนาและปรับเปลี่ยนการบริโภคของตนเองให้สอดคล้องกับยุคประเทศไทย 4.0 ด้วยโดยหันมาบริโภคสินค้าโดยอาศัยช่องทางอิเล็กทรอนิกส์หรือช่องทางออนไลน์มากยิ่งขึ้น ดังจะเห็นได้ว่าธุรกิจ e-Commerce ในปัจจุบันเติบโตอย่างก้าวกระโดด ดังนั้น เพื่อรองรับการประกอบกิจการและรองรับการบริโภคของตนเอง ผู้ประกอบการและผู้บริโภคหลายรายจึงหันมาให้ความสนใจเทคโนโลยีด้านไอทีต่าง ๆ อาทิ ระบบการประมวลผลแบบคลาวด์ เพื่อตอบโจทย์ความต้องการของตน

อย่างไรก็ตาม แม้ว่าระบบการประมวลผลแบบคลาวด์จะได้รับความสนใจจากทั้งผู้ประกอบการและผู้บริโภคเป็นอย่างมาก แต่เมื่อพิจารณาถึงลักษณะของการให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทยในระหว่างปีพ.ศ. 2559 – พ.ศ.2560 ที่ผ่านมา จะพบว่าภาพรวมในด้านความพร้อมและระบบจัดการของการให้บริการระบบการประมวลผลแบบคลาวด์ของประเทศไทยยังคงรั้งท้ายหากเปรียบเทียบกับประเทศอื่นๆ โดยเฉพาะอย่างยิ่งประเทศมาเลเซียซึ่งเป็นประเทศที่อยู่ในช่วงกำลังพัฒนาเช่นเดียวกับประเทศไทย ทั้งนี้ การประเมินความพร้อมและระบบจัดการในการให้บริการระบบการประมวลผลแบบคลาวด์ดำเนินการโดยกลุ่มพันธมิตรธุรกิจซอฟต์แวร์ (Business Software Alliance: BSA) หรือ “บีเอสเอ” ซึ่งทำหน้าที่เป็นองค์กรสำหรับการตรวจจับการละเมิดลิขสิทธิ์ในซอฟต์แวร์ โดยในช่วงปี พ.ศ. 2559 – พ.ศ. 2561 ที่ผ่านมา บีเอสเอได้ทำการสำรวจประเทศที่ให้บริการและใช้บริการระบบการประมวลผลแบบคลาวด์เพื่อนำมาพิจารณาจัดอันดับว่าประเทศใดจะมีระบบการจัดการเกี่ยวกับระบบการประมวลผลแบบคลาวด์ได้เป็นอย่างดีบ้าง โดยใช้ชื่อเรียกการสำรวจความพร้อมและระบบการจัดการของการให้บริการระบบการประมวลผล

แบบคลาวด์ในครั้งนี้ว่า Asia Cloud Computing Association ประเภท Asia Cloud Computing Readiness อนึ่ง ในการพิจารณาว่าประเทศใดจะมีความพร้อมในอันดับใด บีเอสเอจะอาศัยตัวชี้วัดซึ่งคาดการณ์จากนโยบายที่เหมาะสมซึ่งจะส่งผลโดยตรงต่อการเติบโตของเศรษฐกิจจากการให้บริการระบบการประมวลผลแบบคลาวด์ ซึ่งจะพบว่าในปีพ.ศ. 2559 ประเทศไทยอยู่ในอันดับที่ 21 และในปีพ.ศ. 2561 ประเทศไทยอยู่ในอันดับที่ 19 จากทั้งหมด 24 ประเทศ ซึ่งคำนวณเป็น 80% ของตลาดไอทีโลก และสอบตกในประเด็นเรื่องความเป็นส่วนตัวของข้อมูล โดยจากรายงานการประเมินผลของบีเอสเอได้บันทึกเหตุผลที่ประเทศไทยสอบตกไว้ว่าประเทศไทยไม่มีกฎหมายหรือข้อบังคับเกี่ยวกับเรื่องการเก็บ ใช้ หรือดำเนินการต่างๆ กับข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการคุ้มครองความเป็นส่วนตัวตามข้อบังคับด้านการคุ้มครองข้อมูลของสหภาพยุโรปและตามกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค นอกจากนี้ประเทศไทยยังไม่มีกฎหมายที่กำหนดถึงการแจ้งให้เจ้าของข้อมูลทราบในกรณีที่เกิดการละเมิดข้อมูล รวมทั้งไม่มีกฎหมายหรือมาตรการรองรับสิทธิส่วนบุคคลในการดำเนินการในกรณีที่เกิดการละเมิดความเป็นส่วนตัวของข้อมูลอย่างชัดเจนอีกด้วย ซึ่งจุดนี้ถือเป็นจุดอ่อนที่สำคัญของประเทศไทย อนึ่ง หากพิจารณาการจัดลำดับของบีเอสเอจะพบว่าประเทศที่ได้อันดับ 1 สำหรับการมีระบบการจัดการระบบการประมวลผลแบบคลาวด์ที่ดีในปีพ.ศ. 2559 ได้แก่ ประเทศญี่ปุ่น ตามมาด้วยประเทศสหรัฐอเมริกาและประเทศเยอรมนีตามลำดับ ส่วนในปีพ.ศ. 2561 ได้แก่ ประเทศเยอรมนี ประเทศญี่ปุ่นและประเทศสหรัฐอเมริกาตามลำดับ

สำหรับประเทศไทยเองต้องถือว่าผลการจัดอันดับข้างต้นของบีเอสเอส่งผลกระทบโดยตรงต่อความเชื่อมั่นในการใช้บริการระบบการประมวลผลแบบคลาวด์ภายในประเทศไทย อีกทั้งยังส่งผลทางอ้อมต่อเศรษฐกิจ การลงทุนและการค้าระหว่างประเทศด้วย โดยเฉพาะอย่างยิ่งในช่วงระยะเวลาที่ประเทศไทยกำลังเข้าสู่โมเดลการพัฒนาประเทศ “ประเทศไทย 4.0” แล้ว ผลการจัดอันดับดังกล่าวอาจทำให้ประเทศไทยเสียนักลงทุนจำนวนไม่น้อยที่สนใจจะเข้ามาลงทุนดาต้าเซ็นเตอร์ (Data Center) หรือฐานสำหรับจัดเก็บข้อมูลในประเทศไทย

จากกรณีดังกล่าวข้างต้นจึงนำมาสู่ปัญหาที่ว่าประเทศไทยยังขาดกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ของภาคเอกชนเพราะแม้ว่าประเทศไทยจะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่พระราชบัญญัติดังกล่าวก็ใช้บังคับเฉพาะกรณีที่หน่วยงานของรัฐเป็นผู้จัดเก็บข้อมูลเท่านั้น นอกจากนี้เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่หลายฝ่ายให้ความสนใจและมุ่งหวังว่าจะมีผลใช้บังคับกับประเทศไทยในเร็ววันนั้น จะพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ยังคงไม่สอดคล้องกับรูปแบบหรือโมเดลทางธุรกิจของการให้บริการระบบการประมวลผลแบบคลาวด์อยู่ ทั้งนี้ เนื่องจากร่างพระราชบัญญัติดังกล่าวถูกยกร่างมาเป็นระยะเวลา

ที่ยาวนานกว่าสิบปี แม้ว่าจะมีการแก้ไขร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... หลายครั้ง แต่ร่างพระราชบัญญัติดังกล่าวก็ยังคงไม่ครอบคลุมธุรกิจการให้บริการระบบการประมวลผลแบบคลาวด์เช่นเดิม

ดังนั้น ปัญหาของประเทศไทยเกี่ยวกับการคุ้มครองข้อมูลบุคคลที่ถูกจัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์จึงสามารถแบ่งออกได้เป็น 2 ระยะ กล่าวคือ

ระยะที่ 1 ประเทศไทยกำลังประสบปัญหาการขาดแคลนกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ประการหนึ่ง และ

ระยะที่ 2 หากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ที่กำลังอยู่ในการพิจารณามีผลใช้บังคับแล้ว ประเทศไทยจะประสบปัญหาอีกประการหนึ่ง คือ

(1) ร่างพระราชบัญญัติดังกล่าวไม่สอดคล้องกับรูปแบบธุรกิจหรือรูปแบบการให้บริการระบบการประมวลผลแบบคลาวด์

(2) ร่างพระราชบัญญัติดังกล่าวยังขาดหลักการสำคัญหลายประการเพื่อให้สอดรับกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับสากล

ปัญหาข้างต้นย่อมส่งผลกระทบโดยตรงต่อร่างพระราชบัญญัติที่จะมีผลใช้บังคับและจะทำให้ร่างพระราชบัญญัติที่จะมีผลใช้บังคับดังกล่าว ต้องเข้าสู่กระบวนการแก้ไขปรับปรุงใหม่อีกรอบซึ่งอาจใช้ระยะเวลายาวนานในการแก้ไขปรับปรุง ด้วยเหตุนี้ เพื่อประโยชน์ต่อการจัดทำกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมและเหมาะสมกับธุรกิจของการให้บริการระบบการประมวลผลแบบคลาวด์ที่กำลังได้รับความนิยมอย่างต่อเนื่อง จึงนำมาสู่การศึกษาในครั้งนี้

1.2 วัตถุประสงค์ของการศึกษา

(1) เพื่อศึกษารูปแบบการให้บริการของระบบการประมวลผลแบบคลาวด์เพื่อเป็นพื้นฐานสำหรับการบังคับใช้กฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์

(2) เพื่อศึกษากฎเกณฑ์หรือแนวปฏิบัติระหว่างประเทศ ตลอดจนกฎหมายของประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์ที่มีระบบกฎหมายใกล้เคียงกับประเทศไทยและประเทศที่มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับระบบการประมวลผลแบบคลาวด์โดยเฉพาะ เพื่อเป็นแนวทางสำหรับการยกร่างกฎหมายของประเทศไทย

(3) เพื่อศึกษากฎหมายของประเทศไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์และแนวทางการบังคับใช้กฎหมายดังกล่าวแก่การให้บริการระบบการประมวลผลแบบคลาวด์

(4) เพื่อศึกษาปัญหาที่จะเกิดขึ้นจากการบังคับใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กับการให้บริการระบบการประมวลผลแบบคลาวด์ พร้อมทั้งให้ข้อเสนอแนะ

1.3 สมมติฐานของการศึกษา

การคุ้มครองข้อมูลส่วนบุคคลนับเป็นโครงสร้างพื้นฐานของเศรษฐกิจดิจิทัล ซึ่งการคุ้มครองข้อมูลส่วนบุคคลจะเกิดประสิทธิภาพเมื่อประเทศนั้นๆ มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพ สำหรับประเทศไทย แม้ว่าประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไป ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และในลักษณะกฎหมายเฉพาะเรื่อง เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 เป็นต้น แต่กฎหมายดังกล่าวอาจไม่สามารถบังคับใช้กับข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ได้ นอกจากนี้ แม้ว่าประเทศไทยจะพยายามยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ โดยฉบับล่าสุด คือร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) แต่ร่างพระราชบัญญัติดังกล่าวก็ยังมีความไม่เหมาะสมที่จะใช้บังคับกับข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์

1.4 ขอบเขตของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาถึงปัญหาที่อาจเกิดขึ้นจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งมีสถานะเป็นกฎหมายกลางเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อนำเสนอข้อเสนอแนะสำหรับการปรับปรุงแก้ไขกฎหมายหรือยกร่างกฎหมายดังกล่าวโดยศึกษาเปรียบเทียบกับกฎเกณฑ์หรือแนวปฏิบัติระหว่างประเทศ รวมทั้งกฎหมายของต่างประเทศประกอบ

1.5 วิธีการศึกษาและค้นคว้า

การศึกษาของวิทยานิพนธ์ฉบับนี้ใช้วิธีการศึกษาแบบวิจัยเอกสารโดยผ่านทางการค้นคว้าและรวบรวมข้อมูลจากเอกสารต่างๆ (Documentary research) และเอกสารที่จะใช้ในการศึกษาวิจัยครั้งนี้จะปรากฏอยู่ทั้งในรูปแบบหนังสือ เอกสารการประชุม บทความ วารสารทางวิชาการต่างๆ บทกฎหมาย แนวปฏิบัติหรือกฎเกณฑ์อื่นๆ ของประเทศไทย ต่างประเทศ รวมทั้งองค์กรต่างประเทศ สารนิพนธ์ วิทยานิพนธ์และข้อมูลทางอิเล็กทรอนิกส์ทั้งภาษาไทยและภาษาต่างประเทศ เป็นต้น ภายหลังการศึกษาดังกล่าวผู้เขียนจะนำข้อมูลที่ได้รับมาถ่ายทอดโดยวิธีการพรรณนาและการวิเคราะห์ (Descriptive and analytical method)

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

จากการศึกษาในครั้งนี้ผู้เขียนคาดว่าข้อมูลจากการศึกษาพร้อมทั้งข้อเสนอแนะจะเป็นประโยชน์ต่อผู้ที่มีความสนใจศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะนำไปใช้บังคับกับระบบการประมวลผลแบบคลาวด์ นอกจากนี้ ผู้เขียนยังคาดหวังว่าข้อเสนอแนะที่นำเสนอไว้ในวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อการยกร่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) และการแก้ไขปรับปรุงพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ด้วยเช่นกัน

บทที่ 2
ความทั่วไปเกี่ยวกับระบบการประมวลผลแบบคลาวด์ (Cloud Computing)

เมื่อเทคโนโลยีถือเป็นองค์ประกอบที่สำคัญในการทำงานของภาครัฐและการประกอบธุรกิจของภาคเอกชน เพราะเทคโนโลยีสามารถนำมาใช้เพื่อเพิ่มประสิทธิภาพการผลิต ลดต้นทุนการผลิต และสร้างมูลค่าให้แก่ผลิตภัณฑ์หรือบริการของแต่ละภาคส่วนได้ ดังนั้น บริษัทเอกชนใหญ่ๆ จึงนำเทคโนโลยีหลากหลายประเภทมาใช้ในการประกอบธุรกิจของตนเอง อย่างไรก็ตาม การนำเทคโนโลยีแต่ละประเภทมาใช้ย่อมก่อให้เกิดต้นทุนและค่าใช้จ่ายจำนวนมาก อาทิ ค่าใช้จ่ายเกี่ยวกับฮาร์ดแวร์ ซอฟต์แวร์และค่าใช้จ่ายในการบำรุงรักษา เช่น การจ้างผู้เชี่ยวชาญมาคอยควบคุมดูแล เป็นต้น ดังนั้น การจะได้เทคโนโลยีที่มีประสิทธิภาพดี จึงมีราคาแพงและไม่สามารถเข้าถึงได้โดยผู้ประกอบการรายย่อย และแม้กระทั่งผู้ประกอบการรายใหญ่เองก็อาจมองว่าการลงทุนดังกล่าวไม่คุ้มค่ากับผลตอบแทนที่จะได้รับในอนาคต นอกจากนี้ผู้ประกอบการที่ได้ลงทุนไปแล้วบางรายก็อาจไม่อยากเสียค่าใช้จ่ายในการบำรุงรักษา อัพเกรดระบบทุกๆ ปี ดังนั้น ระบบการประมวลผลแบบคลาวด์ซึ่งเป็นเทคโนโลยีการจัดเก็บและประมวลผลข้อมูลจึงเกิดขึ้นมาเพื่อตอบโจทย์ของผู้ใช้บริการ ตั้งแต่ช่วงปลายทศวรรษ 1990 เป็นต้นมา[1] โดยในยุคเริ่มต้นระบบการประมวลผลแบบคลาวด์ได้รับการพัฒนาขึ้นเพื่อรองรับคอมพิวเตอร์รูปแบบต่างๆ ในอนาคตที่จะต้องทำงานได้อย่างรวดเร็ว ถูกต้องแม่นยำ โดยนำเอาแนวคิดของการบูรณาการระหว่างการประมวลผลรูปแบบต่าง ๆ 3 รูปแบบ[2] และเรียกการบูรณาการดังกล่าวโดยใช้คำแทนว่า “คลาวด์” หรือ “กลุ่มเมฆ” เพื่อสื่อถึงเครือข่ายอินเทอร์เน็ตที่เชื่อมโยงฮาร์ดแวร์และซอฟต์แวร์เข้าด้วยกัน ได้แก่

1. การประมวลผลแบบกระจาย (Distributed Computing) ซึ่งเกิดขึ้นจากการที่คอมพิวเตอร์ส่วนบุคคลไม่สามารถตอบสนองความต้องการของผู้ใช้งานภายในองค์กรได้อย่างทั่วถึง และการประมวลผลแบบรวมศูนย์ (Centralized Computing) ที่ใช้อยู่เดิมมีข้อจำกัดในการใช้งาน เนื่องจากจะต้องลงทุนกับโฮสคอมพิวเตอร์ (Host Computer) ที่มีประสิทธิภาพสูงโดยต้องใช้เงิน

---

[1] Jongjin, " ระบบประมวลผลกลุ่มเมฆ (Cloud Computing)," สืบค้นเมื่อวันที่ 28 สิงหาคม 2559, จาก http://www.vcharkarn.com/blog/38378/4390

[2] ชาญชัย อรรคผาติ, “ปัจจัยที่ส่งผลต่อทัศนคติในการยอมรับในเทคโนโลยีคลาวด์คอมพิวติ้ง เพื่อประยุกต์ใช้ในการให้บริการระบบบัญชีออนไลน์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในมุมมองของผู้ทำบัญชี,” (วิทยานิพนธ์มหาบัณฑิต คณะการบัญชี มหาวิทยาลัยธรุกิจบัณฑิตย์, 2557), น.10.

ลงทุนเป็นจำนวนมากตั้งแต่การเริ่มต้นใช้งาน นอกจากนี้การประมวลผลแบบรวมศูนย์นั้นค่อนข้างล่าช้าด้วยเช่นกัน ดังนั้น จึงเกิดแนวคิดที่ผู้คนสามารถอุทิศทรัพยากรคอมพิวเตอร์ส่วนตัวเพื่อใช้ในการประมวลผลงานหรือโปรแกรมของโครงการหนึ่งๆ ได้ หรือที่รู้จักกันอีกชื่อหนึ่งว่า “การประมวลผลแบบอุทิศ” (Volunteer Computing) ทั้งนี้ ภายใต้แนวคิดดังกล่าวก่อให้เกิดความจำเป็นที่จะต้องมีการจัดสรรทรัพยากรเพื่อที่จะทำให้สามารถกระจายและแจกจ่ายการใช้งานข้อมูลในระบบหรือทรัพยากรอื่นๆ ให้สามารถใช้งานร่วมกันได้ทั่วทั้งองค์กร รวมทั้งระหว่างองค์กรย่อยๆ ด้วย อาทิ ฐานข้อมูล (Database) ข่าวสาร เครื่องคอมพิวเตอร์ เครื่องพิมพ์ เครื่องโทรสาร เครื่องสแกนเนอร์ เป็นต้น ซึ่งการประมวลผลแบบนี้จะช่วยเพิ่มประสิทธิภาพของการใช้งานได้เป็นอย่างดี[3] ทั้งนี้ หลักการทำงานของระบบการประมวลผลแบบกระจายนั้น จะประกอบไปด้วยคอมพิวเตอร์เซิร์ฟเวอร์เครื่องหนึ่งหรือหลายเครื่องรวมกัน โดยจะทำหน้าที่ในการกระจายการประมวลผลไปให้คอมพิวเตอร์อื่นๆ บนเครือข่าย นอกจากนี้เซิร์ฟเวอร์ยังทำหน้าที่ในการรวบรวมและบันทึกผลลัพธ์จากการประมวลผลอีกด้วย

2. การประมวลผลแบบกริด (Grid Computing) ซึ่งมีลักษณะเป็นการแชร์ทรัพยากรร่วมกันระหว่างองค์กรเพื่อให้เกิดระบบสารสนเทศระบบเดียวกัน[4] ทั้งนี้ องค์กรที่ใช้หรือแชร์ทรัพยากรร่วมกันนั้นจะถูกกำหนดและควบคุมภายใต้กฎขององค์กรที่เรียกว่า “องค์กรเสมือน” (Virtual organization) โดยการประมวลผลแบบกริดสามารถแบ่งระดับการแชร์ทรัพยากรระหว่างกันออกเป็น 3 ระดับย่อย ได้แก่ Cluster Grid, Campus Grid (หรือบางที่เรียกว่า Corporate Grid) และ Global Grid

ภายใต้ระบบการประมวลผลแบบกริดนั้น หัวใจสำคัญของการประมวลผลประเภทนี้นอกจากจะเป็นการแชร์ทรัพยากรระหว่างกันแล้ว หัวใจสำคัญอีกประการหนึ่งคือ ความปลอดภัย เนื่องจากการประมวลผลแบบกริดเป็นการแชร์ทรัพยากรระหว่างองค์กรหลายองค์กรภายใต้องค์กรเสมือนหนึ่ง ดังนั้น องค์กรแต่ละองค์กรภายในองค์กรเสมือนย่อมมีโดเมนหรือขอบเขตในการรักษาความปลอดภัยที่แตกต่างกันออกไป เช่น การกำหนดผู้ใช้ของทรัพยากร และการจำกัดสิทธิในการใช้

---

[3] _____, "เทคโนโลยีการประมวลผลแบบกระจาย (Distributed Computing)," สืบค้นเมื่อวันที่ 18 กันยายน 2559, จาก http://app.eduzones.com/portal/siamese/1924

[4] Santosh Kumar and R.H. Goudar, “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A survey,” International Hournal of Future Computer and Communication 356, Vol.1, No.4, p.357, (December 2012).

งานทรัพยากรของผู้ใช้แต่ละราย ตลอดจนการเข้ารหัสข้อมูล เป็นต้น[5] การประมวลผลแบบกริด ได้รับความนิยมเป็นอย่างมากในการศึกษาวิจัยทั้งในสถาบันการศึกษาและหน่วยงานภาคเอกชน

3. การประมวลผลแบบสาธารณูปโภค (Utility Computing) จุดเริ่มต้นของการประมวลผลแบบสาธารณูปโภคเกิดขึ้นจากแนวคิดที่พยายามจะให้การให้บริการระบบคอมพิวเตอร์สามารถให้บริการได้อย่างการบริการสาธารณูปโภค ดังนั้น การประมวลผลแบบสาธารณูปโภค จึงหมายถึง การให้บริการทรัพยากรคอมพิวเตอร์ เช่น พลังการประมวลผลของซีพียู และพื้นที่จัดเก็บข้อมูล รวมถึงแบนด์วิธ (Bandwidth) ของเครือข่าย โดยการให้บริการดังกล่าวสามารถวัดออกมาเป็นหน่วยของการใช้บริการได้เหมือนกันกับบริการสาธารณูปโภค ได้แก่ น้ำประปา ไฟฟ้า และโทรศัพท์ เป็นต้น

หากย้อนพิจารณากลับไปถึงต้นกำเนิดของการประมวลผลแบบสาธารณูปโภค ในยุค ค.ศ. 1961 ซึ่งเป็นยุคที่เกิดแนวคิดในการอนุญาตให้บุคคลต่างๆ สามารถเชื่อมต่อคอมพิวเตอร์เมนเฟรมผ่านอุปกรณ์ต่างๆ เพื่อบังคับควบคุมโปรแกรม และจัดการข้อมูลซึ่งถูกจัดเก็บไว้ที่คอมพิวเตอร์เมนเฟรมดังกล่าวได้พร้อมกันทีละหลายๆ คน หรือที่เรียกว่า แนวคิด “Time-sharing”[6] นักวิทยาศาสตร์คอมพิวเตอร์ท่านหนึ่งซึ่งมีนามว่า Dr. John McCarthy เคยกล่าวไว้ว่า

“...เทคโนโลยีระบบคอมพิวเตอร์แบบแชร์เวลาประมวลผล (Time sharing) จะนำไปสู่โลกอนาคตที่พลังการประมวลผลและแอพพลิเคชั่นต่างๆ สามารถขายได้อย่างธุรกิจบริการสาธารณูปโภค...”

จากคำกล่าวดังกล่าว ทำให้ในปลายยุคคริสตศักราชที่ 60 ถึง 70 มีผู้ให้ความสนใจกับไอเดียดังกล่าวเป็นอย่างมากและถือเป็นจุดกำเนิดของการประมวลผลแบบสาธารณูปโภค ทั้งนี้การประมวลผลแบบสาธารณูปโภคที่เกิดขึ้นนั้นจะไม่จำกัดว่าจะต้องใช้สถาปัตยกรรมใดและใช้เทคโนโลยีใดมาสร้างให้เกิดบริการที่เป็นสาธารณูปโภค ดังนั้น ผู้ให้บริการรายหนึ่งอาจจะมีศูนย์ข้อมูลขนาดใหญ่เพียงแห่งเดียวเพื่อให้บริการสาธารณูปโภคแก่ลูกค้าซึ่งกระจายตัวอยู่ทั่วโลกก็ได้

ภายใต้ระบบการประมวลผลแบบสาธารณูปโภค ผู้ให้บริการจะสามารถวัดปริมาณการใช้งานบริการทรัพยากรคอมพิวเตอร์ในช่วงเวลาหนึ่งได้ เช่น หน่วยวัดของการใช้งานซีพียูคิดเป็น

---

[5] SIVADON, “จาก Grid Computing ไปถึง Cloud Computing ตอนที่ 1,” สืบค้นเมื่อวันที่ 18 กันยายน 2559, จาก htttps://javaboom.wordpress.com/2008/11/27grid2cloud

[6] ชินดนัย สังคะคุณ, “การจัดเก็บภาษีเงินได้นิติบุคคลจากการให้บริการของบริษัทต่างประเทศ: กรณีการให้บริการประมวลผลแบบคลาวด์,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), น.10.

CPU-hour ต่อเดือน ซึ่งหมายถึงในหนึ่งเดือนมีการประมวลผลซีพียูทั้งหมดกี่ชั่วโมง และหน่วยวัดของการใช้พื้นที่จัดเก็บข้อมูลคิดเป็นกิกะไบต์ (GB) ต่อเดือน เป็นต้น นอกจากนี้ผู้ใช้บริการยังสามารถเข้าถึงทรัพยากรคอมพิวเตอร์ได้ทุกหนแห่งที่มีระบบเครือข่าย เสมือนกับว่าผู้ใช้บริการสามารถใช้น้ำและไฟฟ้าได้ทุกที่นั่นเอง ซึ่งจากการใช้งานดังกล่าวผู้ให้บริการจะสามารถคิดค่าบริการตามจำนวนการใช้งานได้ก่อให้เกิดตลาดการค้าขายบริการทรัพยากรคอมพิวเตอร์เกิดขึ้น ซึ่งนับเป็นข้อดีของการประมวลผลแบบสาธารณูปโภค

ดังนั้น จะเห็นได้ว่า ระบบการประมวลผลแบบคลาวด์จึงมิใช่เทคโนโลยีที่ถูกคิดค้นขึ้นใหม่ แต่กลับมีลักษณะเป็นเทคโนโลยีที่เกิดขึ้นจากการนำเอาระบบการประมวลผลที่มีอยู่เดิมมาวิวัฒนาการให้เกิดเป็นเทคโนโลยีใหม่ที่ทันสมัยและรองรับการใช้งานได้มากกว่าเทคโนโลยีในรูปแบบเดิม อย่างไรก็ตาม หากพิจารณาในทางวิชาการ ผู้มีพยายามให้คำจำกัดความของระบบการประมวลผลแบบคลาวด์จำนวนมาก แต่ก็ยังไม่ปรากฏแน่ชัดว่าคำจำกัดความใดจะเป็นคำจำกัดความที่ถูกต้องครบถ้วนที่สุด ดังนี้

สำนักสิทธิบัตรและเครื่องหมายการค้าแห่งสหรัฐอเมริกา (United State Patent and Trademark office: USPTO) ให้นิยามของระบบการประมวลผลแบบคลาวด์ไว้คือ “แอพพลิเคชั่นการประมวลผลทางไกล (Remote Computing Applications)”[7]

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology หรือ NIST) ของประเทศสหรัฐอเมริกา ให้นิยามของระบบการประมวลผลแบบคลาวด์ไว้คือ “รูปแบบของการบริการที่ช่วยเพิ่มความสะดวกสบายและความสามารถในการเข้าถึงเครือข่ายของทรัพยากรที่ใช้ในระบบการประมวลผลร่วมกัน ซึ่งเป็นทรัพยากรที่สามารถปรับแต่งได้ (เช่น เครือข่าย เซิร์ฟเวอร์ ที่จัดเก็บข้อมูล แอพพลิเคชั่น และบริการต่างๆ) โดยผู้ใช้งานสามารถเรียกใช้งานเครือข่ายดังกล่าวได้ตามความต้องการของผู้ใช้งานผ่านช่องทางต่างๆ ที่หลากหลายและสามารถเพิ่มหรือลดทรัพยากรที่ต้องการใช้งานได้อย่างสะดวกรวดเร็ว ไม่ก่อให้เกิดความยุ่งยากในการบริหารจัดการหรือการติดต่อกับผู้ให้บริการ”[8]

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย ให้นิยามของระบบการประมวลผลแบบคลาวด์ไว้คือ “ระบบประมวลผลแบบหนึ่ง ภายใต้แนวคิดการใช้งานทรัพยากร

---

[7] Jongjin, “ระบบประมวลผลกลุ่มเมฆ (Cloud Computing),” สืบค้นเมื่อวันที่ 28 สิงหาคม 2559, จาก http://www.vcharkarn.com/blog/38378/4390

[8] ชินดนัย สังคะคุณ, *อ้างแล้ว เชิงอรรถที่ 6*, น.14-15.

เทคโนโลยีสารสนเทศและการสื่อสารจำนวนมหาศาลผ่านระบบอินเทอร์เน็ต ในรูปแบบของสาธารณูปโภคโดยมองทรัพยากรเหล่านั้น เช่น เซิร์ฟเวอร์ เครือข่ายและซอฟต์แวร์ ในรูปแบบเสมือนที่สามารถปรับเปลี่ยนความต้องการของผู้ใช้งานได้โดยง่าย”[9]

สำนักงานราชบัณฑิตยสภาร่วมกับสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ให้นิยามของระบบการประมวลผลแบบคลาวด์ไว้คือ “การประมวลผลแบบแบ่งปันทรัพยากรผ่านเครือข่าย”[10]

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (The Organization for Economic Cooperation and Development หรือ OECD) ให้นิยามของระบบการประมวลผลแบบคลาวด์ไว้คือ “การให้บริการเกี่ยวกับคอมพิวเตอร์ที่เป็นมาตรฐาน สามารถปรับแต่งและเรียกใช้งานได้ตามความต้องการผ่านเครือข่ายอินเทอร์เน็ต ซึ่งบริการดังกล่าวอาจประกอบไปด้วย บริการด้านการประมวลผล บริการด้านการจัดเก็บข้อมูล บริการด้านซอฟต์แวร์ และบริการด้านการจัดการข้อมูล โดยบริการดังกล่าวเหล่านี้เกิดขึ้นจากการทำงานประสานกันของทรัพยากรทั้งที่เป็นทรัพยากรทางกายภาพ (physical resources) และทรัพยากรเสมือน (virtual resources) อันได้แก่ เครือข่าย เซิร์ฟเวอร์ และแอพพลิเคชั่น”[11]

จากบทนิยามดังกล่าว จะเห็นได้ว่าระบบการประมวลผลแบบคลาวด์เป็นระบบที่นำเอาคอมพิวเตอร์มาเชื่อมเข้าหากันผ่านอินเทอร์เน็ตเพื่อจัดเก็บข้อมูลหรือประมวลผลข้อมูลขนาดใหญ่ ซึ่งจะทำให้ผู้ใช้บริการไม่ต้องลงทุนในระบบ แต่ก็สามารถใช้เทคโนโลยีได้อย่างเต็มขีดความสามารถ อนึ่ง เป็นที่น่าสังเกตว่าแม้ว่าระบบการประมวลผลแบบคลาวด์จะเกิดขึ้นมาตั้งแต่ปลายทศวรรษ 1990 เป็นต้นมา แต่ระบบการประมวลผลแบบคลาวด์พึ่งจะได้รับความนิยมเป็นอย่างมากในต่างประเทศในช่วงปีค.ศ. 2009 เป็นต้นมาเท่านั้น ทั้งนี้ เนื่องจากในยุคเริ่มต้นผู้ใช้บริการยังคงมีความวิตกกังวลกับความปลอดภัยของการใช้งาน ความยุ่งยากในการเปลี่ยนแปลงจากระบบเดิมซึ่งเป็นระบบที่ไม่มีการแบ่งปันทรัพยากรระหว่างกัน สำหรับประเทศไทย ระบบการประมวลผลแบบคลาวด์ก็พึ่งจะได้รับความนิยมในช่วงปีค.ศ. 2011 ที่ผ่านมา เนื่องจากในปีดังกล่าวประเทศไทยประสบปัญหา

---

[9] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, คู่มือการเลือกใช้บริการ Cloud Computing, (กรุงเทพมหานคร:กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2556), น.5.

[10] สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, “คำศัพท์ Cloud computing,” สืบค้นเมื่อวันที่ 18 กันยายน 2559, จาก http://www.thaiglossary.org/node/51370

[11] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, *อ้างแล้ว เชิงอรรถที่ 9,* น.16-17.

เกี่ยวกับน้ำท่วมใหญ่ในพื้นที่ภาคกลาง ซึ่งเป็นพื้นที่ตั้งของผู้ประกอบการทั้งรายใหญ่และรายย่อย มีนิคมอุตสาหกรรมมากมายอยู่ในพื้นที่ดังกล่าว ดังนั้น เมื่อภายหลังเหตุการณ์ดังกล่าวผ่านไป ผู้ประกอบการหลายรายที่แต่เดิมใช้เทคโนโลยีโดยลงทุนระบบเซิร์ฟเวอร์ของตน จึงเกิดปัญหาว่าเซิร์ฟเวอร์โดนน้ำท่วมได้รับความเสียหาย และไม่สามารถกู้คืนข้อมูลที่สำคัญกลับมาได้ โดยเฉพาะอย่างยิ่งข้อมูลเกี่ยวกับการเรียกเก็บเงินหรือคำสั่งซื้อของลูกค้า ดังนั้น ภายหลังเหตุการณ์ดังกล่าว ผู้ประกอบการหลายรายในไทยจึงหันมาใช้บริการระบบการประมวลผลแบบคลาวด์มากยิ่งขึ้น[12] โดยบางรายอาจใช้วิธีการใช้คู่ขนานระหว่างเซิร์ฟเวอร์เดิมและระบบบการประมวลผลแบบคลาวด์ ด้วยเหตุนี้ ระบบการประมวลผลแบบคลาวด์จึงได้รับความนิยมตั้งแต่นั้นเป็นต้นมาและเป็นอีกธุรกิจบริการหนึ่งที่จะช่วยสร้างรายได้รวมให้แก่ประเทศในมูลค่ามหาศาล

แม้ระบบการประมวลผลแบบคลาวด์จะมิใช่เทคโนโลยีที่เกิดขึ้นใหม่ แต่ก็เป็นเทคโนโลยีที่มีความซับซ้อนและได้รับการกล่าวถึงในวงแคบ ผู้ใช้บริการบางรายอาจใช้บริการระบบการประมวลผลแบบคลาวด์อยู่ในชีวิตประจำวันโดยไม่อาจทราบว่าสิ่งที่ตนกำลังใช้งานอยู่คือระบบการประมวลผลแบบคลาวด์รูปแบบหนึ่ง ดังนั้น ผู้เขียนจึงศึกษารวบรวมความรู้พื้นฐานเกี่ยวกับระบบการประมวลผลแบบคลาวด์ เพื่อประโยชน์ในการศึกษาทำความเข้าใจ ดังนี้

2.1 ความหมายคำศัพท์และคำย่อที่ใช้ในการศึกษา

แพลตฟอร์ม (Platform) หมายถึง ระบบซอฟต์แวร์ที่ถูกออกแบบให้ทำงานแยกระดับชั้น โดยมีกลุ่มซอฟต์แวร์ระดับล่าง (Low level) ทำงานบริการให้กลุ่มซอฟต์แวร์ระดับที่สูงกว่าจนถึงขั้นระดับ Application[13]

โปรแกรมประยุกต์ หรือแอพพลิเคชั่นซอฟต์แวร์ (Application Software) หรือที่มักจะเรียกกันอย่างย่อว่า แอพพลิเคชั่นนั้น หมายถึง โปรแกรมหรือกลุ่มของโปรแกรมซึ่งถูกออกแบบขึ้นมาเพื่อวัตถุประสงค์ในการใช้งานอย่างใดอย่างหนึ่ง อาทิเช่น ซอฟต์แวร์ฐานข้อมูล (Database) ซอฟต์แวร์ประมวลผลคำ (Word processing) ซอฟต์แวร์ตารางวิเคราะห์แบบอิเล็กทรอนิกส์ (Electronic Spreadsheet) ซอฟต์แวร์นำเสนอ (Presentation Software) ซอฟต์แวร์กราฟิก (Graphic Software) และซอฟต์แวร์สื่อสารโทรคมนาคม เป็นต้น ซึ่งซอฟต์แวร์ต่างๆ เหล่านี้ไม่

---

[12] SuperGrit, “รับมือภัยพิบัติด้วย “คลาวด์ คอมพิวติ้ง,” สืบค้นเมื่อวันที่ 11 พฤศจิกายน 2560, จาก https://www.blognone.com/node/30896

[13] ชินดนัย สังคะคุณ, *อ้างแล้ว เชิงอรรถที่ 6,* น.5.

สามารถทำงานได้ด้วยตัวของมันเอง แต่จะต้องอาศัยการทำงานของระบบปฏิบัติการ (Operating System) ร่วมด้วย[14]

เวิลด์ไวด์เว็บ (World Wide Web) หรือที่มักเรียกกันอย่างย่อว่า www หมายถึง แหล่งรวมข้อมูลขนาดใหญ่บนอินเทอร์เน็ต

เซิร์ฟเวอร์ (Server) หมายถึง เครื่องคอมพิวเตอร์หลักในระบบเครือข่ายหนึ่งๆ ทำหน้าที่เป็นตัวควบคุมคอมพิวเตอร์เครื่องอื่นๆ ที่มาเชื่อมต่อในเครือข่ายเดียวกัน และมีหน้าที่จัดการดูแลคอมพิวเตอร์เครื่องอื่นๆ ว่า ขอใช้โปรแกรมใด ข้อมูลใด เพื่อที่จะได้จัดการส่งไปให้ ในขณะเดียวกันก็เป็นที่เก็บข้อมูลและโปรแกรมคอมพิวเตอร์ในเครือข่ายที่จะมาเรียกใช้ได้

2.2 คุณสมบัติของระบบการประมวลผลแบบคลาวด์

เนื่องจากระบบการประมวลผลแบบคลาวด์เป็นระบบที่มุ่งให้บริการผู้ใช้บริการโดยมีวัตถุประสงค์ให้ผู้ใช้บริการเกิดความสะดวก รวดเร็วในการใช้งาน รวมทั้งเกิดความปลอดภัยในการใช้งานด้วย ดังนั้น โครงสร้างของระบบการประมวลผลแบบคลาวด์จึงจำเป็นต้องพัฒนาเพื่อรองรับวัตถุประสงค์ในการให้บริการดังกล่าว ซึ่งระบบการประมวลผลแบบคลาวด์จะสามารถตอบสนองวัตถุประสงค์การใช้งานได้ก็ต่อเมื่อผู้ให้บริการติดตั้งโครงสร้างพื้นฐาน (Infrastructure) ของระบบให้มีคุณสมบัติ[15]ดังต่อไปนี้

1. Transparency

คุณสมบัติในการ Transparency หมายถึง Transparent load-balancing ซึ่งก็คือความพยายามที่จะทำให้เกิดการทำงานที่สมดุล (Balance) เมื่อผู้ใช้บริการหลายรายเรียกใช้งานแอพพลิเคชั่นพร้อมกัน ทั้งนี้ ระบบการประมวลผลแบบคลาวด์ที่ดีจะต้องสร้างสมดุลของการใช้งานโดยการกระจายการประมวลผลไปให้เซิร์ฟเวอร์อื่นช่วยประมวลผล ดังนั้น ผู้ใช้บริการจะสามารถใช้งานได้อย่างรื่นไหลโดยไม่สะดุด และผู้ใช้บริการจะไม่สามารถทราบได้เลยว่าขณะนี้ระบบได้ให้บริการโดยใช้เซิร์ฟเวอร์อีกตัวหนึ่งมารองรับการใช้งานของผู้บริการ

---

[14] *เพิ่งอ้าง*, น.7.

[15] _____, "โครงสร้างพื้นฐานของระบบ Cloud Computing," สืบค้นเมื่อวันที่ 10 มกราคม 2560, จาก https://blog.sogoodweb.com/Article/Detail/9115

2. Scalability

คุณสมบัติประเภท Scalability จะช่วยให้ผู้ใช้บริการสามารถปรับขนาดระบบได้ตามภาระงาน เนื่องจากระบบการประมวลผลแบบคลาวด์เกิดขึ้นจากแนวคิดที่จะใช้ทรัพยากรอิเล็กทรอนิกส์ร่วมกัน หรือ Time-sharing ดังนั้น เพื่อให้ผู้ใช้บริการอื่นสามารถเข้าถึงศูนย์กลางข้อมูล (Data Center) ได้อย่างสะดวก รวดเร็วและปลอดภัย ระบบการประมวลผลแบบคลาวด์จึงปลดล็อคขนาดระบบการใช้งานของผู้ใช้บริการที่ใช้งานอยู่เดิมเพื่อรองรับการใช้งานของผู้ใช้บริการรายใหม่ หากจะอธิบายให้เห็นภาพโดยง่าย กล่าวคือ เดิมผู้ใช้บริการรายหนึ่งใช้งานอยู่เพียงครึ่งหนึ่งของเซิร์ฟเวอร์ทั้งหมด การที่ระบบมีคุณสมบัติปรับลดขนาดในการใช้งานได้ ผู้ใช้บริการท่านนั้นก็จะชำระค่าบริการเพียงส่วนที่ตนใช้งานและผู้ให้บริการก็จะนำเซิร์ฟเวอร์ที่เหลืออีกครึ่งหนึ่งไปแบ่งปันให้ผู้อื่นใช้งานต่อได้นั่นเอง

3. Intelligent Monitoring

คุณสมบัติประเภท Intelligent Monitoring ของระบบการประมวลแบบคลาวด์ หมายถึง การที่ระบบการประมวลผลแบบคลาวด์มีระบบหรือกลไกการทำงานที่สามารถตรวจสอบได้ว่าแอพพลิเคชั่นหรือบริการใดเกิดปัญหาในการใช้งานตรงไหน อย่างไร เพื่อให้สามารถแก้ไขปัญหาได้อย่างทันท่วงที เนื่องจากในอดีตการใช้งานเทคโนโลยี (อาทิ คอมพิวเตอร์ส่วนบุคคล) และระบบซอฟต์แวร์เกิดมีปัญหาหนทางเดียวที่จะสามารถแก้ไขได้คือการนำเครื่องไปให้ผู้มีความรู้หรือความชำนาญแก้ไข แต่สำหรับระบบการประมวลผลแบบคลาวด์ซึ่งพัฒนาขึ้นเพื่อให้เกิดความสะดวกรวดเร็วในการใช้งาน การแก้ไขปัญหาได้อย่างทันท่วงทีย่อมเป็นคุณสมบัติที่โดดเด่นประการหนึ่งที่จะขาดไปไม่ได้

4. Security

เนื่องจากข้อมูลทั้งหมดถูกเก็บไว้ในระบบการประมวลผลแบบคลาวด์ซึ่งจะมีความเสี่ยงว่าข้อมูลดังกล่าวอาจถูกขโมยหรือทำให้เกิดความเสียหายขึ้นได้จากการโจมตี ดังนั้น ในการออกแบบระบบการประมวลผลแบบคลาวด์จึงต้องคำนึงถึงความปลอดภัยเป็นคุณสมบัติหลักที่ระบบการประมวลผลแบบคลาวด์จะต้องมี

คุณสมบัติของระบบการประมวลผลแบบคลาวด์ข้างต้นถือเป็นปัจจัยหนึ่งในการเลือกใช้งานระบบการประมวลผลแบบคลาวด์ของผู้ใช้บริการ ดังนั้น จึงเป็นคุณสมบัติที่ผู้ให้บริการจำเป็นจะต้องมีเพื่อให้ผู้ใช้บริการมาใช้บริการระบบการประมวลผลแบบคลาวด์ของตน

2.3 องค์ประกอบของระบบการประมวลผลแบบคลาวด์

ในการทำงานเพื่อตอบสนองความต้องการของผู้ใช้บริการนั้น ระบบการประมวลผลแบบคลาวด์ถูกพัฒนาขึ้นโดยอาศัยส่วนประกอบ 3 ส่วนในการให้บริการระบบไม่ว่าจะเพื่อประมวลผล หรือ จัดเก็บข้อมูล ดังนี้

1. อุปกรณ์อิเล็กทรอนิกส์ของผู้ใช้บริการ (Client Computer)

ในการเข้าถึงระบบการประมวลผลแบบคลาวด์ ผู้ใช้บริการจำเป็นจะต้องอาศัยอุปกรณ์อิเล็กทรอนิกส์ของตนซึ่งสามารถเชื่อมต่อระบบอินเทอร์เน็ตได้ในการเข้าถึงระบบ แต่เดิมในอดีตในยุคที่อินเทอร์เน็ตยังมีลักษณะเป็นการเชื่อมต่อโดยอาศัยสาย LAN อุปกรณ์อิเล็กทรอนิกส์ก็เป็นส่วนประกอบหนึ่งในการใช้งานเช่นกัน โดยในอดีตอุปกรณ์อิเล็กทรอนิกส์ที่สำคัญได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer :PC) และคอมพิวเตอร์โน้ตบุ๊ก (Notebook)

อย่างไรก็ตาม แม้ในปัจจุบันระบบอินเทอร์เน็ตจะเข้าสู่ยุคการของเชื่อมต่อไร้สายและเกิดระบบเทคโนโลยีการประมวลผลแบบคลาวด์แล้วก็ตาม อุปกรณ์อิเล็กทรอนิกส์ก็ยังคงเป็นส่วนประกอบหนึ่งในการใช้เทคโนโลยีเช่นเดิม แต่เนื่องจากการพัฒนาอุปกรณ์อิเล็กทรอนิกส์ที่ย่อส่วนอุปกรณ์ภายในให้มีขนาดเล็กลงจากเดิม สามารถพกพาไปใช้งานได้ทุกที่ทุกเวลา ดังนั้น อุปกรณ์อิเล็กทรอนิกส์ที่จะนำมาใช้กับระบบการประมวลผลแบบคลาวด์จึงไม่ได้จำกัดอยู่ที่ คอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC) หรือ คอมพิวเตอร์โน้ตบุ๊ก (Notebook) อีกต่อไป แต่อุปกรณ์อิเล็กทรอนิกส์ที่สามารถใช้งานกับระบบการประมวลผลแบบคลาวด์ยังรวมไปถึง คอมพิวเตอร์เน็ตบุ๊ก (Netbook) แท็บเล็ต (Tablet) หรือ โทรศัพท์มือถือประเภทสมาร์ทโฟน เป็นต้น

หากพิจารณาโทรศัพท์มือถือในยุคปัจจุบันจะพบว่าเทคโนโลยีการผลิตโทรศัพท์มือถือพัฒนาอย่างก้าวกระโดดเป็นอย่างมาก ทั้งนี้ ในอดีตโทรศัพท์มือถือมีฟังก์ชั่นสำหรับการใช้งานเพื่อรับสายเข้าและโทรออกเป็นหลักเท่านั้น แตกต่างจากโทรศัพท์มือถือในรูปแบบของสมาร์ทโฟนในปัจจุบันที่นอกจากการฟังก์ชั่นการทำงานแบบเดิมแล้ว โทรศัพท์มือถือในปัจจุบันยังสามารถทำธุรกรรมต่างๆ ผ่านทางโทรศัพท์มือถือได้อีกด้วย ดังนั้น ในการให้บริการระบบการประมวลผลแบบคลาวด์ จึงมีผู้ให้บริการโทรศัพท์มือถือและผู้ให้บริการเครือข่ายโทรศัพท์จำนวนมากลงทุนในการพัฒนาระบบการประมวลผลแบบคลาวด์เพื่อให้บริการแก่ลูกค้าของตน ไม่ว่าจะเป็น Android, Windows, Apple หรือผู้ให้บริการเครือข่ายโทรศัพท์ เช่น True เป็นต้น

นอกจากนี้ ผู้ผลิตเครื่องคอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์โน้ตบุ๊ก หลายเจ้าก็หันมาให้ความสนใจในการพัฒนาระบบการประมวลผลแบบคลาวด์เพื่อให้บริการแก่ลูกค้าของตนเองเช่นกัน อาทิ Acers, Macs, Lenovo หรือ Dells เป็นต้น อย่างไรก็ตาม สำหรับกรณีของ Dells นับว่า

Dells ได้ให้ความสนใจในการพัฒนาระบบการประมวลผลแบบคลาวด์เพื่อให้บริการแก่ลูกค้าของ Dells มาชั่วระยะเวลาหนึ่งโดยถือเป็นผู้ให้บริการคอมพิวเตอร์รายแรกที่ให้ความสนใจระบบการประมวลผลประเภทนี้ เนื่องจาก ในต้นปี ค.ศ. 2007 Dells ได้ยื่นขอจดทะเบียนเครื่องหมายการค้า "Cloud Computing" สำหรับผลิตภัณฑ์ฮาร์ดแวร์ประเภทศูนย์ข้อมูล (Data Center) และสภาพแวดล้อมของระบบประมวลผลที่ปรับเปลี่ยนขนาดได้ขนาดใหญ่ (Mega-scale computing environment) แต่ในที่สุดเมื่อสำนักสิทธิบัตรและเครื่องหมายการค้าแห่งสหรัฐอเมริกา (United State Patent and Trademark office : USPTO) ได้ใช้เวลาพิจารณากว่า 1 ปี การยื่นขอจดทะเบียนดังกล่าวกลับได้รับการปฏิเสธ[16]

อย่างไรก็ตาม หากพิจารณาถึงการใช้งานของผู้ใช้บริการในปัจจุบัน ในบรรดาอุปกรณ์อิเล็กทรอนิกส์ที่สามารถเข้าถึงการใช้งานระบบการประมวลผลแบบคลาวด์ได้นั้น อุปกรณ์อิเล็กทรอนิกส์ที่ได้รับความนิยมในการเข้าใช้บริการระบบการประมวลผลแบบคลาวด์มากที่สุด ได้แก่ คอมพิวเตอร์โน้ตบุ๊ก (Notebook) และคอมพิวเตอร์เน็ตบุ๊ก (Netbook) ทั้งนี้ เนื่องจากอุปกรณ์ดังกล่าวสามารถพกพาได้ง่าย สามารถตอบสนองความต้องการในการใช้งานได้ดีที่สุด อีกทั้งยังสามารถป้องกันความปลอดภัยของข้อมูลได้เป็นอย่างดี ดังนั้น จึงได้รับความนิยมเป็นอย่างมากในปัจจุบัน

2. ศูนย์กลางข้อมูล (Data Center)

ศูนย์กลางข้อมูล หรือ Data center มีลักษณะเป็นห้องที่ถูกออกแบบมาเพื่อเป็นที่พักอาศัยและที่พักพิงของเซิร์ฟเวอร์ ซึ่งเซิร์ฟเวอร์ดังกล่าวก็จะเป็นที่จัดเก็บแอพพลิเคชั่นอีกทอดหนึ่ง หรือหากจะกล่าวเป็นทางการนั้น ศูนย์กลางข้อมูล คือ พื้นที่ที่ใช้จัดวางระบบประมวลผลกลางและระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่โดยมากผู้ใช้บริการหรือลูกค้าจะเชื่อมต่อมาใช้บริการผ่านระบบเครือข่ายที่มาจากภายนอก ดังนั้น ศูนย์กลางข้อมูลจึงเปรียบได้กับสมองของระบบสำหรับให้บริการ ซึ่งในการออกแบบศูนย์กลางข้อมูลนั้นจะต้องคำนึงถึงปัจจัยต่างๆ ได้แก่ ความมีเสถียรภาพ ความพร้อมใช้งาน การบำรุงรักษา ความเหมาะสมในการลงทุน ความปลอดภัย และการรองรับการขยายในอนาคต

สำหรับการให้บริการระบบการประมวลผลแบบคลาวด์นั้น ศูนย์กลางข้อมูลถือเป็นส่วนประกอบสำคัญที่ผู้ให้บริการจะต้องใช้เม็ดเงินในการลงทุนเป็นจำนวนมาก ทั้งนี้ เนื่องจาก

---

[16] Jim Manica, “Dell Trying to Trademark Cloud Computing,” สืบค้นเมื่อวันที่10 มกราคม 2560, จาก https://www.informationweek.com/mobile/dell-trying-to-trademark-cloud-computing/d/d-id/1070638?

ศูนย์กลางข้อมูลนั้นจะต้องควบคุมอุณหภูมิให้มีความเย็นและความชื้นในอากาศที่เหมาะสมตลอดเวลา ซึ่งค่าปกติที่เหมาะสมนั้นจะอยู่ที่อุณหภูมิ 25 องศาเซลเซียส หรืออุณหภูมิห้อง รวมถึงควบคุมระบบไฟฟ้าต่างๆ ให้พร้อมทำงานอยู่เสมอ ซึ่งผู้ใช้บริการรายย่อยอาจไม่มีเงินทุนเพียงพอในการลงทุนศูนย์กลางข้อมูลส่วนนี้

ในศูนย์กลางข้อมูลที่แห่งหนึ่งอาจจะเป็นที่จัดเก็บเซิร์ฟเวอร์ตั้งแต่ขนาดเล็กไปจนถึงเซิร์ฟเวอร์ขนาดใหญ่ ดังนั้น เมื่อใดที่ศูนย์กลางข้อมูลมีปัญหา การทำงานของเซิร์ฟเวอร์ก็จะมีปัญหาด้วยเช่นกัน ในทางปฏิบัติ ผู้ให้บริการจึงต้องจัดให้มีวิศวกรหรือผู้เชี่ยวชาญคอยดูแลและควบคุมอยู่เสมอ ซึ่งถือเป็นต้นทุนอีกประการหนึ่งในการให้บริการ ซึ่งการใช้งานระบบการประมวลผลแบบคลาดว์ของภาคเอกชนจะช่วยให้สามารถลดต้นทุนในการจ้างผู้เชี่ยวชาญเพื่อประจำการไปได้ส่วนหนึ่ง ดังนั้น ระบบการประมวลผลแบบคลาวด์จึงได้รับความสนใจเป็นอย่างมากในภาคธุรกิจดังที่ได้กล่าวไว้แล้ว

คุณสมบัติของศูนย์กลางข้อมูลที่ดีนั้นจะต้องมีการเชื่อมต่อเครือข่ายความเร็วสูงเพื่อเชื่อมต่อเซิร์ฟเวอร์กับศูนย์กลางข้อมูลเข้าด้วยกันและจะต้องมีความปลอดภัยในการจัดเก็บเซิร์ฟเวอร์อย่างสูงสุด เพราะข้อมูลที่ถูกจัดเก็บบนระบบการประมวลผลแบบคลาวด์นั้น มีข้อมูลจำนวนมากที่เป็นข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับทางการค้าซึ่งมีมูลค่ามหาศาล ดังนั้น ศูนย์กลางข้อมูลของผู้ให้บริการหลายแห่งจึงวางมาตรการรักษาความปลอดภัยอย่างแน่นหนา ไม่ว่าจะใช้ระบบสแกนลายนิ้วมือ จนถึงสแกนรูม่านตาในการเข้าถึงศูนย์กลางข้อมูล เป็นต้น

3. การกระจายเซิร์ฟเวอร์

ในระบบการทำงานของระบบการประมวลผลแบบคลาวด์นั้น เซิร์ฟเวอร์ทั้งหมดไม่จำเป็นต้องถูกจัดเก็บไว้ในศูนย์กลางข้อมูล (Data center) เดียวกัน ดังนั้น ผู้ให้บริการรายหนึ่งอาจมีเซิร์ฟเวอร์กระจายตัวอยู่ในศูนย์กลางข้อมูลในสถานที่ต่างๆ ทั่วโลก ดังเช่นในกรณีของ Amazon ทั้งนี้เนื่องจากเซิร์ฟเวอร์นั้นเป็นสถานที่ในการจัดเก็บแอพพลิเคชั่นสำหรับการใช้งาน ดังนั้น หากเซิร์ฟเวอร์ใดมีปัญหาหรือเกิดเหตุขัดข้องทางเทคนิค ผู้ใช้บริการก็ยังคงสามารถเรียกใช้งานแอพพลิเคชั่นได้อยู่โดยไม่ชะงักแต่อย่างใด เนื่องจากแอพพลิเคชั่นดังกล่าวจะถูกเรียกใช้งานจากเซิร์ฟเวอร์อื่นซึ่งอาจเป็นเซิร์ฟเวอร์สำรองของผู้ให้บริการก็ได้

ด้วยเหตุนี้ การกระจายเซิร์ฟเวอร์ย่อมก่อให้เกิดความคล่องตัวในการเรียกใช้งาน อีกทั้งยังช่วยป้องกันความปลอดภัยในการใช้งานระบบการประมวลผลแบบคลาวด์ด้วยเช่นกัน เพราะแอพพลิเคชั่น หรือข้อมูลของผู้ใช้บริการนั้นจะถูกกระจายจัดเก็บในเซิร์ฟเวอร์ต่างๆ ของผู้ให้บริการและผู้ให้บริการเองก็จะสามารถขยายขอบเขตการให้บริการได้โดยง่าย เนื่องจากมีเซิร์ฟเวอร์กระจาย

ตัวอยู่หลายที่และสามารถขยายเซิร์ฟเวอร์ในศูนย์กลางข้อมูลได้โดยง่ายแทนที่จะต้องหาศูนย์กลางข้อมูลสำหรับจัดเก็บเซิร์ฟเวอร์ใหม่ก็ใช้วิธีขยายศูนย์กลางข้อมูลเพื่อเพิ่มจำนวนเซิร์ฟเวอร์นั่นเอง

2.4 หลักการทำงานและรูปแบบของระบบการประมวลผลแบบคลาวด์

การทำงานของระบบการประมวลผลแบบคลาวด์แบ่งออกเป็นสองส่วนหลักๆ ได้แก่ ระบบการประมวลผล (Processing) และระบบการจัดเก็บข้อมูล (Storage) แต่ ไม่ว่าจะเป็นระบบการประมวลผล หรือระบบการจัดเก็บข้อมูล (Storage) ย่อมเกิดขึ้นได้เมื่อผู้ใช้บริการตกลงที่จะเข้าใช้บริการระบบการประมวลผลแบบคลาวด์จากผู้ให้บริการโดยการทำสัญญาบริการระบบการประมวลผลแบบคลาวด์ระหว่างกัน โดยก่อนการเข้าทำสัญญาบริการระบบการประมวลผลแบบคลาวด์นั้น ผู้ใช้บริการมีสิทธิเลือกจำนวนทรัพยากร กำลังการประมวลผลได้ตามความต้องการในการใช้งาน ซึ่งภายหลังจากการทำสัญญาดังกล่าวแล้วผู้ให้บริการจะเปิดโอกาสให้ผู้ใช้บริการสามารถใช้ซอฟต์แวร์ ระบบต่างๆ รวมทั้งทรัพยากรของเครื่องคอมพิวเตอร์ของผู้ให้บริการผ่านทางเครือข่ายอินเทอร์เน็ตได้ไม่ว่าผู้ใช้บริการจะอยู่ ณ ที่ใด เปรียบเสมือนว่าผู้ใช้บริการใช้หรือเช่าระบบคอมพิวเตอร์หรือทรัพยากรด้านคอมพิวเตอร์ของผู้ให้บริการเพื่อนำมาใช้ในการทำงานโดยที่ผู้ใช้บริการไม่จำเป็นต้องลงทุนสร้างระบบดังกล่าวด้วยตนเอง ทั้งนี้ ข้อมูลที่ผู้ใช้บริการป้อนหรือจัดเก็บเข้าสู่ระบบการประมวลผลแบบคลาวด์นั้น จะถูกจัดเก็บอย่างกระจัดกระจายและมีการทำซ้ำไปยังเซิร์ฟเวอร์ต่างๆ ที่อยู่ในดาต้าเซ็นเตอร์ของผู้ให้บริการ ทำให้ข้อมูลดังกล่าวไม่ได้อยู่รวมกลุ่มกันอยู่อย่างชัดเจน ณ ที่ใดที่หนึ่ง หลักการจัดเก็บข้อมูลเช่นนี้ก็เพื่อป้องกันการสูญหายของข้อมูล รวมทั้งทำให้สามารถเรียกใช้งานข้อมูลได้พร้อมๆ กันอย่างมีประสิทธิภาพตลอดเวลา ซึ่งนับว่าการจัดเก็บข้อมูลเช่นนี้เป็นจุดเด่นที่ทำให้ระบบการประมวลผลแบบคลาวด์แตกต่างจากเซิร์ฟเวอร์ทั่วไป หรือเซิร์ฟเวอร์แบบเดี่ยว (Standalone Server) และหากในภายหลังผู้ใช้บริการต้องการนำข้อมูลที่จัดเก็บอยู่ออกมาใช้งานอีกครั้ง ระบบก็จะส่งคำร้องขอของผู้ใช้บริการซึ่งอาจจะส่งมาจากที่ใดในโลกก็ได้ไปยังเครื่องเสมือนเพื่อแปลคำร้องขอของผู้ใช้บริการและดึงข้อมูลดังกล่าวออกมาให้แก่ผู้ใช้บริการ เครื่องคอมพิวเตอร์จริงหนึ่งเครื่องจะมีเครื่องเสมือนหลายๆ เครื่องที่ทำงานแยกจากกันอย่างเป็นอิสระ ดังนั้น การใช้บริการของผู้ใช้บริการในแต่ละครั้งจึงเกิดความรวดเร็วและแม่นยำ นอกจากนี้ เครื่องเสมือนจะทำการบันทึกประวัติการเรียกใช้งาน ประวัติการตอบสนองต่อคำร้องขอของผู้ใช้บริการเก็บไว้ เพื่อให้การใช้งานในครั้งถัดไปเกิดความรวดเร็วมากยิ่งขึ้นด้วย

ดังที่ได้กล่าวไว้แล้วข้างต้นว่าระบบการประมวลผลแบบคลาวด์นั้นจำเป็นต้องอาศัยอุปกรณ์อิเล็กทรอนิกส์ของผู้ใช้บริการ (Client Computer) ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล

(Personal Computer: PC) คอมพิวเตอร์พกพา (Notebook) แท็บเล็ต (Tablet) หรือโทรศัพท์มือถือประเภทสมาร์ทโฟน (Smart Phone) เพื่อเชื่อมต่อระบบอินเทอร์เน็ตในการเข้าถึงหรือเข้าใช้บริการระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการ ในขณะเดียวกันในฝั่งของผู้ให้บริการนั้น ผู้ให้บริการก็จำเป็นต้องเตรียมศูนย์กลางข้อมูล หรือ ดาต้าเซ็นเตอร์เพื่อจัดเก็บแอพพลิเคชั่นหรือเพื่อจัดวางระบบการประมวลผลกลาง และระบบเครือข่ายคอมพิวเตอร์เพื่อรองรับการเชื่อมต่อของผู้ใช้บริการจากภายนอกเช่นเดียวกัน อย่างไรก็ตาม ในบางกรณีผู้ให้บริการอาจจำเป็นต้องจัดเตรียมอุปกรณ์หรือระบบที่เพิ่มมากขึ้นเพื่อรองรับรูปแบบของการให้บริการระบบการประมวลผลแบบคลาวด์แต่ละประเภทซึ่งมีฟังก์ชั่นในการให้ผู้ใช้บริการเลือกใช้งานที่แตกต่างกันออกไป ซึ่งในปัจจุบันระบบการประมวลผลแบบคลาวด์มีรูปแบบการให้บริการทั้งสิ้น 4 ประเภทดังต่อไปนี้ โดยแต่ละประเภทล้วนตั้งอยู่บนหลักการเดียวกัน คือ ระบบการประมวลผลแบบคลาวด์จะต้องสามารถให้บริการได้กว้างไกลและไม่จำกัดจำนวนของผู้ใช้บริการภายใต้ระบบเดียวกัน ทั้งนี้ เพื่อลดอุปสรรคในการเข้าใช้งานของผู้ใช้บริการโดยการใช้บริการจะไม่จำกัดอยู่เพียงแค่การใช้งานผ่านทางคอมพิวเตอร์ส่วนบุคคลเท่านั้น

2.4.1 บริการประเภท Software as a Service (SaaS)

การให้บริการประเภท SaaS มีลักษณะเป็นการให้บริการที่นำเอาแอพพลิเคชั่นหรือซอฟต์แวร์บางส่วนของผู้ให้บริการออกให้บริการแก่ผู้ใช้บริการ โดยผู้ใช้บริการสามารถเข้าถึงบริการได้โดยอาศัยระบบอินเทอร์เน็ตของตน ในการใช้บริการประเภทนี้ผู้ให้บริการจะเป็นผู้รับผิดชอบในการดูแลและอัพเดตซอฟต์แวร์แทนผู้ใช้บริการ ดังนั้น ผู้ใช้บริการไม่จำเป็นต้องลงทุนในการจัดหาซอฟต์แวร์ด้วยตนเอง แต่ผู้ให้บริการจะทำหน้าที่จัดเตรียมซอฟต์แวร์เพิ่มเติมจากอุปกรณ์หรือระบบทั่วๆ ไปเพื่อรองรับการใช้งานของผู้ใช้บริการที่เลือกใช้บริการประเภท SaaS แทน ตัวอย่างเช่น บริษัทต้องการใช้โปรแกรมบริหารจัดการลูกค้า หรือ Customer Relationship Management (CRM) Software เพื่อที่จะใช้ในการตรวจสอบยอดขายและฐานข้อมูลลูกค้า[17] บริษัทย่อมไม่ต้องซื้อซอฟต์แวร์ดังกล่าวด้วยตนเอง แต่สามารถติดต่อผู้ให้บริการระบบการประมวลผลแบบคลาวด์รายใดก็ได้ที่ให้บริการซอฟต์แวร์ดังกล่าวอยู่แล้ว ซึ่งภายหลังเข้าทำสัญญาเข้าใช้บริการกับผู้ให้บริการระบบการประมวลผลแบบคลาวด์แล้ว บริษัทจะได้รับรหัสสำหรับการเข้าใช้งานซึ่งลูกจ้างของบริษัทสามารถเข้าใช้งานเพื่อสร้างฐานข้อมูลใหม่หรือเรียกดูฐานข้อมูลเดิมได้ไม่ว่าจะอยู่ภายในหรือภายนอกสำนักงานก็ตาม จะเห็นได้ว่าบริการประเภท SaaS มีคุณสมบัติที่โดดเด่น คือ

---

[17] อาณัติ รัตนถิรกุล, ก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ในองค์กร (ภาคปฏิบัติ), (กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น, 2558), น.38.

1. บริการประเภท SaaS สามารถเข้าใช้ผ่านเว็บบราวเซอร์ที่มีอยู่ในอุปกรณ์ประเภทต่างๆ ได้แก่ เครื่องคอมพิวเตอร์พีซี เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ เป็นต้น โดยไม่ต้องติดตั้งซอฟต์แวร์ที่เครื่องของผู้ใช้บริการ

2. ผู้ให้บริการจะเป็นผู้ควบคุมระบบโดยผู้ใช้บริการเพียงแค่ access เข้าสู่ระบบด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อระบุตัวตนของผู้ใช้บริการเท่านั้น

3. ผู้ใช้บริการสามารถปรับแต่งซอฟต์แวร์ตามลักษณะการใช้งานได้โดยสะดวกผ่านโปรแกรมที่เข้าใช้งาน

4. ผู้ใช้บริการสามารถเลือกที่จะจ่ายค่าตอบแทนหรือค่าบริการเมื่อใช้งานซอฟต์แวร์ของผู้ให้บริการตามปริมาณหรือตามจำนวนของซอฟต์แวร์ที่ตนประสงค์จะใช้งานแทนการซื้อเหมา ทั้งนี้ ผู้ให้บริการจะไม่เรียกเก็บค่าบริการช่วยเหลือ ค่าแก้ไขบั๊กของโปรแกรม หรือการอัพเดตต่างๆ แต่อย่างใด

จากคุณสมบัติดังกล่าวข้างต้น ทำให้การให้บริการซอฟต์แวร์แบบ SaaS แตกต่างจากการใช้บริการซอฟต์แวร์ในรูปแบบเก่าที่ผู้ใช้บริการจะต้องซื้อสิทธิในการเข้าใช้งาน (License) จากเจ้าของสิทธิ ดังนี้

ตารางที่ 1.1 เปรียบเทียบซอฟต์แวร์รูปแบบเก่าและซอฟต์แวร์ SaaS

ลักษณะ	ซอฟต์แวร์รูปแบบเก่า	ซอฟต์แวร์แบบ SaaS
ค่าใช้จ่ายในการลงทุน	ลงทุนสูงเนื่องจากต้องลงทุนในการซื้อฮาร์ดแวร์ ซอฟต์แวร์ รวมทั้งค่าใช้จ่ายในการดูแลรักษาระบบ	ลงทุนต่ำเนื่องจากไม่ต้องลงทุนซื้อฮาร์ดแวร์ ซอฟต์แวร์และค่าดูแลรักษาระบบ
ความเป็นเจ้าของซอฟต์แวร์	ผู้ซื้อจ่ายครั้งเดียวและมีสิทธิเป็นเจ้าของซอฟต์แวร์โดยถาวร	ผู้ซื้อเป็นแค่ผู้เช่าเพื่อใช้ซอฟต์แวร์ตามระยะเวลาที่จ่ายค่าบริการไปและไม่มีสิทธิเป็นเจ้าของซอฟต์แวร์โดยถาวร
ทรัพยากรบุคคลด้านไอที	ต้องการทีมงานไอทีที่มีความเชี่ยวชาญ	ต้องการแค่ผู้ประสานงานด้านไอทีซึ่งมีความรู้ด้านไอทีเพียงเล็กน้อยเพื่อติดต่อกับผู้ให้บริการ
ความรวดเร็วของการติดตั้งเพื่อเริ่มต้นการใช้งาน	ใช้ระยะเวลาการเตรียมการนาน	ใช้ระยะเวลาเตรียมการน้อยกว่า

ลักษณะ	ซอฟต์แวร์รูปแบบเก่า	ซอฟต์แวร์แบบ SaaS
ความน่าเชื่อถือและการการันตี	ขึ้นอยู่กับทีมไอทีและอุปกรณ์ฮาร์ดแวร์ขององค์กร	ขึ้นอยู่กับผู้ให้บริการ

จะเห็นได้ว่าข้อดีของการใช้บริการประเภท SaaS นั้นจะช่วยให้ผู้ใช้บริการสามารถลดต้นทุนของตนเองทั้งในการซื้อซอฟต์แวร์และการจ้างงานผู้เชี่ยวชาญด้านไอที นอกจากนี้การใช้บริการประเภทนี้ยังช่วยลดปัญหาการละเมิดลิขสิทธิ์ในทางอ้อมได้อีกด้วยเช่นกัน เนื่องจากผู้ใช้บริการย่อมหมดข้ออ้างในการละเมิดลิขสิทธิ์ซอฟต์แวร์อีกต่อไป

ในปัจจุบันแนวคิดการให้บริการประเภท SaaS ถูกนำไปใช้กับการเข้าใช้เว็บไซต์ทั้งในรูปแบบการให้บริการฟรีและแบบคิดค่าใช้จ่าย สำหรับตัวอย่างบริการฟรี อาทิเช่น Hotmail, gmail, Facebook, Twitter เป็นต้น สำหรับตัวอย่างบริการที่เป็นแบบคิดค่าใช้จ่าย ได้แก่ Netsuite, Salesforce, CRMonDemand เป็นต้น

2.4.2 บริการประเภท Infrastructure as a Service (laaS)

การให้บริการประเภท laaS มีลักษณะเป็นการให้บริการโครงสร้างพื้นฐานหลักของบริการระบบการประมวลผลแบบคลาวด์ไม่ว่าจะเป็นระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบเครือข่าย ตลอดจนอุปกรณ์พื้นฐานที่เกี่ยวข้อง ได้แก่ เซิร์ฟเวอร์จัดเก็บข้อมูล (Storage Server) หรือระบบปฏิบัติการ ซึ่งจะทำให้ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์แอพพลิเคชั่นได้อย่างมีประสิทธิภาพ โดยผู้ใช้บริการไม่จำเป็นต้องบริหารจัดการโครงสร้างพื้นฐานเอง[18]

ตัวอย่างของบริการโครงสร้างพื้นฐาน อาทิเช่น บริการ Compute Engine ของ Google บริการ Azure Virtual Machine ของ Microsoft และบริการ Cloud Service ของ CAT เป็นต้น

2.4.3 บริการประเภท Platform as a Service (PaaS)

การให้บริการประเภท PaaS มีลักษณะเป็นบริการที่มีระดับของความเป็นนามธรรมเพิ่มขึ้นจากการให้บริการประเภท laaS ภายใต้การให้บริการประเภท PaaS ผู้ให้บริการจะนำเสนอแพลตฟอร์มสำหรับการดำเนินงานระบบต่าง ๆ เพื่อให้ผู้ใช้บริการซึ่งก็คือผู้พัฒนาชุดคำสั่งงานสามารถเข้าถึงและใช้ประโยชน์แบบออนไลน์ได้ โดยผู้พัฒนาชุดคำสั่งงานสามารถเขียนชุดคำสั่งงานและอัพโหลดผลงานของตนไปไว้ในระบบการประมวลผลแบบคลาวด์ได้ ทั้งนี้ ผู้ใช้บริการสามารถจัด

---

[18] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, *อ้างแล้ว เชิงอรรถที่ 9*, น.7.

ขนาดทรัพยากรที่ต้องใช้ได้อย่างอัตโนมัติตามการเติบโตของการใช้ชุดคำสั่งงาน เช่น ขนาดของหน่วยจัดเก็บ รวมทั้งสามารถเลือกใช้บริการ PaaS ได้ทั้งเต็มรูปแบบและบางส่วน ทั้งนี้ ในปัจจุบัน ผู้ให้บริการ PaaS ได้แก่ Google Apps Engine Yard และ Force.Com เป็นต้น

2.4.4 บริการประเภท Data as a Service (DaaS)

การให้บริการประเภท DaaS เป็นการให้บริการจัดการข้อมูลที่รองรับการจัดเก็บข้อมูลขนาดใหญ่พร้อมระบบการสืบค้นและการจัดการข้อมูลขั้นสูง หรือ ที่มักเรียกกันโดยทั่วไปว่า “บริการ cloud storage” ซึ่งให้บริการฝากข้อมูลต่างๆ ไม่ว่าจะเป็นไฟล์เอกสาร ภาพ เสียง วีดิโอ และอื่นๆ เช่น บริการ Amazon S3 บริการ Google BigTable บริการ Apache หรือบริการ HBase เป็นต้น[19]

การให้บริการ DaaS โดยส่วนใหญ่นั้นจะเป็นการให้บริการแบบ freemium กล่าวคือ การให้บริการโดยไม่คิดค่าใช้จ่ายในส่วนของบริการพื้นฐาน แต่จะคิดค่าบริการสำหรับการให้บริการส่วนที่เพิ่มเติมจากบริการพื้นฐาน เช่น คิดค่าบริการเพิ่มเติมสำหรับการเพิ่มความจุข้อมูลของระบบจัดเก็บข้อมูล (Cloud storage) หรือค่าบริการสำหรับการดาวน์โหลดด้วยความเร็วที่สูงขึ้นจากบริการพื้นฐาน เป็นต้น

2.5 รูปแบบการเลือกใช้งานระบบการประมวลผลแบบคลาวด์ของผู้ใช้บริการ

เมื่อผู้ใช้บริการได้เลือกประเภทของบริการระบบการประมวลผลแบบคลาวด์แล้วไม่ว่าจะเป็นการให้บริการประเภท SaaS, IaaS, PaaS หรือ DaaS ในขั้นตอนต่อไปผู้ใช้บริการจะต้องเลือกรูปแบบการใช้งานระบบการประมวลผลแบบคลาวด์ ซึ่งในปัจจุบันมีรูปแบบการใช้งานทั้งสิ้น 4 รูปแบบ ดังนี้

2.5.1 Private Cloud หรือ Internal Cloud

Private Cloud หรือที่มักเรียกอีกชื่อหนึ่งว่า Internal Cloud นั้น มีลักษณะเป็นระบบการประมวลผลแบบคลาวด์ที่ใช้สำหรับหน่วยงานใดหน่วยงานหนึ่ง หรือองค์กรใดองค์กรหนึ่งเพียงองค์กรเดียวเท่านั้น แต่ภายในหน่วยงานหรือองค์กรนั้นอาจมีผู้ใช้งานหลายรายโดยไม่จำกัดจำนวนได้ ทั้งนี้ สาเหตุที่ระบบการประมวลผลในลักษณะนี้สามารถใช้งานได้เพียงหน่วยงานหรือองค์กรเดียว ก็เนื่องจากระบบการประมวลผลแบบคลาวด์ชนิดนี้ถูกพัฒนาขึ้นบนแนวคิดในการรักษา

[19] Santosh Kumar and R.H. Goudar, *supra note 4*, p.357.

สิทธิประโยชน์ของหน่วยงานหรือองค์กรเพื่อเป็นศูนย์กลางของการรักษาความปลอดภัยของข้อมูลในองค์กรที่ไม่ต้องการให้เผยแพร่สู่สาธารณะ ดังนั้น Private Cloud จึงตอบโจทย์ในการแก้ปัญหาความมั่นคงและความน่าเชื่อถือในการใช้งานระบบได้เป็นอย่างดี[20]

อย่างไรก็ตาม เพื่อให้การใช้งานระบบการประมวลผลแบบคลาวด์เกิดความมั่นคงปลอดภัยอย่างสูงสุด การบริหารจัดการระบบของ Private Cloud นั้นโดยส่วนใหญ่จึงต้องกระทำโดยบุคลากรภายในองค์กรเป็นหลัก

2.5.2 Community Cloud

Community Cloud มีลักษณะเป็นระบบการประมวลผลแบบคลาวด์ที่ดำเนินการร่วมกันโดยกลุ่มคนจากองค์กรต่างๆ[21] ซึ่งมีการรวมตัวกันในรูปแบบของการจัดตั้งเป็นสมาคม ชมรม หรือสหภาพ ไม่ว่าจะเป็นทางการหรือไม่เป็นทางการก็ตาม โดยมีวัตถุประสงค์จุดมุ่งหมายและความต้องการใช้บริการแบบเดียวกัน เช่น กลุ่มธุรกิจ สถาบันการศึกษา หรือหน่วยงานภาครัฐ เป็นต้น

2.5.3 Public Cloud หรือ External Cloud

Public Cloud หรือที่เรียกอีกชื่อหนึ่งว่า External Cloud[22] มีลักษณะเป็นระบบการประมวลผลแบบคลาวด์ที่เปิดให้สาธารณชนและหน่วยงานต่างๆเข้าใช้งานได้เป็นการทั่วไป โดยการบริหารจัดการหรือผู้ให้บริการอาจมีลักษณะเป็นบริษัท สถาบันการศึกษา หรือหน่วยงานภาครัฐก็ได้

ระบบการประมวลผลแบบคลาวด์ชนิดนี้นับเป็นระบบที่สอดคล้องตามหลักการของระบบการประมวลผลแบบคลาวด์ที่จัดให้มีการแบ่งปันการใช้ทรัพยากรในการประมวลผล โครงสร้างพื้นฐานในการประมวลผล ศูนย์ข้อมูล คำสั่งงานประยุกต์ด้วยวิธีการของเทคโนโลยีเสมือน

---

[20] Mohsin Nazir, “Cloud Computing: Overview & Current Research Challenges,” IOSR Journal of Computer Engineering, 14, Volume 8, Issue 1, p.15, (Nov. – Dec. 2012)

[21] Anna Kaushik and Ashok Kumar, “Application of Cloud Computing in Libraries,” International Journal of Information Dissemination and Technology 270, Vol.3, Issue 4, p.271-272 (October-December 2013).

[22] Winnie Chang, A Practical Guide To Singapore Data Protection Law, (Singapore, C.O.S. Printers Pte Ltd, 2013), p.319.

ขั้นสูง (Virtualization Technology) โดยที่ผู้ใช้บริการสามารถใช้บริการได้ด้วยตนเองและจ่ายค่าใช้บริการตามปริมาณการใช้งานที่เกิดจริง[23] ฉะนั้น ระบบการประมวลผลแบบคลาวด์ชนิด Public Cloud หรือ External Cloud จึงเป็นระบบที่มีความยืดหยุ่นและต้นทุนต่ำที่สุดในบรรดาระบบการประมวลผลแบบคลาวด์ชนิดอื่นๆ[24]

2.5.4 Hybrid Cloud

Hybrid Cloud เป็นระบบการประมวลผลแบบคลาวด์ที่มีลักษณะผสมผสานรูปแบบการบริการตั้งแต่ 2 แบบขึ้นไป[25] โดยเฉพาะอย่างยิ่ง Private และ Public Cloud[26] โดยทั่วไปแล้วการใช้งานระบบการประมวลผลแบบคลาวด์ชนิด Hybrid จะเป็นการใช้งานโดยเฉพาะกิจเท่านั้น ดังนั้น ในการใช้งานระบบการประมวลผลแบบคลาวด์ชนิดนี้ผู้ใช้งานจะต้องมีมาตรฐาน คุณสมบัติทางเทคนิคและเทคโนโลยีที่สามาถใช้งานข้อมูลและถ่ายโอนแอพพลิเคชั่น สำหรับการใช้งานข้ามไปมาระหว่างรูปแบบแต่ละแบบที่เลือกใช้งานได้

ทั้งนี้ ไม่ว่าผู้ใช้บริการเลือกใช้บริการรูปแบบใด ผู้ใช้บริการย่อมต้องรับภาระค่าบริการที่ตามมา ซึ่งโดยทั่วไปแล้วผู้ให้บริการจะคิดค่าบริการออกมาใน 2 รูปแบบด้วยกันขึ้นอยู่กับรูปแบบของบริการแต่ละประเภท ได้แก่

1. การคิดค่าบริการตามการใช้งานจริง (Pay-per-use) ซึ่งจะเป็นการคิดค่าบริการตามการใช้งานจริงเป็นรายชั่วโมง (Per hour) อาทิ ค่าบริการตามประเภทของ Machine สำหรับบริการ Compute Engine ของ Google หรือคิดค่าบริการตามปริมาณข้อมูลที่ใช้งานจริง Per Gigabyte หรือ Per terabyte เช่น ค่าบริการ IRIS Backup ของ CAT ค่าบริการเครือขาย (Network) และบริการ Load Balancing สำหรับบริการ Compute Engine ของ Google และ

---

[23] ศรีสมรัก อินทุจันทร์ยง, “การประมวลผลในกลุ่มเมฆ (Cloud Computing),” วารสารบริหารธุรกิจ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์, ปีที่ 33, ฉบับที่ 128,น.18 , (ตุลาคม-ธันวาคม 2553)

[24] วิวัฒน์ มีสุวรรณ์, “ระบบประมวลผลแบบกลุ่มเมฆในงานทางการศึกษา (Cloud Computing for Education),” วารสารศึกษาศาสตร์ มหาวิทยาลัยนเรศวร, ปีที่ 16, ฉบับที่ 1, น. 151, (มกราคม - มีนาคม 2557)

[25] Winnie Chang, *supra note 22*, p.319.

[26] R. Arokia Paul Rajan and S.Shanmugapriyaa, “Evolution of Cloud Storage as Cloud Computing Infrastructure Service,” IOSR Journal of Computer Engineering 38, Volume 1, Issue 1, p.39, (May-June 2012).

2. การคิดค่าบริการแบบเหมาจ่าย (Lump sum payment) ซึ่งจะเป็นการคิดค่าบริการแบบเหมาจ่ายเป็นรายวัน รายสัปดาห์ รายเดือน หรือรายปี โดยไม่สนใจว่าแท้จริงแล้วผู้รับบริการจะได้ใช้งานไปกี่ชั่วโมง หรือใช้งานไปปริมาณเท่าไร การใช้บริการประเภทนี้จึงเหมาะสำหรับผู้รับบริการที่ต้องมีการใช้บริการประมวลผลแบบคลาวด์ต่อเนื่องกันเป็นระยะเวลานานและใช้งานในปริมาณข้อมูลที่ค่อนข้างมาก ตัวอย่างของบริการประมวลผลแบบคลาวด์ ที่มีการคิดค่าบริการแบบเหมาจ่าย อาทิกรณีค่าบริการ Azure Cloud Services ของ Microsoft และบริการ Cloud SQL ของ Google เป็นต้น[27]

อย่างไรก็ตาม นอกจากการเรียกเก็บค่าบริการทั้งสองรูปแบบข้างต้นแล้ว ผู้ให้บริการบางรายอาจเรียกเก็บค่าบริการอื่นๆ จากผู้ใช้บริการเพิ่มเติม อาทิ ค่าสิทธิการใช้ซอฟต์แวร์ (Software license fee) ซึ่ง CAT จะเรียกเก็บค่าสิทธิการใช้ซอฟต์แวร์เป็นรายปีเพิ่มเติมจากค่าบริการระบบประมวลผลแบบคลาวด์ปกติ เป็นต้น

2.6 ความปลอดภัยในการใช้งานระบบการประมวลผลแบบคลาวด์

ในการให้บริการระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการในปัจจุบันนั้น ผู้ให้บริการจะเก็บรักษาข้อมูลของผู้ใช้บริการไว้ที่เซิร์ฟเวอร์จำนวนหลายเซิร์ฟเวอร์ด้วยกัน ซึ่งเซิร์ฟเวอร์ดังกล่าวจะถูกจัดเก็บไว้ในดาต้าเซ็นเตอร์อีกทอดหนึ่ง ทั้งนี้ ดาต้าเซ็นเตอร์ของผู้ให้บริการอาจตั้งอยู่ในประเทศใดประเทศหนึ่งหรือหลายประเทศก็ได้ แต่โดยส่วนใหญ่เพื่อป้องกันข้อมูลสูญหายหรือเพื่อป้องกันการเกิดปัญหาทางเทคนิค ผู้ให้บริการมักจะเก็บข้อมูลของผู้ใช้บริการโดยใช้วิธีการกระจายเก็บไว้ในดาต้าเซ็นเตอร์มากกว่าหนึ่งประเทศเสมอ ด้วยเหตุนี้ ผู้ใช้บริการจำนวนมากจึงยังเป็นกังวลว่าข้อมูลของตนจะถูกเก็บรักษาไว้ได้อย่างปลอดภัยหรือไม่ เนื่องจากข้อมูลดังกล่าวจะต้องถูกโอนไปจัดเก็บยังต่างประเทศ จะเห็นได้ว่าความปลอดภัยของการใช้งานระบบการประมวลผลแบบคลาวด์นับเป็นปัจจัยสำคัญที่ผู้ใช้บริการจะคำนึงประกอบการตัดสินใจเข้าใช้งานระบบการประมวลผลแบบคลาวด์เสมอ

ในเบื้องต้นผู้ใช้บริการสามารถพิจารณาว่าระบบการประมวลผลแบบคลาวด์ที่ตนใช้บริการอยู่นั้นมีความปลอดภัยเพียงพอหรือไม่ได้โดยสังเกตจากหลักเกณฑ์ ดังต่อไปนี้

---

[27] ชินดนัย สังคะคุณ, *อ้างแล้ว เชิงอรรถที่ 6*, น.27-28.

2.6.1 ความปลอดภัยของผู้ให้บริการ

ความปลอดภัยของผู้ให้บริการเป็นหลักเกณฑ์การพิจารณาว่าผู้ให้บริการรายดังกล่าวมีความน่าเชื่อถือหรือความน่าไว้วางในการให้บริการเพียงพอหรือไม่โดยพิจารณาจากมาตรฐานขององค์การระดับโลก ทั้งนี้ มาตรฐานดังกล่าวเกิดขึ้นเนื่องจากความไม่ไว้วางใจของผู้ใช้บริการในความปลอดภัยของการใช้บริการระบบการประมวลผลแบบคลาวด์ ดังนั้น เพื่อสร้างความไว้วางใจให้แก่ผู้ที่ประสงค์จะเปลี่ยนมาใช้บริการระบบการประมวลผลแบบคลาวด์แต่ยังขาดความมั่นใจ จึงเกิดหน่วยงานซึ่งทำหน้าที่ในการทำวิจัยและเผยแพร่ความรู้ในประเด็นด้านความมั่นคงปลอดภัยของระบบการประมวลผลแบบคลาวด์ขึ้นหลายหน่วยงานไม่ว่าจะเป็น EuroCloud Star Audit (ECSA), Cloud Security Alliance (CSA), International Organization for Standardization (ISO) เป็นต้น และเพื่อสร้างความไว้วางใจให้แก่ผู้ใช้บริการ หน่วยงานเหล่านี้จะทำหน้าที่สร้างมาตรฐานสำหรับตรวจสอบผู้ให้บริการระบบการประมวลผลแบบคลาวด์ขึ้นมาเพื่อให้ผู้ใช้บริการใช้เป็นแนวทางในการบริหารจัดการความปลอดภัยและเป็นเครื่องหมายยืนยันให้ผู้ใช้บริการเกิดความมั่นใจและไว้วางใจในการใช้บริการระบบการประมวลผลแบบคลาวด์ ทั้งนี้ แต่ละหน่วยงานต่างกำหนดมาตรฐานที่มีจุดเด่นแตกต่างกันไปออกไป ดังนั้น ก่อนการใช้บริการแต่ละครั้งผู้ใช้บริการย่อมจะต้องพิจารณาว่าผู้ให้บริการที่ตนประสงค์จะใช้บริการนั้นสามารถดำเนินการด้านความปลอดภัยได้ตามมาตรฐานดังกล่าวหรือไม่ หากผู้ให้บริการสามารถดำเนินการได้ ระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการรายนั้นย่อมมีความน่าเชื่อถือและน่าไว้วางใจสำหรับการใช้บริการ

ทั้งนี้ มาตรฐานความปลอดภัยที่สามารถนำมาเป็นแนวทางในการเลือกผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในปัจจุบันมีทั้งสิ้น 3 ประเภท โดยพิจารณาจากหน่วยงานซึ่งเป็นผู้จัดทำมาตรฐานดังกล่าว ดังนี้[28]

1. มาตรฐานที่ออกโดย ECSA (Euro Cloud Star Audit)

Euro Cloud Star Audit หรือ “ECSA” เป็นองค์กรหรือหน่วยงานที่ก่อตั้งขึ้นโดยกลุ่มประเทศในยุโรป หน่วยงาน ECSA จะสร้างมาตรฐานที่ตรวจสอบผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในทุกๆ ด้านไม่ว่าจะเป็นรายละเอียดของผู้ให้บริการ ข้อมูลทางการเงิน การดำเนินงานโครงสร้างพื้นฐาน ดาต้าเซ็นเตอร์ กระบวนการปฏิบัติงานในการให้บริการระบบการประมวลผลแบบคลาวด์ ข้อตกลงการให้บริการ (Service Level Agreement: SLA) การรักษาความ

[28] ACinfotec, “การให้บริการของ Cloud Provider มั่นใจได้จริงหรือ?,” สืบค้นเมื่อวันที่ 26 สิงหาคม 2559, จาก http://www.acinfotec.com/2015/12/03/cloud-provider/

ปลอดภัย ความเป็นส่วนตัวของข้อมูล สัญญาและกฎหมายที่เกี่ยวข้องตลอดจนการตรวจสอบแอพพลิเคชั่น มาตรฐานที่ออกโดย ECSA สามารถแบ่งออกเป็นระดับโดยใช้ชื่อเรียกว่า “Star Level” ทั้งนี้ ในปัจจุบันมาตรฐานของ ECSA จะให้การรับรองโดยแบ่งออกเป็น 3 ระดับ คือ

ระดับที่ 1: ECSA 3-Star: Practice for Readiness ซึ่งผู้ให้บริการที่จะได้รับมาตรฐานประเภทนี้นั้น จะต้องเป็นผู้ให้บริการที่มีความพร้อมในด้านการรักษาความปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล การปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง รวมทั้งจะต้องมีการจัดทำนโยบายและกระบวนการในการให้บริการลูกค้า และต้องมีการรับประกันการให้บริการ ทั้งนี้ ความพร้อมดังกล่าวจะต้องสามารถตรวจสอบได้ด้วย

ระดับที่ 2: ECSA 4-Star: Maturity of ITSM ซึ่งเป็นมาตรฐานของผู้ให้บริการในระดับบูรณาการของกระบวนการบริหารจัดการงานบริการเทคโนโลยีสารสนเทศ ดังนั้น ผู้ให้บริการที่จะได้รับมาตรฐานนี้จะต้องมีระบบบริหารจัดการความปลอดภัยและการจัดการข้อมูลตาม ISO 27001 ระบบการสำรองข้อมูล (Backup) ระบบการบริหารจัดการบริการที่มีคุณภาพ รวมทั้งระบบการควบคุมการเข้าถึงข้อมูล (Access Management) และกลไกในการเข้ารหัส

ระดับที่ 3: ECSA 5-Star: Resilience & Continuity ซึ่งเป็นมาตรฐานในระดับที่คำนึงถึงการมีความยืดหยุ่นและต่อเนื่องของการให้บริการเทคโนโลยีสารสนเทศเป็นสำคัญ ดังนั้น ผู้ให้บริการที่จะได้รับมาตรฐานนี้จะต้องมีระบบบริหารความต่อเนื่องทางธุรกิจพร้อมจัดทำการทดสอบแผน (Business Continuity Management System) มีดาต้าเซ็นเตอร์อย่างน้อย 2 แห่ง (Advanced DC Redundancy) มีระบบการให้บริการเทคโนโลยีสารสนเทศที่มีเสถียรภาพสูง(High Availability >99.9%) และมีการจัดทำระบบตรวจสอบ (Penetration Testing) รวมทั้งต้องมีความยืดหยุ่นในการให้บริการและมีรูปแบบในการจัดการด้านราคาการให้บริการที่เหมาะสมด้วยเช่นกัน

ทั้งนี้ ในการขอรับมาตรฐานประเภทนี้นั้น หากผู้ให้บริการรายใดได้รับการรับรองมาตรฐานจาก International Organization for Standardization (ISO) ไม่ว่าจะเป็น ISO 20000, ISO 27001 และ ISO 22301 ย่อมเพิ่มความได้เปรียบในการขอการรับรองจาก ECSA

2. มาตรฐานที่ออกโดย CSA-STAR (Cloud Security Alliance – Security, Trust & Assurance Registry)

มาตรฐานที่ออกโดย CSA-STAR เป็นมาตรฐานความปลอดภัยบนระบบการประมวลผลแบบคลาวด์ซึ่งเป็นส่วนเสริมเพิ่มเติมมาจากมาตรฐานความปลอดภัยของ ISO 27001 ทั้งนี้ มาตรฐาน CSA-STAR จะมุ่งเน้นไปที่ความปลอดภัยของการให้บริการระบบการประมวลผลแบบคลาวด์เป็นหลัก และส่วนของการปฏิบัติตาม กฎหมายข้อบังคับที่เกี่ยวข้อง หรือในส่วนของการรักษา

ความเป็นส่วนตัวของข้อมูลเป็นเพียงส่วนประกอบ อย่างไรก็ตาม ในการขอการรับรอง CSA-STAR นั้น ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะต้องได้รับการรับรอง ISO 27001 และใช้ Cloud Control Matrix (CCM) เพิ่มเติมด้วย ในปัจจุบันการให้การรับรอง CSA-STAR แบ่งออกเป็น 3 ระดับ ดังนี้

ระดับที่ 1: STAR Self-Assessment เป็นการให้การรับรองว่าผู้ให้บริการผ่านการเปิดเผยผลลัพธ์การประเมินด้วยตนเองจากแบบสอบถาม CSA Consensus Assessment Initiative Questionnaire (CAIQ) และ / หรือ Cloud Control Matrix (CCM)

ระดับที่ 2: STAR Certification เป็นการให้การรับรองว่าผู้ให้บริการผ่านการตรวจสอบและประเมินโดยผู้ตรวจสอบภายนอก (3rd Party) โดยใช้ Cloud Control Matrix (CCM) และ ISO 27001

ระดับที่ 3: STAR Continuous เป็นการให้การรับรองว่าผู้ให้บริการผ่านการตรวจสอบและประเมินความปลอดภัยบนระบบการประมวลผลแบบคลาวด์ของตนอย่างต่อเนื่อง โดยใช้ Cloud Trust Protocol (CTP) อย่างไรก็ตามในปัจจุบัน CTP ยังคงอยู่ในขั้นตอนการพัฒนา

3. มาตรฐานที่ออกโดย International Organization for Standardization หรือ ISO

International Organization for Standardization (ISO) ได้กำหนดมาตรฐานเพื่อเป็นแนวทางปฏิบัติ (Code of Practice) โดยเรียกชื่อว่า “มาตรฐาน ISO 27001” ทั้งนี้ มาตรฐานดังกล่าวเป็นมาตรฐานที่เกี่ยวกับการให้บริการระบบการประมวลผลแบบคลาวด์โดยเฉพาะ และจะแตกย่อยออกเป็นมาตรฐานต่างๆ ซึ่งจะเน้นในเรื่องแนวปฏิบัติที่แตกต่างกันดังนี้

ISO27017: Cloud Security เป็นมาตรฐานที่เน้นในเรื่องของการจัดการความปลอดภัยของการให้บริการระบบการประมวลผลแบบคลาวด์ ซึ่งเป็นส่วนเสริมเพิ่มเติมจาก ISO 27002 โดยได้เพิ่มเติม Cloud Computing Service Set เพื่อสร้างและรักษาความสัมพันธ์ในการทำงานร่วมกันระหว่างผู้ใช้บริการและผู้ให้บริการในเรื่องการจัดการความปลอดภัยข้อมูลของผู้ใช้บริการ โดยเน้นให้มีการควบคุมการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้บริการระบบการประมวลผลแบบคลาวด์ใน Virtual Environment ที่ใช้ร่วมกัน โดยผู้ใช้บริการต้องได้รับความคุ้มครองและแบ่งแยกอย่างชัดเจนจากผู้ใช้บริการรายอื่นๆ และจากผู้ซึ่งไม่ได้รับอนุญาตให้เข้าถึงข้อมูลดังกล่าวด้วย นอกจากนี้ผู้ให้บริการจะต้องจัดให้มีระบบ Operation Logs และ Logs ซึ่งเกี่ยวข้องกับการเข้าสู่ระบบการประมวลผลแบบคลาวด์ โดยต้องมีระบบการจัดการดังกล่าวที่ถูกต้องเหมาะสม สามารถเรียกดูได้และเก็บรักษาไว้อย่างถูกต้องปลอดภัย สำหรับในด้านของความเสี่ยงที่เกี่ยวข้องกับการรักษา

ความปลอดภัยข้อมูลบนระบบการประมวลผลแบบคลาวด์นั้น ผู้ให้บริการจะต้องจัดให้มีระบบจัดการ Information Security Incident และตอบสนองต่อผู้ใช้บริการอย่างเหมาะสม รวมทั้งต้องจัดให้มีข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับผู้ใช้บริการที่มักเรียกว่า ‘SLA’ ในเรื่องของการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลที่จัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ที่เหมาะสมด้วย

ISO 27018: Cloud Privacy เป็นมาตรฐานที่กำหนดแนวทางปฏิบัติสำหรับการปกป้องรักษาข้อมูลสำหรับการให้บริการระบบการประมวลผลแบบคลาวด์สาธารณะ (Public Cloud) โดยเฉพาะอย่างยิ่งเรื่องของการปกป้องข้อมูล (Data Protection) เป็นต้น

จากมาตรฐานความปลอดภัยต่างๆ ข้างต้น ผู้ใช้บริการซึ่งต้องการใช้บริการระบบการประมวลผลแบบคลาวด์จึงควรต้องพิจารณาถึงมาตรฐานต่างๆ ที่ผู้ให้บริการได้รับก่อนการเข้าใช้บริการเสมอ ทั้งนี้ เพื่อใช้ในการประกอบการตัดสินใจเนื่องจากหากผู้ให้บริการหยุดให้บริการแล้ว ผู้ใช้บริการอาจต้องเสี่ยงต่อการสูญเสียข้อมูลและแอพพลิเคชั่นเหล่านั้นไป อีกทั้งการพิจารณาเรื่องความปลอดภัยของการดูแลข้อมูล เรื่องของการรักษาข้อมูลส่วนบุคคล ก็ถือเป็นสิ่งสำคัญที่ควรพิจารณาเช่นกัน นอกจากนี้ ในฐานะผู้ให้บริการระบบการประมวลผลแบบคลาวด์ ผู้ให้บริการควรพิจารณาการได้การรับรองมาตรฐานต่างๆ ข้างต้น เพื่อสร้างความมั่นใจให้ผู้ใช้บริการ โดยเริ่มต้นเตรียมการ 2 ทางเลือกหลัก ดังนี้

ทางเลือกที่ 1 หากผู้ให้บริการต้องการได้รับการรับรองระบบการประมวลผลแบบคลาวด์แบบครบวงจร ผู้ให้บริการควรเริ่มจากการได้รับการรับรองมาตรฐาน ISO 27001 และมาตรฐาน ISO 20000 จากนั้นจึงเตรียมการและขอรับมาตรฐาน ISO 27017 และ มาตรฐาน ISO 27018 ต่อไปเพื่อขอการรับรองกับ ECSA

ทางเลือกที่ 2 หากผู้ให้บริการต้องการเน้นในด้านความปลอดภัยของระบบการประมวลผลแบบคลาวด์ ผู้ให้บริการควรเริ่มจากการได้รับการรับรองมาตรฐาน ISO 27001 ก่อนจากนั้นจึงจะเตรียมการเพื่อขอการรับรองจาก CSA-STAR ต่อไป

2.6.2 ความปลอดภัยของข้อมูลที่เก็บรักษาไว้ในระบบการประมวลผลแบบคลาวด์

ในการใช้งานระบบการประมวลผลแบบคลาวด์นั้น แม้ว่าผู้ใช้บริการจะได้เลือกสรรผู้ให้บริการที่มีความน่าเชื่อถือและมีความปลอดภัยตามมาตรฐานที่ออกโดยองค์กรหรือหน่วยงานต่างๆ ข้างต้นแล้ว แต่ในมุมมองของผู้ใช้บริการก็อาจจะยังคงขาดความมั่นใจในข้อมูลของตนที่บางครั้งอาจเป็นความลับทางการค้าที่จะต้องถูกเก็บรักษาเป็นอย่างดีหรืออาจเป็นข้อมูลส่วน

บุคคลที่ไม่อยากให้บุคคลอื่นทราบ ดังนั้น เพื่อรักษาความลับหรือข้อมูลของผู้ใช้บริการ ระบบการประมวลผลแบบคลาวด์จึงจำเป็นต้องมีกลไกควบคุมการเข้าถึง หรือที่เรียกว่า “Access Control” ที่จะทำงานร่วมกันกับกลไกในการพิสูจน์ตัวตนของผู้ที่เข้ามาใช้งานว่าเป็นผู้ที่ได้รับอนุญาตและมีสิทธิในการเข้าถึงส่วนใดบ้าง หรือที่เรียกว่า “Authentication” ซึ่งโดยทั่วไป การพิสูจน์ตัวตนจะอาศัยการเข้ารหัสข้อมูล (Cryptography) เพื่อปกป้องความลับของข้อมูลในระหว่างการส่งผ่านเครือข่ายอินเทอร์เน็ต หรือ การอาศัยการกรอกรหัสผ่าน ชุดคำถามลับ รหัสผ่านที่ใช้งานได้ครั้งเดียว (OTP/Token) หรือ อาศัยลายนิ้วมือ ดีเอ็นเอ หรือรูม่านตา เป็นต้น

นอกจากนี้ ภายใต้การใช้งานระบบการประมวลผลแบบคลาวด์ ผู้ที่ไม่ได้รับอนุญาตจะถูกป้องกันไม่ให้แก้ไขหรือเปลี่ยนแปลงข้อมูล ฉะนั้น ในการใช้งานเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถตรวจสอบการแก้ไขหรือสามารถเปลี่ยนแปลงข้อมูลได้ รวมทั้งหากเกิดปัญหาทางเทคนิคหรือถูกโจมตี ระบบการประมวลผลแบบคลาวด์จะมีกลไกป้องกันการหยุดให้บริการอย่างไม่ตั้งใจและมีแผนในการกู้คืนระบบโดยการกระจายงานไปยังระบบคอมพิวเตอร์หรือเซิร์ฟเวอร์อื่น เพื่อเตรียมความพร้อมหากมีการเรียกใช้งานในครั้งถัดไปเสมอ

แม้ว่าระบบการประมวลผลแบบคลาวด์จะมีกลไกในการป้องกันดังกล่าวข้างต้น แต่เพื่อสร้างความไว้วางใจให้แก่ผู้ใช้บริการอีกขั้นหนึ่งและเพื่อให้ระบบการประมวลผลแบบคลาวด์เป็นที่ยอมรับเพิ่มมากขึ้นในวงกว้าง ผู้ให้บริการจำนวนมากจึงหันมาสร้างเกราะป้องกันข้อมูลของผู้ใช้บริการโดยอาศัยซอฟต์แวร์ในการรักษาความปลอดภัย ซึ่งจะช่วยเพิ่มประสิทธิภาพของการให้บริการ โดยซอฟต์แวร์ที่ได้รับความนิยมในปัจจุบัน ได้แก่

1. Trend Micro มีลักษณะเป็นเทคโนโลยีป้องกันไวรัสแบบ Cloud Security ซึ่งสามารถให้บริการเกี่ยวกับ Anti-Virus, Anti-Spam Anti-Spyware, Web Threat Protection (ป้องกันภัยคุกคามทางเว็บไซต์), Parental Controls (โปรแกรมควบคุมสำหรับผู้ปกครอง) และ Data Theft Prevention (การป้องกันโจรกรรมข้อมูล) ซึ่งถือว่าเทคโนโลยีที่ป้องกันความปลอดภัยอย่างรอบด้าน

2. Symantec มีลักษณะเป็นระบบที่ได้มีการให้บริการทางด้านความปลอดภัยผ่านเทคโนโลยี Cloud Computing ในนาม Symantec.cloud ซึ่งครอบคลุมบริการรักษาความปลอดภัยอย่างรอบด้านเช่นเดียวกัน ไม่ว่าจะเป็นความปลอดภัยเกี่ยวกับ Anti-Virus, Anti-Spam, Email Continuity, Email Archiving, Web Security Service และ Content Control เป็นต้น Symantec ถือเป็นผู้ให้บริการการรักษาความปลอดภัยที่ยอมรับในวงกว้างในระดับโลก ดังนั้น Symantec.cloud จะช่วยทำให้ผู้ใช้บริการสามารถวางใจได้มากยิ่งขึ้นว่าข้อมูลที่สำคัญยิ่งขององค์กรจะได้รับการดูแลความปลอดภัยที่ดีและได้มาตรฐานระดับสากล

3. McAfee ซึ่งเป็นผู้ให้บริการด้านการป้องกันความปลอดภัยมาอย่างยาวนาน เมื่อระบบการประมวลผลแบบคลาวด์ได้รับความนิยม McAfee ได้เปิดตัว “McAfee Cloud Platform” เพื่อให้บริการเกี่ยวกับการรักษาความปลอดภัยทั้งอีเมล์ขาเข้า-ขาออก Web และ identity traffic โดยเป้าหมายคือการตรวจจับ traffic ทั้งหมดที่เกิดขึ้นระหว่างธุรกิจและระบบการประมวลผลแบบคลาวด์

4. Panda เมื่อระบบการประมวลผลแบบคลาวด์เริ่มได้รับความนิยม Panda ซึ่งเป็นผู้ให้บริการระบบ Antivirus เดิม จึงได้มีการอัพเดตบริการของตนเวอร์ชั่นล่าสุด ซึ่งเรียกชื่อว่า “Panda Cloud Antivirus 1.1.0 Final” ทั้งนี้ Panda Cloud Antivirus เป็นโปรแกรมสแกนไวรัสรูปแบบใหม่ในการกำจัด Virus, Spyware หรือ Malware โดยระบบใหม่นี้เปลี่ยนแนวคิดของโปรแกรมเดิม ๆ คือ การออกแบบให้โปรแกรมมีขนาดเล็ก เบา กินพื้นที่ และทรัพยากรเครื่องน้อย ในขณะเดียวกันได้ย้ายการทำงานหลักๆ ออกไปทำงานบนเซิร์ฟเวอร์ของระบบการประมวลผลแบบคลาวด์แทน ไม่ว่าจะเป็น Real-time protection, fully scanning และข้อมูลของไวรัสที่ออกมาใหม่ๆ เป็นต้น

2.7 ผู้ให้บริการระบบการประมวลผลแบบคลาวด์

ในปัจจุบันมีผู้ให้บริการระบบการประมวลผลแบบคลาวด์ซึ่งเป็นภาคเอกชนหลายรายที่ให้บริการระบบการประมวลผลแบบคลาวด์อยู่ในตลาดของเทคโนโลยี อาทิ Cisco, Fujitsu, Google, IBM, Intel, Microsoft และ Amazon เป็นต้น[29] ซึ่งผู้ให้บริการแต่ละรายต่างก็นำเสนอผลิตภัณฑ์ภายใต้ระบบการประมวลผลแบบคลาวด์ที่แตกต่างกันออกไป ดังนี้

1. Amazon ถือเป็นผู้ให้บริการรายแรก ๆ ที่ติดตาม พัฒนาและให้บริการระบบการประมวลผลแบบคลาวด์ โดยในปัจจุบัน Amazon ให้บริการผลิตภัณฑ์ที่เกี่ยวข้องกับระบบการประมวลผลแบบคลาวด์มากมาย เช่น Elastic Compute Cloud (Amazon EC2), Elastic Block Store (Amazon EBS), Simple Storage Service (Amazon S3), Simple Queue Service (Amazon SQS), Amazon SimpleDB, CloudFront เป็นต้น

---

[29] Timothy J. O’Leary, Linda I. O’Leary and Daniel A. O’Leary, คอมพิวเตอร์และเทคโนโลยีสารสนเทศสมัยใหม่ COMPUTING ESSENTIALS 2015, แปลโดย ศศลักษณ์ ทองขาว และคณะ, (กรุงเทพมหานคร: แมคกรอ-ฮิล อินเตอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2558): น.42.

2. Google ถือเป็นผู้ให้บริการรายใหญ่ในท้องตลาดซึ่งในปัจจุบัน Google มีบริการที่เกี่ยวเนื่องกับระบบการประมวลผลแบบคลาวด์มากมาย เช่น Gmail, Google Docs, Google analytics, Google Ad words and Ad Sense, Picasa[30] เป็นต้น

3. Microsoft ถือเป็นผู้ให้บริการรายใหญ่อีกรายที่สร้างจุดขายให้แก่ผลิตภัณฑ์ของตนเองโดยการนำมาตรฐานของ ISO/IEC 27018 ซึ่งเป็นมาตรฐานว่าด้วยความเป็นส่วนตัวในระบบการประมวลผลแบบคลาวด์ มาปฏิบัติตามเพื่อให้เกิดความเชื่อมั่นแก่ผู้ใช้บริการ[31] ดังนั้น Microsoft จึงเป็นผู้ให้บริการรายแรกที่ได้รับการยืนยันความปลอดภัยจากสถาบันมาตรฐานแห่งสหราชอาณาจักร (British Standards Insitute: BSI) ในปัจจุบัน Microsoft มีผลิตภัณฑ์ที่เกี่ยวเนื่องกับระบบการประมวลผลแบบคลาวด์มากมาย เช่น Windows Azure, Microsoft SQL Services, Microsoft Dynamics 365 เป็นต้น

4. IBM ถือเป็นผู้ให้บริการที่มีชื่อเสียงเป็นอย่างมากอีกรายหนึ่งในตลาดเทคโนโลยี อย่างไรก็ตาม IBM เพิ่งเปิดตัวระบบการประมวลผลแบบคลาวด์ของตนเองโดยใช้ชื่อเรียกว่า “IBM Bluemix” โดยเป็นการให้บริการระบบการประมวลผลแบบคลาวด์ประเภท PaaS

สำหรับประเทศไทยซึ่งระบบการประมวลผลแบบคลาวด์กำลังได้รับความนิยมเป็นอย่างมากนั้น จากการศึกษาพบว่าประเทศไทยมีผู้ให้บริการระบบการประมวลผลแบบคลาวด์จำนวนมากและมีแนวโน้มที่จะเพิ่มมากขึ้น อาทิ บริษัทคลาวด์คอมพิวติ้งโซลูชั่นส์ จำกัด บริษัท กสท โทรคมนาคม จำกัด (มหาชน) บริษัท ทีโอที จำกัด (มหาชน) บริษัทไซโยโฮสติ้ง จำกัด บริษัท ทรู ไอดีซี จำกัด บริษัทอินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) บริษัทดาต้าโปรบิวสิเนส จำกัด สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) บริษัทคลาวด์บิสซิเนส จำกัด (VPS) บริษัท ไวท์ สเปซ จำกัด บริษัท ไทยดาต้าโฮสติ้ง จำกัด บริษัท นครไฮเทค จำกัด บริษัท เคิร์ซ จำกัด (KIRZ) บริษัท บางกอก วีพีเอส จำกัด บริษัทเว็บเอ็คซเพิร์ท จำกัด (SiamInterHost) บริษัท อมิเพลย์ จำกัด และห้างหุ้นส่วนจำกัดดีเซิร์ฟเวอร์ บริษัท ออราเคิล คอร์ปอเรชั่น (ประเทศไทย) จำกัด บริษัท คลาวด์ เอช เอ็ม จำกัด บริษัท นิภา เทคโนโลยี จำกัด เป็นต้น อย่างไรก็ตาม ผู้ให้บริการที่ผู้ใช้บริการจะคุ้นเคยเป็นอย่างดีนั้น ได้แก่

---

[30] Ahmed E. Youssef, “Exploring Cloud Computing Services and Applications,” Journal of Emerging Trends in Computing and Information Sciences 838, Vol.3, No.6, p.841, (July 2012).

[31] Microsoft, “ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud,” สืบค้นเมื่อวันที่ 23 มิถุนายน 2560, จาก https://www.microsoft.com /en-us/TrustCenter/Compliance/iso-iec-27018

1. ทรู อินเทอร์เน็ต ดาต้า เซ็นเตอร์ หรือ ทรู ไอดีซี ซึ่งก่อตั้งขึ้นเมื่อเดือนเมษายน พ.ศ. 2547 โดยทรู ไอดีซีถือเป็นผู้นำในการให้บริการดาต้าเซ็นเตอร์และให้บริการระบบการประมวลผลแบบคลาวด์แบบครบวงจรรายแรกของประเทศไทยซึ่งได้รับรองมาตรฐานสากลหลายสาขา อาทิ ISO/IEC 20000-1 (Information Technology Service Management) ISO 22301 (Business Continuity Management) ISO/IEC 27001 (Information Security Management) ISO 50001 (Energy Management) และ CSA STAR (Cloud Security) เป็นต้น ในปัจจุบันทรู ไอดีซี ให้บริการทั้งดาต้าเซ็นเตอร์ซึ่งเป็นบริการรับฝากเครื่องเซิร์ฟเวอร์และอุปกรณ์ ICT ต่างๆ รวมทั้งบริการดูแลและจัดการระบบเครือข่าย ระบบรักษาความปลอดภัยของเครือข่ายด้วย หรือ บริการระบบการประมวลผลแบบคลาวด์ ประเภท IaaS และ PaaS เป็นต้น[32]

2. บริษัท กสท โทรคมนาคม จำกัด (มหาชน) หรือ CAT ปัจจุบัน CAT ให้บริการระบบการประมวลผลแบบคลาวด์ที่เรียกว่า “IRIS Cloud” ซึ่งมีลักษณะเป็นระบบการประมวลผลแบบคลาวด์ประเภท IaaS อาทิ บริการ Enterprise IaaS with MSS, Premium IaaS Bundle Windows เป็นต้น และให้บริการ IRIS Backup เสริมด้วย[33]

3. บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) หรือ INET บริการของ INET มีลักษณะเป็นบริการเชื่อมต่ออินเทอร์เน็ตสำหรับธุรกิจ (Full Internet Access for Business) บริการดาต้าเซ็นเตอร์ (Internet Data Center: IDC) บริการ IaaS, PaaS และ SaaS เป็นต้น INET ถือเป็นผู้ให้บริการอีกรายที่ได้รับการรับรองความปลอดภัยสำหรับบริการคลาวด์และดาต้าเซ็นเตอร์ตามมาตราฐาน ISO27001:2013 ด้วย[34]

4. บริษัท ทีโอที จำกัด (มหาชน) หรือ TOT บริการระบบการประมวลผลแบบคลาวด์ของ TOT มีชื่อเรียกว่า “CloudApps” ซึ่งมีลักษณะเป็นการให้บริการระบบการประมวลผลแบบคลาวด์ประเภท IaaS, PaaS และ SaaS และให้บริการดาซ้าเซ็นเตอร์ทั่วประเทศ[35]

---

[32] True IDC, “About us – True IDC,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก https://www.trueidc.com/about/th

[33] Cattelecom, “IRIS Platform Innovative Cloud Ecosystem by CAT,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก http://iris.cattelecom.com/en

[34] INET, “About INET,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก https://inet.co.th/ about/index.php?MainID=4

[35]TOT, “TOT Cloud,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก http://www.tot.co.th/SME/Content.aspx?id=E44917817805434BBEB8DB5D1D1F0F3D

5. บริษัท ออราเคิล คอร์ปอเรชั่น (ประเทศไทย) จำกัด หรือ Oracle บริการระบบการประมวลผลแบบคลาวด์ของ Oracle ครอบคลุมระบบการประมวลผลแบบคลาวด์ทุกประเภท ไม่ว่าจะเป็น Software as a Service (SaaS), Data as a Service (DaaS), Platform as a Service (PaaS) Infrastructure as a Service (IaaS) และ Cloud Marketplace สำหรับการขายสินค้าผ่านทางโลกออนไลน์[36]

2.8 ประเภทของข้อมูลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์

ในการใช้บริการระบบการประมวลผลแบบคลาวด์ ผู้ใช้บริการสามารถอัพโหลดข้อมูลประเภทใดๆ ก็ได้เข้าสู่ระบบการประมวลผลแบบคลาวด์ไม่ว่าจะเป็นไฟล์เอกสารที่ถูกจัดเก็บไว้ในไฟล์ Microsoft ต่างๆ รูปภาพ วิดิโอ ข้อมูลความลับทางการค้า ข้อมูลติดต่อลูกค้า เป็นต้น[37] อย่างไรก็ตาม หากจะจัดประเภทข้อมูลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์จะสามารถแบ่งได้เป็น 3 ประเภท ได้แก่ (1) ข้อมูลส่วนบุคคล (2) ข้อมูลความลับต่าง ๆ เช่น ข้อมูลความลับทางการค้า (Trade Secret Data) และ (3) ข้อมูลทั่วๆ ไปที่มีจำนวนมากบนระบบการประมวลผลแบบคลาวด์ ซึ่งโดยทั่วไปมักเรียกกันว่า “Big data”

อย่างไรก็ตาม ในการศึกษาครั้งนี้ผู้เขียนมุ่งศึกษาเฉพาะข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ เนื่องจากข้อมูลส่วนบุคคลถือเป็นข้อมูลที่ควรได้รับความคุ้มครองเพราะเกี่ยวข้องกับตัวบุคคลโดยเฉพาะ ดังนั้น การศึกษาหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในส่วนถัดไปจะพิจารณาเฉพาะหลักเกณฑ์ที่มีขอบเขตในการใช้บังคับกับข้อมูลส่วนบุคคลเท่านั้น

2.9 การควบคุมการใช้บริการระบบการประมวลผลแบบคลาวด์ของสถาบันการเงินไทย

ในปัจจุบันมีสถาบันการเงินในประเทศไทยจำนวนมากที่หันมาใช้บริการระบบการประมวลผลแบบคลาวด์เพื่อทำการประมวลผลและเก็บข้อมูลของลูกค้าเพราะระบบการประมวลผล

---

[36]Oracle, “Oracle Cloud,” สืบค้นเมื่อวันที่ 21 ธันวาคม 2560, จาก https://cloud.oracle.com/th_TH/home

[37]Vijay Sharma, “What kind of data can be stored in cloud storage?,” สืบค้นเมื่อวันที่ 10 เมษายน 2561, จาก http://www.klientsolutech.com/what-kind-of-data-can-be-stored-in-cloud-storage/

แบบคลาวด์สามารถช่วยเพิ่มประสิทธิภาพในการให้บริการและช่วยในการบริหารต้นทุนของสถาบันการเงินได้เป็นอย่างดี อย่างไรก็ตาม เนื่องจากข้อมูลของลูกค้าที่ธนาคารจัดเก็บไว้นั้น มีทั้งข้อมูลที่เป็นข้อมูลส่วนบุคคลและข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคลซึ่งล้วนแต่เป็นข้อมูลที่ลูกค้าไม่อยากเปิดเผยให้บุคคลอื่นทราบ กรณีจึงเกิดคำถามว่าสถาบันการเงินสามารถใช้บริการระบบการประมวลผลแบบคลาวด์ได้หรือไม่ ซึ่งในประเด็นดังกล่าวธนาคารแห่งประเทศไทย (ธปท.) ซึ่งทำหน้าที่ควบคุม กำกับดูแลสถาบันการเงินได้เข้ามามีบทบาทต่อการใช้บริการระบบการประมวลผลแบบคลาวด์ของสถาบันการเงินเพื่อคงไว้ซึ่งความน่าเชื่อถือในการใช้บริการของลูกค้าและสถาบันการเงิน ซึ่งในปัจจุบันธปท. อนุญาตให้สถาบันการเงินสามารถใช้บริการระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการภายนอกได้ภายใต้เงื่อนไขที่ธปท. กำหนดไว้ในประกาศธนาคารแห่งประเทศไทยที่ สนส.19/2559 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน[38] ดังนี้

(1) ขอบเขตการใช้บริการระบบการประมวลผลแบบคลาวด์ตามประกาศฉบับนี้ หมายถึง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศที่มีการนำเทคโนโลยีระบบการประมวลผลแบบคลาวด์มาใช้ในการให้บริการผ่านเครือข่ายอินเตอร์เน็ต เพื่อประโยชน์ในการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใดๆ เกี่ยวกับข้อมูลหรือระบบงานให้แก่สถาบันการเงิน ซึ่งการใช้บริการดังกล่าวสามารถปรับเปลี่ยนได้ตามความต้องการของผู้ใช้บริการ

(2) เงื่อนไขการใช้บริการระบบการประมวลผลแบบคลาวด์ ได้แก่

- สถาบันการเงินต้องรับผิดชอบต่อการให้บริการอย่างต่อเนื่องแก่ผู้ใช้บริการของสถาบันการเงิน ต้องคงความน่าเชื่อถือของการให้บริการเช่นเดียวกับกรณีที่สถาบันการเงินเป็นผู้ดำเนินการด้านเทคโนโลยีสารสนเทศด้วยตนเองและต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสถาบันการเงินในรูปแบบที่เปลี่ยนแปลงไปจากการดำเนินงานปกติที่กระทำโดยสถาบันการเงินเอง ทั้งนี้ กรณีผู้ให้บริการ sub-contract การให้บริการนั้นต่อ สถาบันการเงินต้องมั่นใจว่าบุคคลที่ให้บริการต่อจะรับผิดชอบต่อสถาบันการเงินเสมือนกับผู้ให้บริการรายแรก

---

[38]ธนาคารแห่งประเทศไทย, “ประกาศธนาคารแห่งประเทศไทยที่ สนส. 19/2559 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน,” สืบค้นเมื่อวันที่ 15 เมษายน 2561, จาก https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2560/ThaiPDF/25600035.pdf

- สถาบันการเงินต้องมีแนวทางบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในเรื่องดังต่อไปนี้

  การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security): สถาบันการเงินต้องมั่นใจว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีมาตรฐานในการรักษาความปลอดภัยตามหลักสากล เช่น มีการเข้ารหัสข้อมูล (Data Encryption) การควบคุมกุญแจที่ใช้เข้าถึงและเข้ารหัสข้อมูลบนระบบการประมวลผลแบบคลาวด์ (key management) เป็นต้น

  ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Intergrity): สถาบันการเงินต้องมีการดำเนินการเพื่อให้มั่นใจว่า ผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูลที่ครอบคลุมตั้งแต่การพัฒนาหรือการเปลี่ยนแปลงแก้ไขระบบงาน การควบคุมทั้งในส่วนของการบันทึกข้อมูลเข้าสู่ระบบ (input validation) การประมวลผล (processing control) และการนำข้อมูลออกจากระบบ (output control) เป็นต้น

  ความพร้อมใช้งานของเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability): สถาบันการเงินต้องมีการดำเนินการเพื่อให้มั่นใจถึงความพร้อมในการใช้งานโดยพิจารณาจากมาตรฐานในการทำให้ระบบการประมวลผลแบบคลาวด์มีความพร้อมในการใช้งาน ตลอดจนสถาบันการเงินต้องจัดให้มีกระบวนการในการติดตาม ประเมินผลและตรวจสอบผู้ให้บริการ

  การคุ้มครองผู้ใช้บริการของสถาบันการเงิน (Consumer Protection): สถาบันการเงินต้องมีการดำเนินการเกี่ยวกับการคุ้มครองผู้ใช้บริการโดยต้องมั่นใจว่าผู้ให้บริการจะไม่นำข้อมูลผู้ใช้บริการไปเปิดเผยโดยไม่ได้รับความยินยอมจากสถาบันการเงิน ต้องมีขั้นตอนกระบวนการติดตาม ประเมินผลและตรวจสอบผู้ให้บริการ ตลอดจนมีระบบร้องเรียนให้แก่ผู้ใช้บริการอย่างเพียงพอและเหมาะสม

- สถาบันการเงินต้องมีการกำกับดูแลความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากผู้ให้บริการระบบการประมวลผลแบบคลาวด์อย่างเหมาะสม โดยต้องมีการประเมินตนเอง (Self-assessment) ควบคุมและจัดการความเสี่ยงอย่างมีประสิทธิภาพ ภายใต้การกำกับดูแลของคณะกรรมการของสถาบันการเงิน

(3) การขออนุญาตต่อธปท.

- กรณีใช้บริการระบบการประมวลผลแบบคลาวด์ ประเภท Private Cloud ที่ให้บริการโดยบริษัทในกลุ่มธุรกิจเดียวกัน สถาบันการเงินสามารถดำเนินการได้โดยไม่ต้องแจ้งหรือขออนุญาตต่อธปท.
- กรณีใช้บริการระบบการประมวลผลแบบคลาวด์ ประเภท Private Cloud ที่ให้บริการโดยบุคคลภายนอก สถาบันการเงินต้องแจ้งให้ธปท. ทราบล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนการเปลี่ยนแปลงการใช้บริการ
- กรณีใช้บริการระบบการประมวลผลแบบคลาวด์ ประเภท Public Cloud (ไม่ว่าให้บริการโดยบริษัทในกลุ่มธุรกิจเดียวกันหรือบุคคลภายนอก) สถาบันการเงินต้องขออนุญาตต่อธปท. ล่วงหน้าอย่างน้อย 30 วันก่อนเริ่มใช้บริการหรือก่อนเปลี่ยนแปลงการใช้บริการ

2.10 การให้บริการระบบการประมวลผลแบบคลาวด์ภาครัฐ (Government Cloud หรือ G-Cloud)

ระบบการประมวลผลแบบคลาวด์ภาครัฐ หรือ Government Cloud (G-Cloud) เป็นการให้บริการระบบการประมวลผลแบบคลาวด์แก่หน่วยงานภาครัฐ ซึ่งดำเนินการโดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (Electronic Government Agency: EGA) เพื่อรองรับความต้องการใช้บริการของหน่วยงานภาครัฐ โดยมีสาระสำคัญดังนี้

2.10.1 ความเป็นมาของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ EGA

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ EGA จัดตั้งขึ้นตามพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ซึ่งมีที่มาจากมติของคณะรัฐมนตรีเมื่อวันที่ 25 พฤศจิกายน 2553 ที่ต้องการพัฒนารัฐบาลอิเล็กทรอนิกส์ จึงมีมติให้จัดตั้ง EGA ขึ้นเพื่อดำเนินการขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ EGA เป็นองค์การมหาชนภายใต้การกำกับดูแลของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในปัจจุบัน[39]

[39] สำนักงานรัฐบาลอิเล็กทรอนิกส์, “ประวัติความเป็นมา,” สืบค้นมื่อวันที่ 15 เมษายน 2561, จาก https://www.ega.or.th/th/profile_history/

ภารกิจสำคัญของ EGA คือ การพัฒนาและการให้บริการระบบรัฐบาลอิเล็กทรอนิกส์ (e-Government) ยกระดับการบริหารงานของภาครัฐให้ก้าวสู่ความทันสมัยที่มาพร้อมกับความสะดวกและรวดเร็วควบคู่ไปกับการปรับบริการให้ประชาชนด้วยระบบอิเล็กทรอนิกส์ที่มีประสิทธิภาพ มั่นคง ปลอดภัย และทั่วถึง อีกทั้งยังพัฒนาให้เกิดการบูรณาการระหว่างหน่วยงานภาครัฐด้วยการเชื่อมโยงข้อมูลของทุกภาคส่วนเข้าด้วยกัน[40]

2.10.2 ที่มาและลักษณะของบริการระบบการประมวลผลแบบคลาวด์ภาครัฐ (Government Cloud: G-Cloud)

ที่มาของโครงการระบบการประมวลผลแบบคลาวด์ภาครัฐหรือ G-Cloud เกิดขึ้นจากการขอใช้งบประมาณในการจัดซื้อระบบสารสนเทศสำหรับภาครัฐเพิ่มขึ้นอย่างต่อเนื่อง ประกอบกับหน่วยงานภาครัฐส่วนใหญ่ยังขาดแคลนบุคลากรที่มีความรู้ความชำนาญในระบบเทคโนโลยีสารสนเทศและยังขาดความพร้อมในเรื่องของโครงสร้างพื้นฐานของระบบเทคโนโลยีสารสนเทศ เช่น Internet Data Center (IDC) ระบบสำรองไฟฟ้า ระบบเครือข่าย รวมถึงระบบรักษาความปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศ ทำให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในปัจจุบัน มอบหมายให้ EGA นำระบบการประมวลผลแบบคลาวด์เข้ามาใช้เพื่อให้บริการแก่หน่วยงานภาครัฐ เพราะ EGA มีความพร้อมทั้งทางด้านบุคลากรและโครงสร้างพื้นฐาน เช่น ระบบเครือข่าย เป็นต้น ทั้งนี้ การให้บริการระบบการประมวลผลแบบคลาวด์ของ EGA จะช่วยลดความซ้ำซ้อนในการจัดซื้ออุปกรณ์หรือระบบ ลดภาระในการบริหารจัดการและบำรุงรักษาอุปกรณ์หรือระบบของหน่วยงาน[41]

ในปัจจุบัน EGA ให้บริการระบบการประมวลผลแบบคลาวด์ครอบคลุมทุกกระทรวง กรม และส่วนราชการระดับภูมิภาค โดยในปี 2560 มีหน่วยงานภาครัฐใช้งานจำนวนทั้งหมด 386 หน่วยงาน ทั้งนี้ หน่วยงานที่ใช้บริการระบบการประมวลผลแบบคลาวด์ของ EGA มากที่สุด ได้แก่ กระทรวงสาธารณสุข และโครงการที่สำคัญของภาครัฐที่ใช้ระบบการประมวลผลแบบคลาวด์ ได้แก่ โครงการระบบภาษีและเอกสารธุรกรรมอิเล็กทรอนิกส์ โครงการ National e-Payment ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โครงการระบบการ

---

[40] สำนักงานรัฐบาลอิเล็กทรอนิกส์, “ประวัติความเป็นมา,” สืบค้นมื่อวันที่ 15 เมษายน 2561, จาก https://www.ega.or.th/th/profile_history/

[41] Thanakrit Lersmethasakul, “e-Government Cloud Computing,” สืบค้นเมื่อวันที่ 15 เมษายน 2561, จาก https://www.slideshare.net/lersmethasakul/e-government-cloud-service

ยื่นแจ้งผลิตภัณฑ์สุขภาพก่อนการนำเข้าของสำนักงานคณะกรรมการอาหารและยา (อย.) โครงการระบบโครงการดูแลสุขภาพตลอดช่วงชีวิต ตามความร่วมมือระหว่างกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ กระทรวงสาธารณสุข กระทรวงมหาดไทย กระทรวงแรงงาน และกระทรวงศึกษาธิการ โครงการระบบบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ ของกรมการปกครอง กระทรวงมหาดไทย และโครงการระบบสารสนเทศเพื่ออำนวยความสะดวกในการดำเนินธุรกิจของสำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) เป็นต้น[42]

2.10.3 บริการระบบการประมวลผลแบบคลาวด์ภาครัฐในต่างประเทศ

เช่นเดียวกับประเทศไทย รัฐบาลต่างประเทศหลายประเทศต่างหันมาใช้บริการระบบการประมวลผลแบบคลาวด์เพื่อประโยชน์ในการพัฒนาและการติดต่อสื่อสารในภาครัฐ อาทิ

(1) ประเทศอังกฤษ: รัฐบาลได้ริเริ่มโครงการ “The G-Cloud Framework” เพื่อรวมกระบวนการจัดซื้อจัดจ้างสินค้าและบริการต่างๆ ของหน่วยงานของรัฐไว้บนระบบการประมวลผลแบบคลาวด์ ซึ่งจะช่วยให้หน่วยงานของรัฐทุกภาคส่วนไม่ว่าจะเป็นหน่วยงานส่วนกลางหรือส่วนภูมิภาคเข้าใช้งานระบบดังกล่าวได้[43]

(2) ประเทศญี่ปุ่น: รัฐบาลได้ริเริ่มโครงการ “Kasumigaseki Cloud” เพื่อสร้างแพลตฟอร์มสำหรับให้หน่วยงานของรัฐใช้ร่วมกันตั้งแต่ปีค.ศ. 2009 และเพื่อรวบรวมระบบเทคโนโลยีสารสนเทศของรัฐให้เป็นหนึ่งเดียว ซึ่งจะช่วยลดต้นทุนและช่วยให้เกิดประสิทธิภาพในการใช้งานอีกทั้งยังช่วยให้การรับส่งเอกสารระหว่างหน่วยงานภาครัฐและหน่วยงานภาคเอกชนเกิดความคล่องตัวด้วยเช่นกัน[44]

---

[42] สำนักงานรัฐบาลอิเล็กทรอนิกส์, “G-Cloud อีจีเอ ตอบโจทย์หน่วยงานภาครัฐ เผย ก.สาธารณสุขแชมป์ใช้งานคลาวด์ พร้อมดันบริการใหม่ๆ เข้าระบบ,” สืบค้นมื่อวันที่ 15 เมษายน 2561, จาก https://www.ega.or.th/th/content/913/11935

[43] Chris Copland, “Betterworking appointed to UK Government G-Cloud procurement framework,” สืบค้นเมื่อวันที่ 15 เมษายน 2561, จาก http://www.betterworking.com/blog/betterworking-appointed-to-uk-government-g-cloud-procurement-framework/

[44]The U.S. Department of Commerce’s International Trade Administration, “Overview of Cloud Computing in Japan,” สืบค้นเมื่อวันที่ 15 เมษายน 2561, จาก https://www.export.gov/article?id=Overview-of-Cloud-Computing-in-Japan

(3) ประเทศเกาหลีใต้: ในปีค.ศ. 2014 รัฐบาลเกาหลีใต้ได้ร่วมมือกับบริษัทซอฟต์แวร์ท้องถิ่นในการพัฒนาระบบการประมวลผลแบบคลาวด์ประเภท PaaS และเรียกชื่อว่า “PaaS-TA” โดยมีเป้าหมายเพื่อให้หน่วยงานภาครัฐใช้บริการ ซึ่งความร่วมมือในการพัฒนาบริการ PaaS-TA ประสบความสำเร็จเมื่อเดือนเมษายน 2016 และเริ่มใช้งานได้เมื่อกุมภาพันธ์ 2017[45] เป็นต้นมา

[45] Alesia Bulanok and Alex Khizhniak, “The Government of South Korea Creates an Open PaaS with Cloud Foundry,” สืบค้นเมื่อวันที่ 16 เมษายน 2561, จาก https://www.altoros.com/blog/south-korea-adopts-cloud-foundry-as-its-paas/

บทที่ 3
การประเมินความพร้อมของกลุ่มพันธมิตรธุรกิจซอฟต์แวร์

3.1 ที่มาและความสำคัญของกลุ่มพันธมิตรธุรกิจซอฟต์แวร์

กลุ่มพันธมิตรธุรกิจซอฟต์แวร์หรือบีเอสเอ เป็นสมาคมเพื่อการค้าที่ไม่หวังผลกำไรซึ่งก่อตั้งขึ้นเมื่อปีพ.ศ. 2531 เพื่อยับยั้งการละเมิดลิขสิทธิ์ในซอฟต์แวร์และส่งเสริมโลกดิจิทัลโดยไม่ได้จำกัดอยู่เพียงซอฟต์แวร์แต่ยังรวมถึงนวัตกรรมและเทคโนโลยีต่างๆ ให้ปลอดภัยและถูกต้องตามกฎหมาย ตลอดจนส่งเสริมสภาวะการทำงานเชิงกฎหมายในระยะยาว ทั้งนี้ ปัจจุบันบีเอสเอเป็นสัญลักษณ์ตัวแทนกลุ่มผู้ผลิตซอฟต์แวร์ที่ใหญ่ที่สุดของโลก ได้แก่ Adobe, Microsoft, Apple, Intels, Dells, McAfee, Siemens PLM Software, Aveva, AVG Technologies, Bentley Systems, CA Technologies, CNC software/mastercam เป็นต้น และบีเอสเอยังเป็นสมาชิกหน่วยหนึ่งของกลุ่มพันธมิตรทรัพย์สินทางปัญญาสากล หรือ International Intellectual Property Alliance (IIPA) อีกด้วย

ปัจจุบันบีเอสเอมีสำนักงานใหญ่อยู่ในกรุงวอชิงตันดีซีและดำเนินการในประเทศต่างๆ กว่า 80 แห่ง และมีเจ้าหน้าที่ในสำนักงาน 11 แห่งทั่วโลก ได้แก่ บรัสเซลส์ ลอนดอน มิวนิค ปักกิ่ง เดลี จาการ์ตา กัวลาลัมเปอร์ ไทเป โตเกียว สิงคโปร์ และเซาเปาโล ทั้งนี้ บีเอสเอได้รับเงินทุนหลักจาก 2 ทาง คือ จากการแบ่งปันรายได้ของบริษัทผู้ผลิตซอฟต์แวร์ซึ่งเป็นสมาชิกของบีเอสเออยู่และจากข้อตกลงระงับคดีต่อบริษัทที่ถูกฟ้องร้องการละเมิดลิขสิทธิ์

3.2 ความสำคัญของกลุ่มพันธมิตรธุรกิจซอฟต์แวร์ต่อระบบการประมวลผลแบบคลาวด์

ดังที่ได้กล่าว ณ ข้างต้นว่าว่าสมาชิกของบีเอสเอเป็นบริษัทผู้ผลิตซอฟต์แวร์รายใหญ่ของโลก ซึ่งในปัจจุบัน สมาชิกส่วนใหญ่ของบีเอสเอต่างหันมาเพิ่มรูปแบบธุรกิจของตนให้ครอบคลุมถึงการให้บริการระบบการประมวลผลแบบคลาวด์ด้วย ด้วยเหตุนี้ บีเอสเอจึงจำเป็นต้องเข้ามามีบทบาทในการส่งเสริมการให้บริการระบบการประมวลผลแบบคลาวด์มากขึ้น โดยเริ่มต้นจากการสำรวจความพร้อมของแต่ละประเทศในการส่งเสริมระบบการประมวลผลแบบคลาวด์ โดยเฉพาะอย่างยิ่งความพร้อมของหลักเกณฑ์ ระเบียบ กฎหมายที่จะช่วยสร้างสภาพแวดล้อมที่ดีในการให้บริการระบบการประมวลผลแบบคลาวด์ได้ ซึ่งหากนานาประเทศมีความพร้อมในการรองรับการให้บริการระบบการประมวลผลแบบคลาวด์แล้ว ธุรกิจการให้บริการระบบการประมวลผลแบบคลาวด์ย่อมเติบโตและ

ได้รับความนิยมมากยิ่งขึ้น ซึ่งจะเป็นผลดีต่อภาคธุรกิจเนื่องจากบีเอสเอมีมุมมองว่าระบบการประมวลผลแบบคลาวด์สามารถแก้ไขปัญหาการใช้งานเทคโนโลยีในรูปแบบเดิมได้และช่วยให้ภาคธุรกิจสามารถลดต้นทุนด้านไอทีหรือเทคโนโลยีได้เป็นจำนวนมาก

3.3 การประเมินความพร้อมโดยบีเอสเอ

3.3.1 จุดประสงค์ของการประเมินความพร้อม

บีเอสเอมีวัตถุประสงค์ในการประเมินความพร้อมเพื่อสร้างพื้นที่สำหรับการแลกเปลี่ยนความคิดเห็นระหว่างผู้จัดทำนโยบาย (ภาครัฐ) และผู้ที่เกี่ยวข้องกับระบบการประมวลผลแบบคลาวด์ ในประเด็นเรื่องการพัฒนาระบบกฎหมายและกฎระเบียบเกี่ยวกับระบบการประมวลผลแบบคลาวด์ในรูปแบบที่สอดคล้องกันในระดับสากล ซึ่งจะช่วยให้แต่ละประเทศเห็นจุดที่ต้องปรับปรุงและสามารถกำหนดขั้นตอนดำเนินการที่จำเป็นต่อไปได้ และเพื่อช่วยส่งเสริมการเติบโตของเทคโนโลยีระบบการประมวลผลแบบคลาวด์ในระดับสากล

3.3.2 หลักเกณฑ์และวิธีการที่ใช้ในการประเมินความพร้อมประจำปีค.ศ. 2013 และปีค.ศ. 2016

บีเอสเอได้จัดทำรายงานการประเมินความพร้อมในระบบการประมวลผลแบบคลาวด์ของประเทศต่างๆ โดยมุ่งพิจารณาโครงสร้างพื้นฐานด้านไอทีและสภาพแวดล้อมเชิงนโยบายของประเทศต่างๆ ทั่วโลกทั้งหมด 24 ประเทศ ซึ่งมีขนาดตลาดไอทีขนาดใหญ่รวมกันคิดเป็น 80% ของตลาดไอทีทั่วโลก ทั้งนี้ บีเอสเอได้ประเมินและให้คะแนนจุดแข็งและจุดอ่อนที่บีเอสเอเล็งเห็นว่าจะส่งผลต่อการเติบโตของเศรษฐกิจและการปรับเปลี่ยนรูปแบบการดำเนินธุรกิจของประเทศที่จะเกิดขึ้นอันเนื่องมาจากการสนับสนุนเทคโนโลยีระบบการประมวลผลแบบคลาวด์ โดยใช้วิธีการตั้งคำถามที่ตั้งอยู่บนหลักเกณฑ์การพิจารณาของบีเอสเอ จำนวนทั้งสิ้น 7 ประการ ดังนี้[1]

[1] BSA and Galexia, “ผลการประเมินความพร้อมของประเทศต่างๆ ทั่วโลก สำหรับเทคโลโยลีคลาวด์คอมพิวติ้ง โดยบีเอสเอ (BSA) ประจำปี พ.ศ. 2559 : การเผชิญหน้ากับความท้าทายใหม่,” สืบค้นเมื่อวันที่ 10 ตุลาคม 2559, จาก http://cloudscorecard.bsa.org/2016/Pdf/BSA_2016_Global_Cloud_Scorecard_th.pdf

3.3.2.1 การรับประกันความเป็นส่วนตัว

เนื่องจากความสำเร็จของการให้บริการระบบการประมวลผลแบบคลาวด์นั้นขึ้นอยู่กับกระแสตอบรับของผู้ใช้บริการเป็นสำคัญ หากระบบการประมวลผลแบบคลาวด์มีผู้ใช้บริการเป็นจำนวนมากย่อมแสดงให้เห็นว่าระบบการประมวลผลแบบคลาวด์ได้รับการตอบรับเป็นอย่างดีจากผู้ใช้บริการ อย่างไรก็ตาม การตัดสินใจของผู้ใช้บริการว่าจะใช้บริการระบบการประมวลผลแบบคลาวด์หรือไม่นั้น มิได้ขึ้นอยู่กับว่าระบบการประมวลผลแบบคลาวด์ดังกล่าวมีผู้ใช้บริการมากน้อยเพียงใด แต่ขึ้นอยู่กับว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์รายใดจะสามารถทำให้ผู้ใช้บริการวางใจได้ว่าข้อมูลของตนจะไม่ถูกนำไปใช้หรือเปิดเผยโดยที่ไม่ได้รับอนุญาต แต่ในขณะเดียวกันเมื่อพิจารณาในมุมมองของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ ประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์จะต้องเปิดโอกาสให้ผู้ให้บริการนั้นๆ มีความอิสระในการเคลื่อนย้ายข้อมูลผ่านระบบการประมวลผลแบบคลาวด์ด้วยวิธีการที่มีประสิทธิภาพมากที่สุดซึ่งสามารถป้องกันข้อมูลของผู้ใช้บริการรั่วไหลออกจากระบบได้ด้วย ซึ่งสิ่งที่จะเป็นตัวชี้จุดได้ดีว่าประเทศนั้นๆ มีการเปิดโอกาสให้ผู้ให้บริการสามารถเคลื่อนย้ายข้อมูลได้หรือไม่ ได้แก่ กฎหมายหรือข้อบังคับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และหน่วยงานที่ได้รับมอบหมายให้บังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ดังนั้น บีเอสเอจึงได้ตั้งคำถามเกี่ยวกับความเป็นส่วนตัวของข้อมูลเพื่อใช้เป็นเกณฑ์ในการพิจารณาความพร้อมของแต่ละประเทศโดยให้น้ำหนักอัตราส่วนคะแนนในเรื่องความเป็นส่วนตัวของข้อมูล 10% คิดเป็นคะแนนเต็ม 10 คะแนน จากการพิจารณาคำถามดังนี้

1. มีกฎหมายหรือข้อบังคับเรื่องการเก็บ ใช้ หรือการดำเนินการต่างๆ กับข้อมูลส่วนบุคคลหรือไม่
2. กฎหมายเรื่องความเป็นส่วนตัวมีขอบเขตและครอบคุลมเรื่องอะไรบ้าง
3. กฎหมายเรื่องความเป็นส่วนตัวมีความสอดคล้องกับหลักการคุ้มครองความเป็นส่วนตัวตามข้อบังคับด้านการคุ้มครองของสหภาพยุโรปหรือไม่
4. กฎหมายเรื่องความเป็นส่วนตัวมีความสอดคล้องกับหลักการเรื่องความเป็นส่วนตัวตามกรอบการคุ้มครองความเป็นส่วนตัวของเอเปคหรือไม่
5. มีสิทธิส่วนบุคคลในการดำเนินการในกรณีที่เกิดการละเมิดความเป็นส่วนตัวของข้อมูลหรือไม่
6. มีหน่วยงาน (ผู้กำกับดูแล) ที่ได้รับมอบหมายให้บังคับใช้กฎหมายเรื่องความเป็นส่วนตัวอย่างมีประสิทธิภาพหรือไม่
7. ผู้กำกับดูแลความเป็นส่วนตัวมีลักษณะการทำงานอย่างไร
8. ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการยกเว้นจากข้อกำหนดเรื่องการขึ้นทะเบียนหรือไม่

9. การถ่ายโอนข้อมูลข้ามประเทศได้รับยกเว้นจากข้อกำหนดเรื่องการขึ้นทะเบียนหรือไม่
10. มีกฎหมายว่าด้วยเรื่องการแจ้งให้ทราบเมื่อเกิดการละเมิดข้อมูลหรือไม่

3.3.2.2 การรักษาความมั่นคงปลอดภัย

เช่นเดียวกันกับการรับประกันความเป็นส่วนตัว ประเทศที่จะถือว่ามีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์จะต้องเป็นประเทศที่นำเอามาตรการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีความทันสมัยมากำหนดให้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะต้องมีโดยไม่ระบุเป็นการเฉพาะเจาะจงว่าจะต้องเป็นการใช้เทคโนโลยีใดเทคโนโลยีหนึ่งเป็นการเฉพาะ ทั้งนี้ ก็เพื่อให้การให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศนั้นๆ ได้รับความมั่นใจจากผู้ใช้บริการว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ตระหนักและจัดการกับความเสี่ยงที่มีในการจัดเก็บข้อมูลของผู้ใช้บริการในระบบการประมวลผลแบบคลาวด์ได้เป็นอย่างดี

เพื่อเป็นการพิจารณาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของแต่ละประเทศ บีเอสเอได้ตั้งคำถามเกี่ยวกับการรักษาความมั่นคงปลอดภัยเพื่อใช้เป็นเกณฑ์ในการพิจารณาความพร้อมของแต่ละประเทศโดยให้น้ำหนักอัตราส่วนคะแนนในเรื่องการรักษาความมั่นคงปลอดภัย 10% คิดเป็นคะแนนเต็ม 10 คะแนน โดยอัตราส่วน 10 คะแนนนี้พิจารณาจากคำถามดังนี้

1. มีกฎหมายหรือข้อบังคับที่ให้น้ำหนักทางกฎหมายอย่างชัดเจนกับลายมือชื่ออิเล็กทรอนิกส์หรือไม่
2. ผู้ให้บริการอินเทอร์เน็ตและเนื้อหาได้รับการยกเว้นจากการถูกคัดกรองเนื้อหา (Filtering) หรือการควบคุม (Censoring) ตามที่มีข้อบังคับหรือไม่
3. มีกฎหมายหรือข้อกำหนดบังคับใช้ที่ระบุเรื่องการรักษาความมั่นคงปลอดภัยทั่วไป สำหรับผู้ใช้บริการโฮสติ้งข้อมูลดิจิทัลและผู้ให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
4. มีกฎหมายหรือข้อกำหนดบังคับใช้ที่ระบุให้มีการตรวจสอบการรักษาความมั่นคงปลอดภัยอย่างเฉพาะเจาะจงสำหรับผู้ให้บริการโฮสติ้งข้อมูลดิจิทัลและผู้ให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
5. มีกฎหมายและกฎระเบียบที่กำหนดให้มีการรับรองเฉพาะสำหรับผลิตภัณฑ์เทคโนโลยีหรือไม่

3.3.2.3 การต่อสู้กับอาชญากรรมทางไซเบอร์

เนื่องจากระบบการประมวลผลแบบคลาวด์เป็นระบบที่จัดเก็บข้อมูลสำคัญจำนวนมากรวมทั้งข้อมูลส่วนบุคคลของผู้ใช้บริการ ดังนั้น ระบบการประมวลผลแบบคลาวด์จึงเป็นระบบที่ดึงดูดการก่ออาชญากรรมทางไซเบอร์ ประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์จึงควรจะมีมาตรการในการรับมืออาชญากรรมทางไซเบอร์ ยกตัวอย่างเช่น มีการออกกฎหมายเพื่อควบคุมการก่ออาชญากรรมทางไซเบอร์โดยเฉพาะหรือกำหนดวิธีการสืบสวนสอบสวนโดยเฉพาะสำหรับกรณีที่มีการก่ออาชญากรรมทางไซเบอร์ เป็นต้น ด้วยเหตุนี้ในการพิจารณาความพร้อมเพื่อจัดอันดับประเทศที่มีความพร้อมในการให้บริการของบีเอสเอจึงมุ่งพิจารณาว่าประเทศต่างๆ ที่มีการให้บริการระบบการประมวลผลแบบคลาวด์มีระบบกฎหมายที่มีประสิทธิภาพสำหรับการบังคับใช้อย่างจริงจังกับการก่ออาชญากรรมทางไซเบอร์หรือไม่ ซึ่งกฎหมายดังกล่าวครอบคลุมถึงระเบียบที่เกี่ยวข้องกับการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ด้วย ทั้งนี้ เครื่องมือในการพิจารณาของ บีเอสเอในเรื่องการต่อสู้กับอาชญากรรมทางไซเบอร์ ได้แก่ การตั้งคำถามจำนวน 4 ข้อ โดยให้น้ำหนักกับการประเมิน 10% คิดเป็น 10 คะแนน จากทั้งหมด 100 คะแนน ดังนี้

1. มีกฎหมายอาชญากรรมไซเบอร์หรือไม่
2. กฎหมายอาชญากรรมไซเบอร์สอดคล้องกับอนุสัญญากรุงบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์หรือไม่
3. หน่วยงานบังคับใช้กฎหมายมีสิทธิเข้าถึงข้อมูลที่เข้ารหัสลับที่ถูกจัดเก็บหรือส่งโดยผู้ให้บริการโฮสติ้งข้อมูล ผู้ให้บริการเครือข่าย หรือผู้ให้บริการอื่นๆ ถึงระดับใด
4. กฎหมายดังกล่าวจัดการกับการกระทำความผิดที่อยู่นอกราชอาณาจักรอย่างไร

3.3.2.4 การคุ้มครองทรัพย์สินทางปัญญา

การคุ้มครองทรัพย์สินทางปัญญานั้นถือเป็นปัจจัยสำคัญในการส่งเสริมความก้าวหน้าด้านนวัตกรรมและเทคโนโลยีให้มีความต่อเนื่อง โดยเฉพาะอย่างยิ่งในการวิจัยและพัฒนาระบบการประมวลผลแบบคลาวด์ให้สามารถรองรับการใช้งานของผู้บริโภคที่เพิ่มมากขึ้นอย่างต่อเนื่อง ดังนั้น ประเทศที่จะถือว่ามีความพร้อมสำหรับการให้บริการระบบการประมวลผลแบบคลาวด์จึงจะต้องมีกฎหมายคุ้มครองทรัพย์สินทางปัญญาที่ชัดเจนและมีการใช้บังคับกฎหมายคุ้มครองทรัพย์สินทางปัญญาอย่างจริงจังเมื่อเกิดการกระทำที่ไม่ถูกต้องหรือการกระทำอันถือเป็นการละเมิดทรัพย์สินทางปัญญา ทั้งนี้ บีเอสเอได้ประเมินการคุ้มครองทรัพย์สินทางปัญญาโดยให้น้ำหนัก 20% คิดเป็น 20 คะแนน จากทั้งหมด 100 คะแนน โดยอาศัยคำถามจำนวน 12 ข้อ ดังนี้

1. ประเทศไทยเป็นสมาชิกตามความตกลงว่าด้วยสิทธิในทรัพย์สินทางปัญญาที่เกี่ยวกับการค้า (TRIPS) หรือไม่
2. มีการบังคับใช้กฎหมายทรัพย์สินทางปัญญาเพื่อทำตามความตกลง TRIPS หรือไม่
3. ประเทศไทยร่วมเป็นภาคีสนธิสัญญาลิขสิทธิ์ขององค์การทรัพย์สินทางปัญญาโลกหรือไม่
4. มีการออกกฎหมายโดยนำสนธิสัญญาลิขสิทธิ์ขององค์การทรัพย์สินทางปัญญาโลกมาใช้หรือไม่
5. มีบทลงโทษทางแพ่งสำหรับการเผยแพร่ (โพสต์) งานของเจ้าของลิขสิทธิ์โดยไม่ได้รับอนุญาตบนอินเทอร์เน็ตหรือไม่
6. มีบทลงโทษทางอาญาสำหรับการเผยแพร่ (โพสต์) งานของเจ้าของลิขสิทธิ์โดยไม่ได้รับอนุญาตบนอินเทอร์เน็ตหรือไม่
7. มีกฎหมายว่าด้วยความรับผิดของผู้ให้บริการอินเทอร์เน็ต สำหรับเนื้อหาที่ละเมิดลิขสิทธิ์ที่พบบนเว็บไซต์และระบบของผู้ให้บริการดังกล่าวหรือไม่
8. มีเกณฑ์ความรับผิดของผู้ให้บริการอินเทอร์เน็ต สำหรับเนื้อหาที่ละเมิดลิขสิทธิ์ที่พบบนเว็บไซต์และระบบของผู้ให้บริการดังกล่าวหรือไม่
9. มีบทลงโทษประเภทใดบ้าง สำหรับความรับผิดของผู้ให้บริการอินเทอร์เน็ตในกรณีมีเนื้อหาละเมิดลิขสิทธิ์พบอยู่บนเว็บไซต์หรือระบบของผู้ให้บริการดังกล่าว
10. ผู้ให้บริการอินเทอร์เน็ตต้องลบเนื้อหาที่ละเมิดลิขสิทธิ์หรือไม่ เมื่อเจ้าของลิขสิทธิ์แจ้งให้ทราบ
11. ผู้ให้บริการอินเทอร์เน็ตจำเป็นต้องแจ้งสมาชิกผู้ใช้บริการ ในกรณีที่ได้รับการแจ้งว่าสมาชิกรายนั้นใช้บริการของผู้ให้บริการอินเทอร์เน็ตพื่อเผยแพร่เนื้อหาที่ละเมิดลิขสิทธิ์หรือไม่
12. มีการคุ้มครองทางกฎหมายที่ชัดเจน รวมถึงการบังคับใช้ที่มีประสิทธิภาพหรือไม่ ในกรณีของการใช้บริการระบบการประมวลผลแบบคลาวด์อย่างไม่เหมาะสม

3.3.2.5 การรับประกันด้านการเคลื่อนย้ายข้อมูลและการปรับปรุงกฎระเบียบระหว่างประเทศให้สอดคล้องกัน

เนื่องจากหลักการของระบบการประมวลผลแบบคลาวด์คือการจัดเก็บประมวลผลข้อมูลแบบไร้ขอบเขต ซึ่งจะก่อให้เกิดการเคลื่อนย้ายข้อมูลในระบบระหว่างประเทศเป็นจำนวนมาก ทั้งนี้ ก็เพื่อให้ระบบการประมวลผลแบบคลาวด์สามารถใช้บริการได้เต็มประสิทธิภาพ อย่างไรก็ตาม เมื่อพิจารณากฎหมายของนานาประเทศจะพบว่ากฎหมายดังกล่าวยังคงมีข้อจำกัดเกี่ยวกับการเคลื่อนย้ายข้อมูลระหว่างประเทศ โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคล ซึ่งในปัจจุบันองค์กรหลายองค์กรในภาคอุตสาหกรรมของระบบการประมวลผลแบบคลาวด์มีความพยายามที่จะ

พัฒนามาตรฐานระหว่างประเทศเพื่อรองรับการเคลื่อนย้ายข้อมูลได้อย่างเสรีในระหว่างประเทศ ดังนั้น ในการพิจารณาประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์ บีเอสเอจึงจำเป็นต้องพิจารณาว่าประเทศนั้นๆ ได้รับการสนับสนุนจากรัฐบาลหรือภาครัฐในการปรับปรุงกฎหมายเกี่ยวกับเรื่องนี้หรือไม่ และรวมถึงกฎหมายหรือกฎระเบียบด้านพาณิชย์อิเล็กทรอนิกส์ ภาษีศุลกากรและกฎระเบียบทางการค้าอื่นๆ ด้วย ทั้งนี้ บีเอสเอได้ตั้งคำถามเพื่อพิจารณาหลักเกณฑ์ส่วนนี้จำนวน 7 ข้อ โดยให้น้ำหนัก 10% คิดเป็น 10 คะแนน จากทั้งหมด 100 คะแนน ดังนี้

1. มีกฎหมาย ข้อบังคับ หรือนโยบายที่จัดตั้งกรอบการทำงานในการตั้งมาตรฐาน สำหรับการทำงานร่วมกันและการเคลื่อนย้ายข้อมูลหรือไม่
2. มีหน่วยงานกำกับดูแลที่ทำหน้าที่ในการพัฒนามาตรฐานในประเทศไทยหรือไม่
3. มีกฎหมายพาณิชย์อิเล็กทรอนิกส์หรือไม่
4. กฎหมายพาณิชย์อิเล็กทรอนิกส์อ้างอิงจากเอกสารสากลฉบับใด
5. การดาวน์โหลดแอพพลิเคชั่นหรือข้อมูลดิจิทัลจากผู้ให้บริการระบบการประมวลผลแบบคลาวด์ต่างประเทศ ได้รับการยกเว้นจากภาษีศุลกากรหรือการกีดกันทางการค้าแบบอื่นๆ หรือไม่
6. มีการสนับสนุนให้ใช้มาตรฐานสากลมากกว่ามาตรฐานในประเทศหรือไม่
7. รัฐบาลเข้าร่วมในกระบวนการจัดตั้งมาตรฐานสากลหรือไม่

3.3.2.6 การส่งเสริมการค้าเสรี

ลักษณะที่สำคัญประการหนึ่งของระบบการประมวลผลแบบคลาวด์ คือ การทำงานที่ก้าวข้ามขอบเขตพรมแดนประเทศ ดังนั้น ในประเทศที่มีความพร้อมสำหรับการให้บริการระบบการประมวลผลแบบคลาวด์จึงต้องไม่ขัดขวางระบบการค้าเสรี รวมถึงไม่มีการให้สิทธิพิเศษกับผลิตภัณฑ์บางผลิตภัณฑ์ หรือผู้ให้บริการเฉพาะราย โดยเฉพาะอย่างยิ่งหากเป็นการจัดซื้อจัดจ้างของรัฐบาลของประเทศนั้นๆ ทั้งนี้ ในการพิจารณาบีเอสเอได้ตั้งคำถามเกี่ยวกับการส่งเสริมการค้าเสรีจำนวน 4 ข้อ โดยให้น้ำหนัก 10% คิดเป็น 10 คะแนน จากทั้งหมด 100 คะแนน ดังนี้

1. มีกฎหมายและนโยบายที่นำหลักการความเป็นกลางทางเทคโนโลยีไปใช้ในภาครัฐหรือไม่
2. บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินการโดยไม่ขึ้นอยู่กับนโยบายที่บังคับให้ใช้งานผลิตภัณฑ์บางประเภท (ซึ่งรวมถึงแต่ไม่จำกัดเพียงประเภทของซอฟต์แวร์) บริการมาตรฐาน หรือเทคโนโลยีหรือไม่

3. บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินการโดยไม่ขึ้นอยู่กับกฎหมายและนโยบายที่กำหนดลักษณะผลิตภัณฑ์บางประเภท (ซึ่งรวมถึงแต่ไม่จำกัดเพียงประเภทของซอฟต์แวร์) บริการ มาตรฐาน หรือเทคโนโลยีหรือไม่
4. บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินการโดยไม่ขึ้นอยู่กับกฎหมายที่เลือกปฏิบัติกับสัญชาติของผู้ค้า นักพัฒนาหรือผู้ให้บริการหรือไม่

3.3.2.7 การสร้างโครงสร้างพื้นฐานด้านไอทีที่จำเป็น (ความพร้อมทางด้านไอทีและการปรับใช้บรอดแบรนด์)

ในการใช้บริการระบบการประมวลผลแบบคลาวด์นั้นจำเป็นต้องพึ่งพาการเข้าถึงบรอดแบรนด์และอินเทอร์เน็ตที่มีความยืดหยุ่น มีความรวดเร็ว มีความครอบคลุมแพร่หลายทุกหนแห่ง รวมทั้งต้องมีราคาถูก ดังนั้น ความพร้อมเกี่ยวกับโครงสร้างพื้นฐานด้านไอทีจึงเป็นปัจจัยที่สำคัญประการหนึ่งในการชี้วัดว่าประเทศนั้นมีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่ ซึ่งการที่ประเทศต่างๆ จะมีโครงสร้างพื้นฐานด้านไอทีที่จำเป็นได้นั้น ประเทศดังกล่าวจำเป็นต้องอาศัยนโยบายของภาครัฐที่ให้สิทธิประโยชน์หรือสิ่งจูงใจให้ภาคเอกชนเข้ามาลงทุนในโครงสร้างพื้นฐานด้านบรอดแบรนด์ รวมถึงการบัญญัติกฎหมายที่ส่งเสริมการเข้าถึงบรอดแบรนด์จากทุกหนทุกแห่งด้วย ทั้งนี้ ในการพิจารณาบีเอสเอได้ตั้งคำถามเกี่ยวกับความพร้อมทางด้านไอทีและการปรับใช้บรอดแบนด์ จำนวน 7 ข้อ โดยให้น้ำหนัก 30% คิดเป็น 30 คะแนน จากทั้งหมด 100 คะแนน ดังนี้

1. มีแผนงานบรอดแบนด์แห่งชาติหรือไม่
2. มีกฎหมายหรือนโยบายที่กำกับดูแลการจัดตั้งระดับการให้บริการต่างๆ สำหรับการส่งข้อมูลโดยขึ้นอยู่กับประเภทของข้อมูลที่ถูกส่งหรือไม่
3. พิจารณาตัวชี้วัดพื้นฐาน
   -จำนวนประชากร (ล้าน)
   -ประชากรในเมือง (%)
   -จำนวนครัวเรือน (ล้าน)
   -ความหนาแน่นของประชากร (จำนวนคนต่อตารางกิโลเมตร)
   -GDP ต่อหัว (ดอลลาร์สหรัฐ)
   -การส่งออกบริการไอที (พันล้านดอลลาร์สหรัฐ)
   -จำนวนคอมพิวเตอร์ส่วนบุคคล
4. ตัวชี้วัดความพร้อมทางด้านไอทีและเครือข่าย

-ดัชนีการพัฒนาทางเทคโนโลยีสารสนเทศและการสื่อสาร (IDI) ของสหภาพโทรคมนาคมระหว่างประเทศ

-ดัชนีบ่งชี้ระดับความพร้อมของการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร (NRI) ของการประชุมเวทีเศรษฐกิจโลก

-คะแนนด้านการเชื่อมต่อไปต่างประเทศ

5. ผู้ใช้งานอินเทอร์เน็ตและแบนด์วิดธ์ต่างประเทศ

-จำนวนผู้ใช้งานอินเทอร์เน็ต (ล้าน)

-จำนวนผู้ใช้งานอินเทอร์เน็ตคิดเป็นร้อยละของจำนวนประชากร

-แบนด์วิธอินเทอร์เน็ตต่างประเทศ (บิดต่อวินาทีต่อจำนวนผู้ใช้งานอินเทอร์เน็ต)

-แบนด์วิธอินเทอร์เน็ตต่างประเทศ (จำนวนกิกะบิตต่อวินาทีต่อประเทศ)

6. บรอดแบนด์ตามสาย

-จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสาย

-จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนครัวเรือน

-จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนประชากร

-จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนผู้ใช้งานอินเทอร์เน็ต

7. บรอดแบนด์แบบเคลื่อนที่

-จำนวนผู้สมัครใช้บริการโทรศัพท์เคลื่อนที่แบบเซลลูลาร์ (ล้าน)

-จำนวนผู้สมัครใช้บริการบรอดแบนด์แบบเคลื่อนที่ที่เปิดใช้งานอยู่ต่อประชากร 100 คน

-จำนวนของผู้สมัครใช้สมาชิกบรอดแบนด์แบบเคลื่อนที่ที่เปิดใช้งานอยู่ (ล้าน)

3.3.3 หลักเกณฑ์และวิธีการที่ใช้ในการประเมินความพร้อมประจำปีค.ศ. 2018

ในปี 2018 BSA ได้ปรับเปลี่ยนคำถามบางส่วนและปรับปรุงอัตราคะแนนสำหรับการประเมินใหม่ โดยมีรายละเอียดดังนี้[2]

3.3.3.1 การรับประกันความเป็นส่วนตัว

BSA ปรับปรุงอัตราคะแนนส่วนนี้จากเดิม 10 คะแนน คิดเป็น 10% โดยเปลี่ยนเป็น 12.5 คะแนน คิดเป็น 12.5% และปรับเปลี่ยนคำถาม ดังต่อไปนี้

[2] BSA and Galexia, “2018 BSA GLOBAL CLOUD COMPUTING SCORECARD: Powering a Bright Future,” สืบค้นเมื่อวันที่ 10 กุมภาพันธ์ 2560, จาก http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

1. มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับหรือไม่
2. กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีขอบเขตและครอบคลุมเรื่องอะไรบ้าง
3. มีหน่วยงานคุ้มครองข้อมูลส่วนบุคคลหรือไม่
4. ลักษณะการทำงานของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างไร
5. หน่วยงานคุ้มครองข้อมูลส่วนบุคคลบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและโปร่งใสหรือไม่
6. กฎหมายคุ้มครองข้อมูลส่วนบุคคลสอดคล้องกับ Framework ต่างประเทศที่อำนวยความสะดวกในการโอนข้อมูลส่วนบุคคลระหว่างประเทศหรือไม่
7. ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการยกเว้นจากข้อกำหนดเรื่องการขึ้นทะเบียนหรือไม่
8. มีเงื่อนไขการโอนข้อมูลส่วนบุคคลระหว่างประเทศบังคับใช้หรือไม่
9. การโอนข้อมูลส่วนบุคคลระหว่างประเทศไม่ตกอยู่ภายใต้ข้อจำกัดที่ไม่เหมาะสมหรือไม่
10. มีกฎหมายว่าด้วยเรื่องการแจ้งให้ทราบเมื่อเกิดการละเมิดข้อมูลส่วนบุคคลหรือไม่
11. เงื่อนไขการแจ้งเตือนการละเมิดข้อมูลส่วนบุคคลมีการกำหนดความโปร่งใส ฐานความเสี่ยง และการไม่ละเมิดสิทธิหรือไม่
12. มีสิทธิที่เป็นอิสระในการดำเนินการใดๆ กรณีที่มีการละเมิดข้อมูลส่วนบุคคลหรือไม่

3.3.3.2 การรักษาความมั่นคงปลอดภัย

BSA ปรับปรุงอัตราคะแนนส่วนนี้จากเดิม 10 คะแนน คิดเป็น 10% โดยเปลี่ยนเป็น 12.5 คะแนน คิดเป็น 12.5% และปรับเปลี่ยนคำถาม ดังต่อไปนี้

1. มีมาตรการในระดับรัฐสำหรับการคุ้มครองความปลอดภัยทางไซเบอร์หรือไม่
2. มาตรการในระดับรัฐสำหรับการคุ้มครองความปลอดภัยทางไซเบอร์เป็นปัจจุบันและครอบคลุมหรือไม่
3. มีกฎหมายหรือ Guidance ที่กำหนดเงื่อนไขเรื่องความปลอดภัยทางไซเบอร์สำหรับผู้ให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
4. กฎหมายหรือ Guidance มีการกำหนดความโปร่งใส ฐานความเสี่ยง และการไม่ละเมิดสิทธิหรือไม่
5. มีกฎหมายหรือ Guidance ที่กำหนดเงื่อนไขเรื่องการตรวจสอบ (Audit) ความปลอดภัยทางไซเบอร์สำหรับผู้ให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
6. มีเงื่อนไขกำหนดให้ต้องปฏิบัติตามมาตรฐานสากลเรื่องความปลอดภัย ใบรับรอง (Certification) หรือการทดสอบ (Testing) หรือไม่

3.3.3.3 การต่อสู้กับอาชญากรรมไซเบอร์

BSA ปรับปรุงอัตราคะแนนส่วนนี้จากเดิม 10 คะแนน คิดเป็น 10% โดยเปลี่ยนเป็น 12.5 คะแนน คิดเป็น 12.5% และปรับเปลี่ยนคำถาม ดังต่อไปนี้

1. มีกฎหมายอาชญากรรมไซเบอร์ใช้บังคับหรือไม่
2. กฎหมายอาชญากรรมไซเบอร์สอดคล้องกับอนุสัญญากรุงบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์หรือไม่
3. กฎหมายท้องถิ่นหรือนโยบายการบังคับใช้กฎหมายสามารถเข้าถึง (access) การหลีกเลี่ยงคำสั่งเฉพาะทางเทคโนโลยีหรืออุปสรรคอื่นๆ สำหรับการให้บริการและความปลอดภัยของสินค้าหรือไม่
4. มีข้อตกลงที่ใช้บังคับเกี่ยวกับการแลกเปลี่ยนข้อมูลระหว่างประเทศสำหรับวัตถุประสงค์ในการบังคับใช้กฎหมายที่โปร่งใสและเป็นธรรมหรือไม่

3.3.3.4 สิทธิทางทรัพย์สินทางปัญญา

BSA ปรับปรุงอัตราคะแนนส่วนนี้จากเดิม 10 คะแนน คิดเป็น 10% โดยเปลี่ยนเป็น 12.5 คะแนน คิดเป็น 12.5% และปรับเปลี่ยนคำถาม ดังต่อไปนี้

1. มีกฎหมายลิขสิทธิ์หรือกฎหมายทรัพย์สินทางปัญญาอื่นใดที่บังคับใช้สอดคล้องกับมาตรฐานสากลในการให้ความคุ้มครองผู้ให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
2. มีกฎหมายลิขสิทธิ์หรือกฎหมายทรัพย์สินทางปัญญาอื่นใดที่มีผลและใช้บังคับอย่างมีประสิทธิภาพหรือไม่
3. มีการคุ้มครองทางกฎหมายที่ชัดแจ้งซึ่งต่อต้านความลับทางการค้าที่ใช้อย่างไม่เหมาะสมหรือไม่
4. มีกฎหมายเกี่ยวกับความลับทางการค้าที่บังคับใช้อย่างมีประสิทธิภาพหรือไม่
5. มีการคุ้มครองทางกฎหมายเพื่อต่อต้านการใช้อุบายจำกัดมาตรการคุ้มครองทางเทคโนโลยีหรือไม่
6. มีกฎหมายต่อต้านการใช้อุบายจำกัดมาตรการคุ้มครองทางเทคโนโลยีใช้บังคับหรือไม่
7. มีการคุ้มครองทางกฎหมายใช้บังคับสำหรับ Software-implemented inventions หรือไม่
8. มีกฎหมายเกี่ยวกับการคุ้มครอง Software-implemented inventions ใช้บังคับอย่างมีประสิทธิภาพหรือไม่

3.3.3.5 มาตรฐานและการปรับปรุงให้สอดคล้องกันในระดับสากล

BSA เพิ่มคำถามในส่วนนี้มาโดยให้อัตราส่วนคะแนนเป็น 12.5 คะแนน คิดเป็น 12.5% ดังนี้

1. มีหน่วยงานตามกฎหมายที่รับผิดชอบในการพัฒนามาตรฐานของประเทศนั้นๆ หรือไม่
2. มาตรฐานระดับสากลเอื้อต่อมาตรฐานภายในประเทศหรือไม่
3. รัฐบาลมีส่วนร่วมในการกำหนดขั้นตอนตามมาตรฐานสากลหรือไม่
4. มีกฎหมายเกี่ยวกับ e-Commerce ใช้บังคับหรือไม่
5. กฎหมายเกี่ยวกับ e-Commerce มีรากฐานจากกฎหมายหรือเครื่องมือใดในระดับสากล
6. มีกฎหมายที่ให้น้ำหนักทางกฎหมายกับลายมือชื่ออิเล็กทรอนิกส์หรือไม่
7. ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ไม่อยู่ภายใต้บังคับของคำสั่งหรือข้อบังคับเกี่ยวกับการควบคุม (Filtering or censoring) หรือไม่

3.3.3.6 การสนับสนุนการค้าเสรี

BSA เพิ่มคำถามเกี่ยวกับการสนับสนุนการค้าเสรีโดยให้น้ำหนักจำนวน 12.5 คะแนน คิดเป็น 12.5% จากคำถามดังต่อไปนี้

1. มี National strategy ที่ใช้บังคับเพื่อส่งเสริมหรือสนับสนุนการให้บริการระบบการประมวลผลแบบคลาวด์หรือไม่
2. มีกฎหมายที่ใช้บังคับที่นำเอาหลักการเรื่อง Technology neutrality มาใช้ในภาครัฐหรือไม่
3. การให้บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินธุรกิจโดยเป็นอิสระจากการส่งเสริมหรือสนับสนุนบริการหรือเทคโนโลยีบางประเภทหรือไม่
4. การให้บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินธุรกิจโดยเป็นอิสระจากการได้รับอนุญาตซึ่งกำหนดเงื่อนไขจากสัญชาติของผู้ให้บริการหรือไม่
5. ประเทศนั้นมีการลงนามและนำเอาข้อตกลงระหว่างประเทศมาใช้บังคับเพื่อทำให้เกิดความมั่นใจว่าการให้บริการระบบการประมวลผลแบบคลาวด์จะไม่ตกอยู่ภายใต้หลักการเลือกปฏิบัติหรือไม่
6. การให้บริการระบบการประมวลผลแบบคลาวด์ไม่ตกอยู่ภายใต้อุปสรรคทางการค้าหรือกำแพงภาษีหรือไม่
7. การให้บริการระบบการประมวลผลแบบคลาวด์สามารถดำเนินการได้โดยไม่ต้องอยู่ภายใต้ข้อจำกัดของกฎหมายเกี่ยวกับเรื่อง Data Localization หรือไม่

3.3.3.7 การสร้างโครงสร้างพื้นฐานด้านไอทีที่จำเป็น (ความพร้อมทางด้านไอทีและการพัฒนาบรอดแบรนด์)

BSA ปรับปรุงอัตราคะแนนส่วนนี้จากเดิม 30 คะแนน คิดเป็น 30% โดยเปลี่ยนเป็น 25 คะแนน คิดเป็น 25% และปรับเปลี่ยนคำถาม ดังต่อไปนี้

1. มีแผนงานบรอดแบนด์แห่งชาติหรือไม่
2. แผนงานบรอดแบนด์แห่งชาติมีผลใช้บังคับอย่างมีประสิทธิภาพหรือไม่
3. มีกฎหมายกำหนดเรื่องเกี่ยวกับ “net neutrality” หรือไม่
4. พิจารณาตัวชี้วัดพื้นฐาน
   -จำนวนประชากร (ล้าน)
   -ประชากรในเมือง (%)
   -จำนวนครัวเรือน (ล้าน)
   -ความหนาแน่นของประชากร (จำนวนคนต่อตารางกิโลเมตร)
   -GDP ต่อหัว (ดอลลาร์สหรัฐ)
   -การส่งออกบริการไอที (พันล้านดอลลาร์สหรัฐ)
   -จำนวนคอมพิวเตอร์ส่วนบุคคล
5. ตัวชี้วัดความพร้อมทางด้านไอทีและเครือข่าย
   -ดัชนีการพัฒนาทางเทคโนโลยีสารสนเทศและการสื่อสาร (IDI) ของสหภาพโทรคมนาคมระหว่างประเทศ
   -ดัชนีบ่งชี้ระดับความพร้อมของการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร (NRI) ของการประชุมเวทีเศรษฐกิจโลก
6. ผู้ใช้งานอินเทอร์เน็ตและแบนด์วิดธ์ต่างประเทศ
   -จำนวนผู้ใช้งานอินเทอร์เน็ต (ล้าน)
   -จำนวนผู้ใช้งานอินเทอร์เน็ตคิดเป็นร้อยละของจำนวนประชากร
   -แบนด์วิธอินเทอร์เน็ตต่างประเทศ (บิดต่อวินาทีต่อจำนวนผู้ใช้งานอินเทอร์เน็ต)
   -แบนด์วิธอินเทอร์เน็ตต่างประเทศ (จำนวนกิกะบิตต่อวินาทีต่อประเทศ)
7. บรอดแบนด์ตามสาย
   -จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสาย
   -จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนครัวเรือน
   -จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนประชากร
   -จำนวนผู้สมัครใช้บริการบรอดแบนด์ตามสายคิดเป็น % ของจำนวนผู้ใช้งานอินเทอร์เน็ต

3.3.4 ผลการประเมินความพร้อม

จากการประเมินความพร้อมในปี 2013 และปี 2016 ปรากฏผลการประเมินความพร้อม ดังนี้

ปี 2013			ปี 2016		
อันดับที่	**ประเทศ**	**คะแนนรวม**	**อันดับที่**	**ประเทศ**	**คะแนนรวม**
1	ญี่ปุ่น	84.1	1	ญี่ปุ่น	84.8
2	ออสเตรเลีย	79.9	2	สหรัฐอเมริกา	82.4
3	สหรัฐอเมริกา	79.7	3	เยอรมนี	82.0
4	เยอรมนี	79.1	4	แคนาดา	80.9
5	สิงคโปร์	78.5	5	ฝรั่งเศส	80.7
6	ฝรั่งเศส	78.3	6	ออสเตรเลีย	80.0
7	สหราชอาณาจักร	76.9	7	สิงคโปร์	79.5
8	เกาหลีใต้	76.2	8	อิตาลี	79.3
9	แคนาดา	75.8	9	สหราชอาณาจักร	78.9
10	อิตาลี	75.5	10	โปแลนด์	76.7
11	สเปน	73.7	11	สเปน	76.3
12	โปแลนด์	72.0	12	เกาหลีใต้	75.5
13	มาเลเซีย	69.5	13	มาเลเซีย	69.7
14	รัสเซีย	59.1	14	แอฟริกาใต้	61.3
15	แม็กซิโก	56.9	15	แม็กซิโก	60.8
16	อาร์เจนตินา	56.5	16	อาร์เจนตินา	58.0
17	อินเดีย	53.1	17	รัสเซีย	56.4
18	ตุรกี	52.4	18	อินเดีย	56.1
19	จีน	51.5	19	ตุรกี	54.5
20	แอฟริกาใต้	51.3	20	อินโดนีเซีย	49.4
21	อินโดนีเซีย	48.4	21	ไทย	48.8
22	บราซิล	44.1	22	บราซิล	48.5
23	ไทย	44.0	23	จีน	47.9
24	เวียดนาม	40.1	24	เวียดนาม	43.7

สำหรับผลการประเมินความพร้อมของประเทศไทยจะพบว่าในปี 2013 ประเทศไทยอยู่ในอันดับที่ 23 มีคะแนนรวมจำนวน 44 คะแนน แต่ในปี 2016 ประเทศไทยขึ้นมาอยู่ในอันดับที่ 21 โดยมีคะแนนรวมอยู่ที่ 48.8 คะแนน ดังนี้

เกณฑ์การพิจารณา	คะแนนปี 2013	คะแนนปี 2016	รายละเอียด
1. ความเป็นส่วนตัวของข้อมูล	3.5	3.5	ประเทศไทยยังคงไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตลอดจนหน่วยงานผู้ที่กำกับดูแลหรือบังคับใช้กฎหมายในเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคล
2.การรักษาความมั่นคงปลอดภัย	1.6	1.6	ประเทศไทยยังคงไม่มีกฎหมายที่ระบุเรื่องการรักษาความมั่นคงปลอดภัยทั่วไปตลอดจนไม่มีกฎหมายที่ระบุให้มีการตรวจสอบการรักษาความมั่นคงปลอดภัยอย่างเฉพาะเจาะจง สำหรับผู้ให้บริการโฮสติ้งข้อมูลดิจิทัลและผู้ให้บริการระบบการประมวลผลแบบคลาวด์
3.อาชญากรรมไซเบอร์	7.4	7.4	ประเทศไทยมีกฎหมายอาชญากรรมไซเบอร์ที่สอดคล้องกับอนุสัญญากรุงบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์ ซึ่งครอบคลุมการกระทำความผิดที่อยู่นอกราชอาณาจักร แต่ภายใต้กฎหมายไทยหน่วยงานบังคับใช้กฎหมายมีสิทธิเข้าถึงข้อมูลที่เข้ารหัสลับที่ถูกเก็บหรือส่งโดยผู้ให้บริการโฮสติ้งข้อมูล ผู้ให้บริการเครือข่ายหรือผู้ให้บริการอื่นๆแบบไม่จำกัด ซึ่งหากประเทศไทยจะแก้ไขในส่วนนี้ประเทศไทยควรกำหนดการเข้าถึงข้อมูลดังกล่าวแบบจำกัด เช่น ต้องมีหมายค้น เป็นต้น

เกณฑ์การพิจารณา	คะแนนปี 2013	คะแนนปี 2016	รายละเอียด
4.สิทธิในทรัพย์สินทางปัญญา	8.0	10.6	ในปี 2016 ประเทศไทยได้รับคะแนนในส่วนนี้ดีขึ้น อันเนื่องมาจากการดำเนินการดังนี้ (1) มีการออกและบังคับใช้กฎหมายทรัพย์สินทางปัญญาเพื่อทำตามความตกลง TRIPS ตามที่ประเทศไทยร่วมเป็นภาคีสนธิสัญญาลิขสิทธิ์ขององค์การทรัพย์สินทางปัญญาโลก (2) มีกฎหมายกำหนดความรับผิดและโทษ (เฉพาะทางแพ่ง) ของผู้ให้บริการอินเทอร์เน็ตในส่วนของเนื้อหาที่มีการละเมิดลิขสิทธิ์ที่พบบนเว็บไซต์และระบบของผู้ให้บริการ (3) มีกฎหมายที่คุ้มครองการใช้ระบบการประมวลผลแบบคลาวด์ที่ไม่เหมาะสมอย่างครอบคลุม
5.การรับประกันด้านการเคลื่อนย้ายข้อมูลและการปรับปรุงกฎระเบียบระหว่างประเทศให้สอดคล้องกัน	8.8	8.8	ประเทศไทยมีกฎหมายพาณิชย์อิเล็กทรอนิกส์ที่อ้างอิงมาจากกฎหมายแม่แบบของคณะกรรมาธิการกฎหมายการค้าระหว่างประเทศแห่งสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ ตามหลักเกณฑ์ของสากล ตลอดจนการดาวน์โหลดแอพพลิเคชั่นหรือข้อมูลดิจิทัลจากผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในต่างประเทศก็ได้รับยกเว้นภาษีศุลกากรและการกีดกันทางการค้าแบบอื่นๆ

เกณฑ์การพิจารณา	คะแนนปี 2013	คะแนนปี 2016	รายละเอียด
6.การส่งเสริมการค้าเสรี	3.0	3.0	ในประเทศไทยการให้บริการระบบการประมวลผลแบบคลาวด์ สามารถดำเนินการได้โดยไม่ขึ้นอยู่กับนโยบายที่บังคับให้ใช้งานแค่ผลิตภัณฑ์บางประเภทเท่านั้น ซึ่งเป็นการแสดงออกซึ่งการส่งเสริมการค้าเสรี
7.ความพร้อมทางด้านไอทีและการปรับใช้บรอดแบนด์	11.7	13.9	ประเทศไทยได้คะแนนในส่วนนี้เพิ่มขึ้น เนื่องมาจากนโยบายที่จะขยายบรอดแบนด์ให้ครอบคลุม 95% และจะให้การเข้าถึงอินเทอร์เน็ตบรอดแบนด์ที่มีความเร็วอย่างน้อย 100 Mbps ในจังหวัดที่มีความสำคัญทางเศรษฐกิจ ภายในปี พ.ศ. 2563

ตารางที่ 1.2 ผลการประเมินความพร้อมของบีเอสเอประจำปี 2013 และ 2016

อย่างไรก็ตาม เมื่อไม่นานมานี้ บีเอสเอได้เผยแพร่การประเมินในปี 2018 ออกมา ประเทศไทยได้รับการจัดอันดับอยู่ในอันดับที่ 19 จากทั้งหมด 24 อันดับ โดยบีเอสเอพิจารณาว่าประเทศไทยยังมีนโยบายที่เกี่ยวข้องกับการให้บริการระบบการประมวลผลแบบคลาวด์ไม่ครอบคลุมตามที่บีเอสเอกำหนด แต่เนื่องจากประเทศไทยมีการพัฒนาระบบกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ e-Commerce ลายมือชื่ออิเล็กทรอนิกส์และลิขสิทธิ์ให้สอดรับกับสากลทำให้ประเทศไทยได้รับการจัดอันดับที่ดีขึ้น ทั้งนี้ทั้งนั้น ประเทศไทยก็ยังมีจุดอ่อนในด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลอยู่เช่นเดิม

ด้วยเหตุนี้ จากผลการประเมินข้างต้น หากประเทศไทยต้องการพัฒนาเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคล บีเอสเอคาดหวังให้ประเทศไทยมีการดำเนินการ ดังต่อไปนี้

1 .ให้ประเทศไทยมีกฎหมายหรือข้อบังคับเรื่องการเก็บ ใช้ หรือการดำเนินการต่างๆ กับข้อมูลส่วนบุคคล โดยกฎหมายดังกล่าวจะต้องมีหลักการสำคัญสอดคล้องกับข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค และมีสาระสำคัญดังต่อไปนี้กำหนดอยู่

- กำหนดให้มีการแจ้งให้ทราบเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล

- กำหนดให้ผู้ควบคุมข้อมูลได้รับการยกเว้นจากข้อกำหนดด้านการขึ้นทะเบียน
- กำหนดให้การถ่ายโอนข้อมูลระหว่างประเทศได้รับการยกเว้นจากข้อกำหนดด้านการขึ้นทะเบียน

2. ให้ประเทศไทยจัดตั้งหน่วยงานในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

3.3.5 ผลกระทบต่อประเทศไทย

ผลการประเมินความพร้อมของบีเอสเอไม่ได้มีบทบังคับหรือบทลงโทษกับประเทศไทยโดยตรง ผลการประเมินความพร้อมนี้เป็นเพียงการแสดงออกของภาคธุรกิจเพื่อร้องขอให้รัฐบาลของทุกประเทศทำงานร่วมกันเพื่อส่งเสริมการเข้าถึงและใช้ประโยชน์จากระบบการประมวลผลแบบคลาวด์อย่างทั่วถึง ซึ่งแตกต่างจากการประเมินมาตรฐานความปลอดภัยด้านการบินพลเรือนขององค์การการบินพลเรือนระหว่างประเทศ (ICAO) หรือ การทำประมงผิดกฎหมายของสหภาพยุโรปที่มีบทบังคับหรือบทลงโทษกับประเทศไทยโดยตรง

อย่างไรก็ตาม แม้ว่าผลการประเมินดังกล่าวจะไม่มีบทบังคับหรือบทลงโทษกับประเทศไทยโดยตรง แต่การที่ประเทศไทยสอบตกหลายประเด็นของการประเมินของบีเอสเอและได้รับการจัดอันดับเกือบรั้งท้าย ย่อมส่งผลกระทบโดยตรงต่อความเชื่อมั่นของนักลงทุน ผู้ให้บริการและผู้ใช้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทย นอกจากนี้ หากนักลงทุนประสงค์จะก่อตั้งบริษัทในประเทศไทยและส่งข้อมูลเพื่อทำการติดต่อกับคู่ค้าในประเทศอื่นๆ ที่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานสูงกว่าประเทศไทย การส่งข้อมูลจากประเทศไทยอาจถูกกีดกันหรือทำได้โดยไม่สะดวก อีกทั้งยังส่งผลกระทบต่อความเชื่อมั่นของผู้ประกอบการธุรกิจขนาดย่อม (SMEs) และผู้บริโภคทั่วไปในการใช้บริการระบบการประมวลผลแบบคลาวด์ของประเทศไทยด้วย

บทที่ 4
หลักเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

4.1 ความทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

4.1.1 ความหมายของ “สิทธิในความเป็นอยู่ส่วนตัว” และ “ข้อมูลส่วนบุคคล”

ข้อมูลส่วนบุคคล (Personal Data) จัดเป็นวัตถุแห่งสิทธิประเภทหนึ่งที่รวมอยู่ในเรื่องของสิทธิในความเป็นอยู่ส่วนตัวของบุคคล (Right of Privacy) และเป็นวัตถุที่อยู่ภายใต้การบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยตรง ดังนั้น จึงเห็นสมควรต้องศึกษาความหมายของสิทธิในความเป็นอยู่ส่วนตัว และข้อมูลส่วนบุคคลก่อน ดังนี้

4.1.1.1 สิทธิในความเป็นอยู่ส่วนตัว

สิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่สังคมยุคใหม่เกือบทุกประเทศให้ความสำคัญ สิทธิในความเป็นอยู่ส่วนตัว หมายถึง การจำกัดการเข้าถึงบุคคลโดยบุคคลอื่นเพื่อมิให้ผู้อื่นทราบข้อมูลที่เกี่ยวข้องกับตนเอง หรือเพื่อมิให้ทราบว่าตนเป็นใคร ชื่อเสียงเรียงนามว่าอย่างไร รวมทั้งเพื่อกีดกันหวงห้ามมิให้ผู้อื่นมาอยู่ใกล้ชิดตนเองในทางกายภาพ ซึ่งจากความหมายดังกล่าว สิทธิในความเป็นอยู่ส่วนตัวจะครอบคลุมถึงสิทธิต่าง ๆ หลายประการคือ[1]

(1) ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy)

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูล หมายถึง การให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

(2) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy)

สิทธิในความเป็นส่วนตัวในชีวิตร่างกาย หมายถึง การให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว เช่น การทดลองยา หรือ การทดลองทางพันธุกรรม เป็นต้น

---

[1] สุภัทท์ บุญญานนท์, “คำอธิบายกฎหมายไอทีในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....,” สรรพากรสาส์น, ฉบับที่ 12, ปีที่ 49, น.66, (ธันวาคม 2545).

(3) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)

สิทธิในความเป็นส่วนตัวในการติดต่อสื่อสาร หมายถึง การให้ความคุ้มครองในความปลอดภัยและความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้ไม่ได้

(4) ความเป็นส่วนตัวในเคหสถาน (Territorial Privacy)

สิทธิในความเป็นส่วนตัวในเคหสถาน หมายถึง การกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในเคหสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวิดีโอและการตรวจสอบรหัสประจำตัวบุคคลด้วย

4.1.1.2 ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลตามพจนานุกรมฉบับราชบัณฑิตยสถาน หมายถึง ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน[2]

ข้อมูลส่วนบุคคลตามกฎเกณฑ์ของกลุ่มสหภาพยุโรป (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) หมายถึง ข้อมูลใดๆ ที่สามารถระบุตัวหรืออาจจะระบุตัวตนของบุคคลนั้นได้ (เจ้าของข้อมูล) ซึ่งบุคคลที่อาจระบุตัวตนได้ไม่ว่าโดยทางตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะตัวของบุคคลหรือจากปัจจัยอื่นๆ ที่มีลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสภาพสังคมของบุคคลนั้น เป็นต้น[3]

ข้อมูลส่วนบุคคลตามแนวปฏิบัติและข้อแนะนำขององค์การความร่วมมือทางเศรษฐกิจและการพัฒนาว่าด้วยการคุ้มครองความเป็นอยู่ส่วนตัวและการส่งโอนข้อมูล

---

[2] ราชบัณฑิตยสถาน, “พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๕๔,” สืบค้นเมื่อวันที่ 30 ธันวาคม 2559, จาก http://www.royin.go.th/dictionary/

[3] Article 2(a): ‘Personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

ส่วนบุคคลข้ามประเทศ ค.ศ. 1980 หมายถึง ข้อมูลข่าวสารใดๆ ที่เกี่ยวกับตัวบุคคลธรรมดาที่ระบุตัวหรืออาจระบุตัวบุคคลได้

ข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หมายถึง ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีหมายเลข รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้ความหมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

ข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) หมายถึง ข้อมูลเกี่ยวกับตัวบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับที่เสนอโดยคณะรัฐมนตรีซึ่งนางสาว ยิ่งลักษณ์ ชินวัตร ดำรงตำแหน่งเป็นนายกรัฐมนตรี) หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้ความหมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมด้วย

ข้อมูลส่วนบุคคลตามคำพิพากษาศาลฎีกาที่ 4126/2543 หมายถึง สิ่งที่แสดงถึงเรื่องราวความเป็นมาที่เกี่ยวพันกับชีวิตความเป็นอยู่ของบุคคลหนึ่งบุคคลใดอันเป็นเรื่องราวเฉพาะตัวของบุคคลผู้นั้นซึ่งจำแนกให้เห็นความแตกต่างจากเรื่องราวของบุคคลอื่น ทั้งนี้ ไม่ว่าจะบันทึกหรือทำให้ปรากฏในเอกสารหรือวัตถุใดๆ

ข้อมูลส่วนบุคคลตามความเห็นของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร (ตามคำวินิจฉัยที่ สค 1/2541, สค1/2542 และสค 8/2542) หมายถึง ข้อมูลฐานะการเงิน ประวัติสุขภาพ ประวัติการทำงาน บันทึกสรุปประวัติและพฤติการณ์ของบุคคล และประวัติอาชญากรรมของบุคคล[4]

[4] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,” วารสารนิติศาสตร์, เล่มที่ 4, ปีที่ 34, น.634, (ธันวาคม 2547).

จากบทนิยามดังกล่าวข้างต้นจะเห็นได้ว่าข้อมูลส่วนบุคคลมักจะประกอบด้วย 2 องค์ประกอบหลัก ได้แก่ องค์ประกอบด้านเนื้อหาและองค์ประกอบด้านรูปแบบ ดังนี้[5]

(1) องค์ประกอบด้านเนื้อหา

ข้อมูลข่าวสารส่วนบุคคลจะประกอบด้วยข้อมูลลักษณะหนึ่งหรือหลายลักษณะ คือ (ก) ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น ชื่อ ที่อยู่ เพศ อาชีพ (ข) ข้อมูลที่บ่งบอกให้รู้ตัวผู้นั้น เช่น รหัสหรือเลขประจำตัวประชาชน ลักษณะทางกายภาพ เช่นลายพิมพ์นิ้วมือ รหัสดีเอ็นเอ หรือสิ่งบ่งชี้อื่นๆ เช่น จดหมายอิเล็กทรอนิกส์ (Email address) หมายเลขโทรศัพท์ส่วนบุคคล เป็นต้น หรือ (ค) ข้อมูลที่เป็นความลับของบุคคล เช่น เชื้อชาติ ประวัติทางวินัย ประวัติทางการแพทย์หรือสุขภาพอนามัย ประวัติทางอาชญากรรม ข้อมูลทางการเงินและหนี้สิน ข้อมูลเชิงทัศนคติของบุคคล เช่น ความเชื่อทางการเมือง การปกครอง การนับถือศาสนา หรือรสนิยมในเรื่องต่างๆ

(2) องค์ประกอบด้านรูปแบบ

ข้อมูลส่วนบุคคลมักจะเป็นข้อมูลที่มีการจัดเก็บหรือประมวลขึ้นมาอย่างเป็นระบบโดยบุคคลเจ้าของข้อมูลนั้นหรือบุคคลอื่นๆ เพื่อจะให้สามารถสื่อเรื่องราวหรือความหมายอย่างใดอย่างหนึ่งออกมาได้โดยผ่านทางวิธีการใดวิธีการหนึ่ง เช่น การบันทึกในแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ หรือ การบันทึกภาพ บันทึกเสียง หรือการบันทึกโดยอาศัยเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่น เป็นต้น

กล่าวโดยสรุป ข้อมูลส่วนบุคคลมีลักษณะเป็นวัตถุแห่งสิทธิประการหนึ่ง ได้แก่ สิทธิในความเป็นอยู่ส่วนตัวประเภทความเป็นส่วนตัวเกี่ยวกับข้อมูลที่บุคคลอื่นจะมาล่วงรู้โดยไม่ได้รับอนุญาตไม่ได้ ทั้งนี้ ข้อมูลส่วนบุคคลมักจะเป็นข้อมูลที่บ่งบอกลักษณะเฉพาะของบุคคลนั้นๆ ซึ่งบางครั้งข้อมูลส่วนบุคคลอาจมีลักษณะเป็นความลับหรือไม่เป็นความลับก็ได้เช่นเดียวกัน

4.1.2 ระบบกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ในยุคที่ข้อมูลส่วนบุคคลจำนวนมากสามารถส่งถึงกันได้ผ่านเครือข่ายอินเทอร์เน็ตส่งผลให้บุคคลต่างหันมาให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของตน ในปัจจุบันการคุ้มครองข้อมูลส่วนบุคคลนั้นก็มีหลายแนวทางในการคุ้มครอง อาทิ การพัฒนาเทคโนโลยีขึ้นเพื่อให้ความคุ้มครองข้อมูลส่วนบุคคล การอาศัยซอฟต์แวร์ในการป้องกันการละเมิดส่วนบุคคล

---

[5] *เพิ่งอ้าง*, น.627.

หรือ การออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ การออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลมีลักษณะเป็นแนวทางในการคุ้มครองที่อ้อมเมื่อเทียบกับการอาศัยเทคโนโลยีในการป้องกันข้อมูลส่วนบุคคล อย่างไรก็ตาม การออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลกลับเป็นวิธีการหนึ่งที่จะสามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ เนื่องจากการออกกฎหมายเพื่อใช้บังคับจะเป็นการทำให้ผู้ที่ล่วงละเมิดข้อมูลส่วนบุคคลของคนอื่นจะเกิดความเกรงกลัวไม่มากก็น้อย อีกทั้งยังมีมาตรการในการดำเนินการหากตรวจพบการละเมิดข้อมูลส่วนบุคคลอีกด้วย

แนวคิดในการคุ้มครองข้อมูลส่วนบุคคลโดยการออกกฎหมายนั้นมิได้เพิ่งเกิดขึ้นในยุคที่อินเทอร์เน็ตมีบทบาทต่อชีวิตประจำวันของผู้คน แต่ได้เกิดขึ้นมาอย่างยาวนานโดยปรากฏอยู่ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนซึ่งถือเป็นมาตรฐานขั้นต่ำของมนุษยชาติที่ได้รับการยอมรับกันทั่วโลกตั้งแต่ พ.ศ. 2491 ดังที่ปรากฏในข้อ 12 ที่ระบุว่า “บุคคลใดๆ จะถูกแทรกสอดโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถานหรือในการสื่อสาร หรือจะถูกหลบหลู่ในเกียรติและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกสอดหรือการหลบหลู่ดังกล่าวนั้น” ดังนั้น หลายประเทศรวมทั้งองค์กรระหว่างประเทศจึงหันมาออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อบังคับใช้ในประเทศของตน

ทั้งนี้ โดยทั่วไปในประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลโดยการตราเป็นกฎหมายออกใช้บังคับนั้น จะสามารถแบ่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลออกเป็น 2 ระบบด้วยกัน ได้แก่[6]

(1) ระบบกฎหมายกลาง (Comprehensive and Coded law)

ระบบที่บัญญัติกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายกลางเป็นระบบที่ได้รับความนิยมเป็นอย่างมากในกลุ่มประเทศสหภาพยุโรปโดยหมายถึงระบบกฎหมายที่รวบรวมเอาหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลทุกเรื่อง ทุกกิจกรรมที่กระทำโดยหน่วยงานของรัฐ ภาคธุรกิจหรือเอกชน มาบัญญัติไว้ในกฎหมายกลาง ดังนั้น ในประเทศที่มีกฎหมายกลางนั้น กฎหมายกลางจะให้หลักประกันขั้นต่ำสุดแก่การคุ้มครองข้อมูลส่วนบุคคล แต่หากมีกฎหมายเฉพาะหรือกฎหมายใดหรือหน่วยงานใดกำหนดหลักเกณฑ์วิธีการที่ให้หลักประกันแก่ข้อมูลส่วนบุคคลได้มากกว่า กฎหมายหรือหลักเกณฑ์ดังกล่าวย่อมสามารถใช้บังคับแทนกฎหมายกลางได้ ในทางกลับกันหากกฎหมายเฉพาะหรือกฎเกณฑ์ใดให้ความคุ้มครองที่ต่ำกว่า กฎหมายกลางย่อมมีผลใช้บังคับแทน

---

[6] จันทจิรา เอี่ยมมยุรา, *อ้างแล้ว เชิงอรรถที่ 4,* น.657-658.

(2) ระบบกฎหมายเฉพาะ (Sectoral law or ad hoc law)

ระบบกฎหมายเฉพาะเป็นระบบที่บัญญัติรับรองสิทธิในข้อมูลส่วนบุคคลเป็นเรื่องๆ โดยกำหนดไว้ในกฎหมายแต่ละฉบับ ซึ่งประเทศที่ใช้ระบบกฎหมายเฉพาะ ได้แก่ ประเทศสหรัฐอเมริกา เป็นต้น ทั้งนี้ ลักษณะของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาที่มีลักษณะเป็นกฎหมายเฉพาะ จะเป็นการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาโดยสภา Congress ซึ่งจะออกกฎหมายก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือมีการละเมิดความเป็นอยู่ส่วนตัวของประชาชนเกิดขึ้น หากพิจารณาเหตุผลเบื้องต้นในการใช้ระบบกฎหมายเฉพาะของประเทศสหรัฐอเมริกาจะพบว่า ประเทศสหรัฐอเมริกามีที่มาทางประวัติศาสตร์ในการสร้างชาติที่เน้นไม่ให้เจ้าหน้าที่ของรัฐดำเนินการใดๆ ที่จะเป็นการริดรอนสิทธิเสรีภาพของประชาชนและประชาชนก็มีสิทธิดำเนินธุรกิจแบบทุนนิยมได้ ปัจจุบันประเทศสหรัฐอเมริกามีกฎหมายคุ้มครองข้อมูลส่วนบุคคลจำนวนมาก อาทิ The Federal Trade Commission Act (FTC Act), The Privacy Act of 1974, Bank Secrecy Act 1974, The Children's Online Privacy Protection Act ("COPPA"), The Telecommunication Act, The Fair Credit Reporting Act ("FCRA") and Fair Accurate Credit Transactions Act ("FACTA"), The Video Privacy Protection Act เป็นต้น[7]

4.1.3 ความท้าทายในการคุ้มครองข้อมูลส่วนบุคคล

ในปัจจุบันการคุ้มครองข้อมูลส่วนบุคคลได้รับความสนใจจากทุกภาคส่วนไม่ว่าจะเป็นภาครัฐ ภาคเอกชน หรือประชาชนทั่วไปซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นโครงสร้างพื้นฐานประการหนึ่งในการสร้างเศรษฐกิจดิจิทัลของแต่ละประเทศ ข้อมูลส่วนบุคคลเปรียบเสมือนทองคำและสามารถช่วยให้ผู้ประกอบการสามารถวางกลยุทธ์ในการประกอบธุรกิจได้ตรงตามความต้องการของผู้บริโภคได้ ด้วยเหตุนี้ จึงมีผู้ตั้งประเด็นทางกฎหมายเพื่อท้าทายการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันหลายประเด็นดังต่อไปนี้

4.1.3.1 ข้อมูลส่วนบุคคลถือเป็นทรัพยสิทธิหรือบุคคลสิทธิ

ในทางวิชาการมีประเด็นที่เป็นที่ถกเถียงกันอยู่ว่า หากพิจารณาในแง่กฎหมายเอกชน ข้อมูลส่วนบุคคลจะถือเป็นทรัพยสิทธิหรือไม่ ซึ่งการถกเถียงดังกล่าวเกิดขึ้นทั้งใน

---

[7] Aaron P.Simpson and Jenna Rode, "Data Protection 2017 | USA," สืบค้นเมื่อวันที่ 5 มกราคม 2561, จาก https://iclg.com/practice-areas/data-protection/data-protection-2017/usa

ประเทศสหรัฐอเมริกาและในสหภาพยุโรป ตั้งแต่ยุคค.ศ. 1970 - 1979 และได้รับการวิพากษ์วิจารณ์เรื่อยมาอย่างต่อเนื่องจนถึงช่วงยุคค.ศ. 2000 – 2009[8] ทั้งนี้ จากการศึกษาผู้เขียนพบว่าการจะพิจารณาว่าข้อมูลส่วนบุคคลถือเป็นทรัพยสิทธิหรือไม่ จะต้องย้อนกลับไปพิจารณาถึงประวัติความเป็นมาของหลักการคุ้มครองข้อมูลส่วนบุคคล ซึ่งแต่เดิมก่อนที่สหภาพยุโรปจะออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลในปีค.ศ. 1995 นั้น ได้มีการถกเถียงกันว่าข้อมูลส่วนบุคคลควรได้รับการคุ้มครองในรูปแบบใด อาทิ การกำหนดระบบกฎหมายขึ้นมาคุ้มครองข้อมูลส่วนบุคคลโดยมองว่าเป็นสิทธิขั้นพื้นฐาน (Fundamental right) ที่ประชาชนควรจะได้รับดังเช่นที่สหภาพยุโรปดำเนินการ หรือจะใช้ “Property rights Model” ซึ่งเป็นแนวคิดของนักวิชาการฝั่งประเทศสหรัฐอเมริกาโดยมีหลักการสำคัญ 2 ประการ คือ[9]

(1) Property right model จะก่อสิทธิให้แก่เจ้าของข้อมูลในการขายข้อมูลส่วนบุคคลของตนเองให้แก่บุคคลอื่นได้ในลักษณะคล้ายคลึงกับสิทธิในทรัพย์สินทางปัญญา

(2) Property right model จะทำให้บุคคลที่ใช้ข้อมูลส่วนบุคคลขณะนี้ใช้ข้อมูลส่วนบุคคลอย่างจำกัดเนื่องจากภาระค่าใช้จ่ายที่จะเกิดขึ้นจากการได้ข้อมูลมาค่อนข้างสูง ดังนั้น บุคคลผู้ใช้ข้อมูลจึงจำเป็นต้องไตร่ตรองอย่างละเอียดอีกครั้งว่าข้อมูลใดที่จำเป็นต้องใช้ การละเมิดข้อมูลส่วนบุคคลก็จะน้อยลงไปด้วย

เมื่อพิจารณาแนวคิดของ Property right model ข้างต้นย่อมสะท้อนได้ว่าปัจจุบันข้อมูลส่วนบุคคลยังไม่อยู่ในสถานะของทรัพยสิทธิแต่อย่างใด แม้ว่าโดยความรู้สึกของประชาชนทั่วไปจะมองว่าเจ้าของข้อมูลควรจะเป็นเจ้าของข้อมูลของตนเองเพราะเจ้าของข้อมูลย่อมสามารถหวงกันไม่ให้บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของตนได้ตามสิทธิที่กฎหมายรองรับ แต่อย่างไรก็ตาม แม้ว่ากฎหมายจะให้ความคุ้มครองข้อมูลส่วนบุคคลโดยไม่ให้บุคคลอื่นนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปใช้ในทางที่ไม่ควร แต่การให้ความคุ้มครองดังกล่าวก็ไม่ใช่ฐานในการก่อให้เกิดทรัพยสิทธิในข้อมูลส่วนบุคคลแต่อย่างใด เพราะทรัพยสิทธิจะต้องแต่งตั้งขึ้นโดยกฎหมาย

---

[8] Nadezhda Purtova, “Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence,” สืบค้นเมื่อวันที่ 2 กุมภาพันธ์ 2561, จาก https://papers.ssrn.com/sol3/papers.cfm?abstract_Id=1641027

[9] Pamela Samuelson, “Privacy As Intellectual Property? ,” สืบค้นเมื่อวันที่ 2 กุมภาพันธ์ 2561, จาก http://people.ischool.berkeley.edu//~pam/papers/privasip_draft.pdf

เท่านั้น[10] ประกอบกับมุมมองกฎหมายของประเทศสหรัฐอเมริกาที่มีมุมมองว่าไม่มีบุคคลใดสามารถเป็นเจ้าของข้อมูลได้แล้วนั้น ยิ่งแสดงให้เห็นชัดเจนว่าไม่มีบุคคลใดมีทรัพยสิทธิเหนือข้อมูลส่วนบุคคล

อย่างไรก็ตาม หากพิจารณาต่อไปว่าแล้วกฎหมายควรกำหนดให้บุคคลมีทรัพยสิทธิในข้อมูลส่วนบุคคลหรือไม่นั้น ในระยะหลังมานี้มีนักวิชาการหลายท่านสนับสนุนแนวทางดังกล่าว[11] โดยมองว่ากฎหมายควรกำหนดให้บุคคลมีทรัพยสิทธิเหนือข้อมูลส่วนบุคคล เพราะว่าการดำเนินการเช่นว่านั้นจะสามารถคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งกว่า โดยให้บุคคลซึ่งเป็นเจ้าของข้อมูลมีโอกาสต่อรองกับอีกฝ่ายหากเจ้าของข้อมูลต้องการขายข้อมูลส่วนบุคคลของตนเองให้แก่อีกฝ่ายหนึ่งเพื่อให้ตนเองได้รับผลตอบแทนที่คุ้มค่ากับข้อมูลนั้น ในขณะที่ฝ่ายที่ได้รับข้อมูลส่วนบุคคลไป ก็จะตระหนักถึงคุณค่าของข้อมูลมากขึ้น เพราะมีต้นทุนในการได้ข้อมูลส่วนบุคคลมาและสามารถเข้าถึงข้อมูลส่วนบุคคลได้ตรงจุดมากยิ่งขึ้น ดังนั้น วิธีการนี้จึงทำให้เกิดความเท่าเทียมกันในตลาดข้อมูลและเป็นการรองรับสิทธิในความเป็นส่วนตัวได้ดียิ่งกว่าระบบการคุ้มครองข้อมูลส่วนบุคคลปัจจุบัน

เมื่อเจ้าของข้อมูลไม่มีทรัพยสิทธิเหนือข้อมูลส่วนบุคคล ย่อมเกิดคำถามต่อไปว่าแล้วเจ้าของข้อมูลมีสิทธิใดเหนือข้อมูลส่วนบุคคล มีบุคคลสิทธิเหนือข้อมูลส่วนบุคคลนั้นหรือไม่นั้น ผู้เขียนมีความเห็นว่า เมื่อบุคคลสิทธิ หมายถึง สิทธิซึ่งมีวัตถุแห่งสิทธิเป็นการกระทำหรืองดเว้นกระทำ จึงเป็นสิทธิเรียกร้องที่บังคับเอาแก่ตัวบุคคลโดยเฉพาะเจาะจง ซึ่งโดยทั่วไปมักจะเป็นหนี้ที่จะต้องปฏิบัติตามความตกลงที่ทำกันไว้[12] ดังนั้น ในบางกรณีที่เจ้าของข้อมูลเข้าทำสัญญาใช้บริการหรือสัญญาเปิดเผยข้อมูลกับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลอาจมีบุคคลสิทธิเหนือข้อมูลดังกล่าวได้โดยอาศัยสัญญาที่ได้กระทำระหว่างกัน ซึ่งจะส่งผลให้เจ้าของข้อมูลสามารถบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการหรืองดดำเนินการใดๆ ตามสัญญาได้

กล่าวโดยสรุป กรณีนี้ยังคงต้องศึกษาต่อไปในอนาคตว่านอกเหนือจากสิทธิในความเป็นส่วนตัวที่เจ้าของข้อมูลมีเหนือข้อมูลส่วนบุคคลตามรัฐธรรมนูญแล้ว เจ้าของข้อมูล

---

[10] Nadezhda Purtorva, “Illusion of Personal Data as No One's Property,” สืบค้นเมื่อวันที่ 2 กุมภาพันธ์ 2561, จาก https://papers.ssrn.com/sol3/papers.cfm?abstract_Id=2346693

[11] Pamela Samuelson, *supra note 14*, p.6.

[12] ศรีราชา เจริญพานิช, คำอธิบายกฎหมายว่าด้วยทรัพย์สิน, พิมพ์ครั้งที่ 5, (กรุงเทพฯ : วิญญูชน, 2557), น.82-83.

จะมีทรัพยสิทธิหรือบุคคลสิทธิเหนือข้อมูลส่วนบุคคลอีกหรือไม่ ซึ่งในเบื้องต้นผู้เขียนมีความเห็นเจ้าของข้อมูลส่วนบุคคลไม่มีทรัพยสิทธิหรือบุคคลสิทธิเหนือข้อมูลส่วนบุคคลเป็นการทั่วไปทุกกรณี

4.1.3.2 การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายการแข่งขันทางการค้า (Competition Law)[13]

ในยุคปัจจุบันรัฐบาลหลายประเทศให้ความสำคัญกับเศรษฐกิจโดยการส่งเสริมให้เกิดเศรษฐกิจดิจิทัลภายในประเทศขึ้น ทั้งนี้ ปัจจัยสำคัญที่จะทำให้เศรษฐกิจดิจิทัลประสบความสำเร็จได้ คือ ข้อมูลส่วนบุคคล เนื่องจากการประกอบธุรกิจในยุคดิจิทัล ผู้ประกอบธุรกิจต้องใช้ข้อมูลส่วนบุคคลจำนวนมากเป็นเครื่องมือในการทำธุรกิจโดยนำข้อมูลส่วนบุคคลมาจัดเก็บอย่างเป็นระบบและนำไปวิเคราะห์เพื่อประโยชน์ในการวางกลยุทธ์หรือเพิ่มทางเลือกการใช้บริการให้แก่ลูกค้า โดยลูกค้าสามารถนำข้อมูลส่วนบุคคลมาเป็นสิ่งตอบแทนในการใช้บริการโดยไม่คิดค่าตอบแทน ดังเช่นกรณีการให้บริการสื่อสังคมออนไลน์ของ Facebook เป็นต้น

แม้ว่ารัฐบาลจะพยายามสนับสนุนเศรษฐกิจดิจิทัลเพียงใด รัฐบาลยังคงมีหน้าที่ต้องให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชนอยู่ดี เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลถือเป็นสิทธิและเสรีภาพขั้นพื้นฐานของประชาชนที่รัฐจะละเลยไม่ได้ ดังนั้น เครื่องมือหนึ่งที่รัฐนำมาใช้ในการคุ้มครองข้อมูลส่วนบุคคลตามสิทธิเสรีภาพของประชาชนและในขณะเดียวกันก็ส่งเสริมเศรษฐกิจดิจิทัลไปพร้อมๆ กัน ก็คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคลในยุคปัจจุบันถูกออกแบบให้รองรับสิทธิเสรีภาพของประชาชน แต่ในขณะเดียวกันก็ไม่ทำลายหรือขัดขวางการเกิดขึ้นของเศรษฐกิจดิจิทัลซึ่งจำเป็นต้องอาศัยข้อมูลส่วนบุคคลในการพัฒนา ตัวอย่างกฎหมายที่มีการผสมผสานทั้งสองสิ่งข้างต้นเข้าด้วยกันอย่างลงตัว ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป (General Data Protection Regulation: GDPR)

นอกเหนือจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว รัฐบาลบางประเทศยังอาศัยกฎหมายแข่งขันทางการค้า (Compettition Law) เป็นเครื่องมืออีกหนึ่งช่องทางในการคุ้มครองข้อมูลส่วนบุคคลและส่งเสริมเศรษฐกิจดิจิทัล ยกตัวอย่างเช่น กรณีที่สำนักงานป้องกันการผูกขาดทางการค้าของประเทศเยอรมนี (Bundeskartellamt) ได้มีคำวินิจฉัยเมื่อวันที่ 19 ธันวาคม 2560 ที่ผ่านมาว่า Facebook ใช้อำนาจเหนือตลาดที่ตนเองมีอยู่เหนือตลาดในการ

---

[13] กนกนัย ถาวรพาริช, “บทเรียนจากข่าวฉาวเฟซบุ๊กถึงไทย : การคุ้มครองข้อมูลส่วนบุคคลด้วยกฎหมายแข่งขันทางการค้า,” สืบค้นเมื่อวันที่ 21 มิถุนายน 2561, จาก https://www.the101.world/privacy_and_trade_competition_act/

ให้บริการ Social Network ไปในทางที่ผิดโดยการกำหนดข้อตกลงการเข้าใช้บริการ (terms and conditions) ในลักษณะ “Take it or Leave it” ให้ผู้ใช้บริการต้องยินยอมเปิดเผยข้อมูลส่วนบุคคลทุกอย่างที่เกิดขึ้นระหว่างการใช้ Facebook หากผู้ใช้บริการไม่ยินยอมจะไม่สามารถใช้บริการ Facebook ได้ เช่น กรณีที่ผู้ใช้บริการใช้บริการ Website หรือ Application อื่นที่เชื่อมโยงบริการเข้ากับ Facebook โดยการฝังปุ่ม Like/Share ไว้ใน Website หรือ Application นั้นๆ หรือโดยการให้ผู้ใช้บริการล็อกอินเข้าใช้บริการผ่านทางบัญชี Facebook ผู้ใช้บริการต้องยินยอมเปิดเผยข้อมูลจาก Website หรือ Application ดังกล่าวให้แก่ Facebook ด้วย ซึ่งสำนักงานป้องกันการผูกขาดทางการค้าของเยอรมนีพิจารณาว่าผู้ใช้บริการไม่สามารถเลือกได้ว่าจะเปิดเผยข้อมูลกับ Facebook ได้ในปริมาณแค่ไหน ดังนั้น ข้อตกลงการใช้บริการดังกล่าวจึงเป็นข้อตกลงที่ไม่เป็นธรรม

จากคำวินิจฉัยของสำนักงานป้องกันการผูกขาดทางการค้าของเยอรมนีจะแสดงให้เห็นได้ว่าประเทศเยอรมนีนำกฎหมายแข่งขันทางการค้ามาให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ Facebook อีกทางหนึ่งนอกเหนือจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของเยอรมนี ซึ่งการดำเนินการดังกล่าวมีทั้งผู้ที่เห็นด้วยและไม่เห็นด้วยกับการใช้กฎหมายแข่งขันทางการค้าในการคุ้มครองข้อมูลส่วนบุคคล โดยฝ่ายที่เห็นด้วยและสนับสนุนการใช้กฎหมายแข่งขันทางการค้ามาเป็นเครื่องมือในการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นว่า การใช้กฎหมายแข่งขันทางการค้ามาใช้คุ้มครองข้อมูลส่วนบุคคลจะส่งเสริมให้เกิดตลาดที่มีการแข่งขันกันในระดับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะเช่นเดียวกับการแข่งขันเรื่องราคาและคุณภาพของสินค้าและบริการโดยทั่วไป ในขณะที่ฝ่ายที่ไม่เห็นด้วยและไม่สนับสนุนให้นำกฎหมายแข่งขันทางการค้ามาเป็นเครื่องมือในการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นว่า กฎหมายแข่งขันทางการค้าไม่มีเครื่องมือหรือกลไกที่เพียงพอในการคุ้มครองข้อมูลส่วนบุคคลและควรปล่อยให้เป็นเรื่องของกฎหมายคุ้มครองข้อมูลส่วนบุคคลมากกว่า เนื่องจากบุคคลกลุ่มนี้มองว่าในมุมมองของผู้ใช้บริการระดับการคุ้มครองข้อมูลส่วนบุคคลอาจไม่ใช่สิ่งที่ผู้ใช้บริการคำนึงถึงเมื่อเลือกใช้บริการก็ได้ หรือแม้ให้ความสำคัญกับระดับการคุ้มครองข้อมูลส่วนบุคคลแต่ก็อาจยอมแลกข้อมูลส่วนบุคคลของตนเองกับการให้บริการโดยไม่คิดค่าตอบแทนของผู้ให้บริการได้ ดังนั้น เมื่อผู้ใช้บริการยินยอมจะละทิ้งการคุ้มครองข้อมูลส่วนบุคคลของตนเองไปแล้ว การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ใช่เรื่องที่ผู้ให้บริการต้องคำนึงถึงเมื่อแข่งขันในตลาด ประกอบกับหากกฎหมายแข่งขันทางการค้ามีวัตถุประสงค์เรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วยแล้ว ขอบเขตของกฎหมายจะไม่มีที่สิ้นสุดและอาจถูกนำมาใช้เพื่อควบคุมผู้มีอำนาจเหนือตลาดในทุกๆ เรื่อง รวมทั้งอาจเข้าไปควบคุมการกระทำที่อาจขัดต่อกฎหมายอื่นที่ไม่ใช่เรื่องการแข่งขันโดยตรงเพื่อแสวงหาข้อได้เปรียบทางการแข่งขันเหนือคู่แข่ง (Competitive Advantage

through violation of the law) ด้วย ดังนั้น หากมีกฎหมายเฉพาะเรื่องอยู่แล้ว กฎหมายแข่งขันทางการค้าก็ไม่ควรก้าวล่วง

สำหรับมุมมองของผู้เขียน ผู้เขียนมองว่าการที่รัฐจะอาศัยกฎหมายหลายแขนงเป็นเครื่องมือในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนย่อมเป็นเจตนาที่ดีและควรสนับสนุน แต่อย่างไรก็ตาม ในทางปฏิบัติจะบังคับใช้อย่างไร เป็นประเด็นที่ยังคงต้องศึกษาต่อไปในอนาคต

4.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับสากลที่บีเอสเอยอมรับ

หลักเกณฑ์คุ้มครองข้อมูลส่วนบุคคลที่บีเอสเอให้การยอมรับโดยนำเอามาเป็นเกณฑ์ในการพิจารณาจะเป็นหลักเกณฑ์ที่จะใช้ในการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ โดยไม่ครอบคลุมถึงข้อมูลความลับทางการค้า ข้อมูลทั่วๆ ไป หรื Big Data ซึ่งมีกฎหมายอื่นให้ความดูแลคุ้มครองอยู่แล้ว ทั้งนี้ หลักเกณฑ์ที่บีเอสเอให้การยอมรับ ได้แก่ แนวปฏิบัติและข้อแนะนำตามองค์กรความร่วมมือทางเศรษฐกิจในเอเชีย-แปซิฟิก (Asia-Pacific Economic Cooperation: APEC) ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป อย่างไรก็ตาม หากพิจารณาหลักเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลที่ปรากฏในปัจจุบัน จะพบว่าหลักเกณฑ์ในการคุ้มครองข้อมูลในระดับสากลประกอบไปด้วย (1) แนวปฏิบัติและข้อแนะนำองค์การความร่วมมือทางเศรษฐกิจและการพัฒนาว่าด้วยการคุ้มครองความเป็นอยู่ส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามประเทศ ค.ศ.1980 (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) (2) แนวปฏิบัติและข้อแนะนำตามองค์กรความร่วมมือทางเศรษฐกิจในเอเชีย-แปซิฟิก (Asia-Pacific Economic Cooperation: APEC) ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ (3) หลักเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป[14] โดยมีสาระสำคัญดังนี้

[14] อรอมล อาระพล, “หลักการคุ้มครองข้อมูลส่วนบุคคล: กรอบแนวคิดในทางระหว่างประเทศ,” Thailand Economic & Business Review, ฉบับที่ 4, ปีที่12, น.44, (เมษายน 2559).

4.2.1 แนวปฏิบัติและข้อแนะนำองค์การความร่วมมือทางเศรษฐกิจและการพัฒนาว่าด้วยการคุ้มครองความเป็นอยู่ส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามประเทศ ค.ศ. 1980 (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

แนวปฏิบัติและข้อแนะนำองค์การความร่วมมือทางเศรษฐกิจและการพัฒนาว่าด้วยการคุ้มครองความเป็นอยู่ส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามประเทศ ค.ศ. 1980 หรือ “OECD Guidelines 1980” จัดทำขึ้นครั้งแรกในปีค.ศ. 1979[15] โดยองค์การเพื่อความร่วมมือทางเศรษฐกิจและพัฒนาซึ่งเป็นองค์กรที่จัดตั้งขึ้นตั้งแต่ปีค.ศ. 1961 เพื่อส่งเสริมและสนับสนุนนโยบายที่ส่งผลต่อการพัฒนาเศรษฐกิจและความเป็นอยู่ที่ดีทางสังคมของประชากรทั่วโลกและเพื่อสนับสนุนให้รัฐบาลของประเทศสมาชิกสามารถทำงานร่วมกันได้โดยการแบ่งปันประสบการณ์และการค้นหาแนวทางในการแก้ปัญหาร่วมกัน ทั้งนี้ การจัดทำแนวปฏิบัติ OECD Guidelines 1980 ขึ้นนั้นก็เพื่อวางกรอบการคุ้มครองข้อมูลส่วนบุคคลและเพื่อเป็นเครื่องมือในการสร้างความเป็นอันหนึ่งอันเดียวกันของประเทศสมาชิกของ OECD ที่มีกว่า 34 ประเทศ เพราะความไม่เท่าเทียมกันของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศนั้นก่อให้เกิดปัญหาเกี่ยวกับการไหลเวียนของข้อมูลข่าวสารระหว่างประเทศและส่งผลกระทบโดยตรงต่อการค้าระหว่างประเทศ ทั้งนี้ ภายใต้ OECD Guidelines 1980 ปรากฏหลักการคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นแนวปฏิบัติขั้นต่ำ เพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติภายในแต่ละประเทศ โดยไม่แบ่งแยกว่าเป็นแนวปฏิบัติของเอกชนหรือภาครัฐ[16] หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ OECD ประกอบด้วยหลักการสำคัญ 8 ประการดังต่อไปนี้[17]

---

[15] Chris Reed, Computer Law, Seventh Edition, (New York, Oxford University Press Inc., 2011), p.580.

[16] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, (กรุงเทพฯ: พี.เพรส, 2557), น.147.

[17] OECD, “THIRTY YEARS AFTER THE OECD PRIVARY GUIDELINES,” สืบค้นเมื่อวันที่ 20 ตุลาคม 2559, จาก http://www.oecd.org/sti/ieconomy/49710223.pdf

4.2.1.1 หลักข้อจำกัดในการเก็บรวบรวมข้อมูลส่วนบุคคล (Collection Limitation Principle)

OECD Guidelines 1980 กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมายและเป็นธรรม โดยเจ้าของข้อมูลส่วนบุคคลจะต้องรับรู้หรือให้ความยินยอมในการเก็บรวบรวมส่วนบุคคลของตนด้วย

4.2.1.2 หลักคุณภาพของข้อมูล (Data Quality Principle)

OECD Guidelines 1980 กำหนดให้ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมจะต้องเกี่ยวข้องและจำเป็นตามวัตถุประสงค์ที่จะนำไปใช้ ทั้งนี้ ข้อมูลส่วนบุคคลที่เก็บรวบรวมจะต้องเป็นข้อมูลที่มีคุณภาพ กล่าวคือ เป็นข้อมูลที่ถูกต้อง สมบูรณ์และทันสมัยด้วย

4.2.1.3 หลักการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูล (Purpose Specification Principle)

OECD Guidelines 1980 กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องกำหนดวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลให้ชัดเจนว่าการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวดำเนินการโดยมีวัตถุประสงค์เพื่ออะไร ทั้งนี้ วัตถุประสงค์ดังกล่าวจะต้องถูกระบุไว้อย่างช้าที่สุด คือเมื่อจะจัดเก็บข้อมูล

4.2.1.4 หลักข้อจำกัดในการใช้ข้อมูล (Use Limitation Principle)

OECD Guidelines 1980 กำหนดให้การใช้ข้อมูลจะต้องเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ การใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ที่กำหนดไว้ย่อมไม่สามารถกระทำได้ เว้นเสียแต่ว่าจะได้รับความยินยอมจากเจ้าของข้อมูลหรือเมื่อมีกฎหมายอนุญาตให้ทำได้

4.2.1.5 หลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguards Principle)

OECD Guidelines 1980 กำหนดให้ผู้ที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลให้เพียงพอเพื่อป้องกันความเสียหาย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตด้วย

4.2.1.6 หลักการเปิดเผยข้อมูลส่วนบุคคล (Openness Principle)

OECD Guidelines 1980 กำหนดให้ต้องมีการกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผย หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูลโดยไม่กระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลด้วย

4.2.1.7 หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

OECD Guidelines 1980 กำหนดให้เจ้าของข้อมูลต้องมีส่วนร่วมกับการจัดเก็บข้อมูลส่วนบุคคล โดยมีสิทธิต่างๆ ดังนี้[18]

1. สิทธิรับรู้หรือได้รับการยืนยันจากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลได้มีการจัดเก็บข้อมูลส่วนบุคคลของตนอยู่หรือไม่

2. สิทธิได้รับแจ้งจากผู้ควบคุมข้อมูลภายในระยะเวลาที่เหมาะสม ด้วยวิธีการที่เหมาะสมและเข้าใจง่าย โดยค่าธรรมเนียมการแจ้งจะต้องเป็นธรรม (กรณีที่มีการจัดเก็บข้อมูลส่วนบุคคล)

3. สิทธิรับรู้เหตุผลในการปฏิเสธคำร้องขอตามสิทธิของตนและสิทธิอุทธรณ์คัดค้านคำปฏิเสธดังกล่าว

4. สิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง หากมีการพิจารณาและเห็นชอบตามคำอุทธรณ์ของผู้คัดค้านแล้ว จะต้องมีการลบล้างแก้ไข เปลี่ยนแปลง หรือทำข้อมูลให้สมบูรณ์ ตามที่มีมติในการพิจารณาอุทธรณ์นั้น

4.2.1.8 หลักความรับผิดชอบ (Accountability Principle)

OECD Guidelines 1980 กำหนดให้ผู้ที่จัดเก็บข้อมูลส่วนบุคคลเอาไว้หรือผู้ควบคุมข้อมูลจะต้องกำหนดความรับผิดในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลเอาไว้ด้วย และผู้ควบคุมข้อมูลจะต้องปฏิบัติตามมาตรการที่เกี่ยวข้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines 1980 เช่นกัน

---

[18] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ, (กรุงเทพฯ: สำนักพิมพ์นิติธรรม, 2555), น.246.

4.2.2 แนวปฏิบัติและข้อแนะนำตามองค์กรความร่วมมือทางเศรษฐกิจในเอเชีย-แปซิฟิก (Asia-Pacific Economic Cooperation: APEC) ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ความร่วมมือทางเศรษฐกิจในเอเชีย-แปซิฟิก หรือ APEC ได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลเนื่องจากข้อมูลส่วนบุคคลเกี่ยวข้องกับการดำเนินธุรกิจการค้าในปัจจุบันเป็นอย่างมาก ดังนั้น คณะกรรมการเกี่ยวกับการค้าอิเล็กทรอนิกส์ (APEC's Electronic Commerce Steering Group: ECSG) จึงได้สร้างหลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการค้าขายทางอิเล็กทรอนิกส์ (Electronic commerce) ขึ้นโดยใช้ชื่อเรียกว่า "APEC Privacy Framework" เพื่อเป็นแนวทางในการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สมบูรณ์ของประเทศสมาชิกในระหว่างปี ค.ศ. 2003 ถึง ค.ศ. 2004 จนท้ายที่สุดที่ประชุมคณะรัฐมนตรีของ APEC ครั้งที่ 16 จึงได้ลงมติรับหลักการของ APEC Privacy Framework ในปีค.ศ. 2004 ทั้งนี้ เพื่อการรักษาสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นสิทธิในความเป็นส่วนตัวกับความต้องการในการเก็บ ประมวลผล ใช้ เผยแพร่ รับ-ส่ง หรือแลกเปลี่ยนข้อมูลส่วนบุคคลของธุรกิจภาคเอกชน[19]

APEC Privacy Framework ถูกยกร่างขึ้นโดยแบ่งออกเป็น 4 ส่วน ได้แก่ บทนำ ขอบเขต หลักการที่สำคัญ และการอนุวัติการ โดยมีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อพัฒนาการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม
2. เพื่อป้องกันการสร้างข้อจำกัดในการไหลเวียนของข้อมูล
3. เพื่อเปิดช่องทางให้ธุรกิจข้ามชาติสามารถรับเอาวิธีการในการเก็บรวบรวม ใช้และประมวลผลข้อมูลมาใช้ในกิจการของตนได้
4. เพื่ออำนวยความสะดวกให้แก่ประเทศต่างๆ ในการส่งเสริมหรือบังคับการคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม ภายหลังการยกร่างคณะกรรมการ ECSG จึงได้เพิ่มเติมประเด็นเรื่องการโอนหรือส่งข้อมูลระหว่างประเทศ (Data Export) เข้าไปในหมวดของการอนุวัติการส่งผลให้ APEC Privacy Framework เสร็จสมบูรณ์ในปีค.ศ. 2005

---

[19] จอมพล พิทักษ์สันตโยธิต, "APEC privacy framework กับความพร้อมด้านกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย," บทบัณฑิตย์, เล่มที่ 70, น.136, (2557).

4.2.2.1 ขอบเขต

APEC Privacy Framework กำหนดแนวปฏิบัติสำหรับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล (ไม่ใช้กับข้อมูลอื่นๆ เช่น ข้อมูลความลับทางการค้า ข้อมูลทั่วๆ ไป หรือ Big Data) โดยผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นบุคคลธรรมดาหรือองค์กรที่ควบคุมการเก็บรวบรวม ถือครอง ประมวลผล หรือใช้ข้อมูลส่วนบุคคล รวมทั้งบุคคลที่มีคำสั่งให้แก่บุคคลอื่นในการดำเนินการเช่นว่านั้นด้วย[20] (บุคคลหรือองค์กรที่ทำหน้าที่ตามคำสั่งของบุคคลข้างต้นไม่ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายนี้) ทั้งนี้ ภายใต้ APEC Privacy Framework ข้อมูลส่วนบุคคล หมายถึง ข้อมูลส่วนตัวของบุคคลธรรมดา (ไม่รวมถึงนิติบุคคล)[21] ตัวอย่างเช่น กรุ๊ปเลือด การวิเคราะห์พันธุกรรม (DNA) ลายพิมพ์นิ้วมือ เป็นต้น โดยไม่ได้หมายความเฉพาะเจาะจงว่าต้องเป็นข้อมูลชิ้นใด ดังนั้น จึงให้ความคุ้มครองถึงข้อมูลหลายๆ ชิ้น ซึ่งแต่ละชิ้นอาจจะไม่สามารถระบุตัวตนของบุคคลได้ แต่เมื่อนำมารวมกันจะสามารถใช้ระบุตัวตนของบุคคลได้

อย่างไรก็ตาม ขอบเขตของ APEC Privacy Framework จะไม่ใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลที่เก็บรวบรวม รักษาและประมวลผลข้อมูลส่วนบุคคลที่มีจุดประสงค์เกี่ยวกับกิจการส่วนตัว ครอบครัว หรือกิจกรรมในบ้าน เช่น การทำรายชื่อ หมายเลขโทรศัพท์ ที่อยู่ หรือการมีบัญชีรายชื่อของสมาชิกในตระกูล และจะไม่ใช้บังคับกับข้อมูลส่วนบุคคลที่มีลักษณะเป็นข้อมูลสาธารณะ เช่น ข้อมูลส่วนบุคคลที่หน่วยงานรัฐจัดเก็บอยู่ ข้อมูลในรายงานของสื่อ หรือข้อมูลที่ศาลสั่งให้เปิดเผยต่อสาธารณะ เป็นต้น[22]

อนึ่ง APEC Privacy Framework จะไม่บังคับใช้ในกรณีที่บุคคลธรรมดาหรือองค์กรซึ่งอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวม ถือครอง ประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ส่วนตน หรือเพื่อครอบครัวหรือเพื่อกิจการในครัวเรือน

---

[20] *เพิ่งอ้าง,* น.145.

[21] Definitions:

9. Personal information means any information about an identified or identifiable individual.

[22] จอมพล พิทักษ์สันตโยธิต, *อ้างแล้ว เชิงอรรถที่ 20,* น.146.

4.2.2.2 หลักการสำคัญของ APEC Privacy Framework

หลักการสำคัญของ APEC Privacy Framework เป็นหลักการที่กำหนดโดยเทียบเคียงมาจากหลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD Guidelines 1980 ตามที่ได้อธิบายไว้ ณ ข้างต้น โดยมีรายละเอียดดังต่อไปนี้[23]

(1) หลักการป้องกันความเสียหาย (Preventing Harm)

เพื่อที่จะคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องมีหลักการป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการใช้ข้อมูลส่วนบุคคลโดยมิชอบหรือใช้ข้อมูลส่วนบุคคลดังกล่าวในทางที่ผิด เช่น การกำหนดมาตรการกำกับตนเอง การให้ความรู้ความเข้าใจรวมถึงความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูล เป็นต้น

(2) หลักการแจ้งให้ทราบ (Notice)

ผู้ที่ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงข้อเท็จจริงว่าข้อมูลส่วนบุคคลของตนจะถูกจัดเก็บไว้โดยมีวัตถุประสงค์ตามที่กำหนดและเจ้าของข้อมูลสามารถจำกัดการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของตนได้ รวมถึงแจ้งให้ทราบถึงรายละเอียดของผู้ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ในการจัดเก็บ ข้อมูลว่าจะนำข้อมูลส่วนบุคคลดังกล่าวไปเปิดเผยต่อองค์กรใด เป็นต้น ทั้งนี้ การแจ้งให้ทราบควรเป็นไปก่อนหรือขณะใดๆ ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลโดยใช้ถ้อยคำที่เจ้าของข้อมูลสามารถเข้าใจได้ง่ายด้วย

(3) หลักการจำกัดการจัดเก็บข้อมูลส่วนบุคคล (Limited Collection)

การเก็บรวบรวมข้อมูลส่วนบุคคลจะจำกัดเฉพาะการเก็บรวบรวมตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมเอาไว้แล้วเท่านั้น ทั้งนี้ เนื่องจากหลักความยินยอมถือเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคลโดยภายใต้ APEC Privacy Framework กำหนดให้ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการเก็บรวบรวม รักษาและประมวลผลข้อมูลส่วนบุคคลด้วย

---

[23] Carla Bulford, “Between East and West: The APEC Privacy Framework and the Balance of International Data Flows,” I/S Journal of law and policy for the information society, p.711-717 (2012).

(4) หลักการใช้ข้อมูลส่วนบุคคล (Uses of Personal Information)

การใช้ข้อมูลส่วนบุคคลภายใต้ APEC Privacy Framework จำกัดเฉพาะการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมเอาไว้แล้วเท่านั้น เช่นเดียวกับกรณีของการรวบรวมข้อมูลส่วนบุคคลข้างต้น

(5) หลักทางเลือก (Choice)

เจ้าของข้อมูลควรได้รับทางเลือกตามสมควรในการเปิดเผยข้อมูลส่วนบุคคลของเขา หมายความว่า เจ้าของข้อมูลมีสิทธิที่จะกำหนดได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลจะสามารถเปิดเผยข้อมูลของตนได้ในระดับมากหรือน้อยเพียงใด

(6) หลักความสมบูรณ์ของข้อมูลส่วนบุคคล (Intergrity of Personal Information)

ข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้จะต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบันและจำเป็นต่อวัตถุประสงค์ในการใช้ข้อมูลนั้นด้วย

(7) หลักการป้องกันความเสียหาย (Security Safeguards)

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีมาตรการป้องกันความเสียหายของข้อมูลส่วนบุคคลจากความเสี่ยงในรูปแบบต่างๆ ที่จะก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้ เช่น การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผยหรือใช้ข้อมูลส่วนบุคคลในทางที่ไม่ชอบ ข้อมูลสูญหาย หรือการที่ข้อมูลส่วนบุคคลถูกทำลายโดยไม่ได้รับอนุญาต เป็นต้น

(8) หลักการเข้าถึงและการแก้ไข (Access and Correction)

หลักการเข้าถึงและการแก้ไขถือเป็นหลักการที่กำหนดไว้เพื่อรองรับสิทธิของเจ้าของข้อมูล โดย APEC Privacy Framework กำหนดให้เจ้าของข้อมูลส่วนบุคคลจะต้องมีสิทธิเข้าถึงข้อมูลส่วนบุคคลของตนที่ถูกจัดเก็บไว้ได้เพื่อที่จะขอแก้ไขในกรณีที่ข้อมูลดังกล่าวไม่ถูกต้องหรือขอลบข้อมูลนั้น และมีสิทธิในการได้รับความชัดเจนจากผู้ควบคุมข้อมูลส่วนบุคคลว่าได้มีการเก็บ ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของตนหรือไม่

(9) หลักความรับผิดชอบ (Accountability)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องรับผิดชอบในการปฏิบัติตามหลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามที่ได้กล่าวมา ณ ข้างต้นด้วย

4.2.2.3 การอนุวัติการตาม APEC Privacy Framework

โดยหลัก APEC Privacy Framework จะไม่บังคับประเทศสมาชิกให้ต้องอนุวัติการ APEC Privacy Framework ให้เป็นกฎหมายภายในของตนเนื่องจาก APEC ตระหนักเป็นอย่างดีว่าแต่ละประเทศย่อมมีสังคม วัฒนธรรม เศรษฐกิจและภูมิหลังทางกฎหมายที่แตกต่างกัน[24] ดังนั้น การไม่ปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลที่ APEC Privacy Framework กำหนดไว้จึงไม่มีโทษใดๆ กับประเทศสมาชิก แต่อย่างไรก็ตาม เพื่อส่งเสริมให้ประเทศสมาชิกมีหลักการว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐานไปในแนวทางเดียวกัน APEC Privacy Framework จึงสนับสนุนให้ประเทศสมาชิกรับหลักการทั้ง 9 ประการไปบัญญัติเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนด้วย

4.2.3 กฎหมายสหภาพยุโรป: DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data และ THE GENERAL DATA PROTECTION REGULATION (“Directive 95/46/EC”) และ The General Data Protection Regulation (“GDPR”)

4.2.3.1 แนวคิดและความเป็นมา

แนวคิดและความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนั้นเกิดขึ้นและมีผลใช้บังคับมาอย่างยาวนาน โดยพัฒนาการของกฎหมายเกิดขึ้นพร้อมกับการใช้คอมพิวเตอร์ในช่วงค.ศ. 1970[25] เป็นต้นมา เนื่องจากการใช้งานคอมพิวเตอร์เริ่มก่อให้เกิดการละเมิดข้อมูลส่วนบุคคลกันมากขึ้น ทั้งนี้ ในสหภาพยุโรปนั้น ประชาชนมีสิทธิที่จะได้รับความคุ้มครองข้อมูลส่วนบุคคลตามที่บัญญัติไว้ทั้งในกฎหมายแม่บทและกฎหมายลำดับรอง โดยกฎหมายแม่บทที่เกี่ยวเนื่องกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนั้น ได้แก่ อนุสัญญาแห่งสหภาพยุโรปว่าด้วยสิทธิมนุษยชน (European Convention of Human Rights: ECHR) ส่วนกฎหมายลำดับรองที่เกี่ยวเนื่องกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ได้แก่ DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 on the protection of individuals with regard to the processing of personal data

---

[24] *Ibid*., p.711.

[25] Peter Carey, Data Protection A practical Guide to UK and EU Law, (Second Edition), (New York: Oxford University Press Inc., 2004), p1.

and on the free movement of such data (“Directive 95/46/EC”) ซึ่งจะถูกแทนที่ด้วยกฎหมายฉบับใหม่ที่เรียกว่า THE GENERAL DATA PROTECTION REGULATION (“GDPR”) ในต้นปีค.ศ. 2018 เพื่อประโยชน์แก่การศึกษาจึงจำเป็นต้องศึกษาทั้งกฎหมายฉบับเดิมและฉบับใหม่ที่จะมีผลใช้บังคับควบคู่กันไป

สำหรับ Directive 95/46/EC นั้น นับเป็นบทบัญญัติที่มีผลบังคับระหว่างประเทศเป็นฉบับแรกของสหภาพยุโรป โดยถูกยกร่างขึ้นในช่วงกลางของยุค ค.ศ. 1990 เนื่องจากในยุคดังกล่าวสหภาพยุโรปถือเป็นผู้ที่มีบทบาทสำคัญในวงการการคุ้มครองข้อมูลส่วนบุคคล จนกระทั่งยกร่างเป็นที่สำเร็จเมื่อวันที่ 24 ตุลาคม ค.ศ. 1995[26] และมีผลใช้บังคับเป็นกฎหมายเมื่อวันที่ 13 ธันวาคม ค.ศ. 1995 อย่างไรก็ตาม กฎหมายฉบับดังกล่าวยังไม่มีผลต่อประเทศสมาชิกของสหภาพยุโรปจนกว่าประเทศสมาชิกจะมีการตรากฎหมายภายในตามแนวของ Directive 95/46/EC หรือรับเอา Directive 95/46/EC ดังกล่าวมาบังคับใช้เป็นกฎหมายภายในของตนเอง ซึ่งประเทศสมาชิกในขณะนั้นจะต้องตรากฎหมายเพื่อรองรับ Directive 95/46/EC ภายในวันที่ 24 ตุลาคม ค.ศ. 1998[27]

Directive 95/46/EC มีวัตถุประสงค์หลักเพื่อรองรับการเคลื่อนย้ายข้อมูลส่วนบุคคลอย่างอิสระระหว่างประเทศสมาชิกด้วยกันเอง แต่อย่างไรก็ตาม สิทธิขั้นพื้นฐานได้แก่ สิทธิในการได้รับความคุ้มครองข้อมูลส่วนบุคคลจะยังคงได้รับความคุ้มครองอยู่เช่นเดิม หรือหากจะกล่าวอีกนัยหนึ่งคือ Directive 95/46/EC มีความพยายามในการสร้างสมดุลระหว่างความเป็นส่วนตัวของบุคคลและผลประโยชน์ของตลาดภายในของสหภาพยุโรปที่เป็นผลประโยชน์ของภาคเอกชน อย่างไรก็ตาม เนื่องจาก Directive 95/46/EC มีผลใช้บังคับเป็นกฎหมายมาเป็นระยะกว่า 25 ปีโดยไม่ได้รับการแก้ไขปรับปรุงบทบัญญัติให้รองรับกับเทคโนโลยีที่เปลี่ยนแปลงไป ประกอบกับแต่ละประเทศที่บัญญัติกฎหมายภายในเพื่อนำเอา Directive 95/46/EC ไปใช้บังคับต่างบัญญัติและตีความกฎหมายดังกล่าวแตกต่างกันไป กรณีจึงนำมาสู่ความพยายามในการแก้ไขปรับปรุง Directive 95/46/EC ให้เหมาะสมกับสถานการณ์ปัจจุบันมากยิ่งขึ้น ดังนั้น คณะทำงานหรือผู้ที่เกี่ยวข้องของสหภาพยุโรปจึงได้ยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นใหม่โดยมีหลักการพื้นฐานคล้ายกับ Directive 95/46/EC และเรียกชื่อว่า “THE GENERAL DATA

---

[26] Graham J H Smith Bird & Bird, Internet Law and Regulation, (Fourth Edition), (London: Sweet & Maxwell, 2007), p.687.

[27] Christopher Kuner, European Data Privacy Law and Online Business, (New York: Oxford University Press Inc., 2003), p.17.

PROTECTION REGULATION" หรือ "GDPR" โดยเมื่อวันที่ 12 มีนาคม ค.ศ. 2014 สภาแห่งสหภาพยุโรปได้ลงคะแนนสนับสนุนกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่นี้ถึง 621 เสียง ทั้งนี้มีผู้คัดค้านจำนวน 10 เสียง และไม่ออกเสียงลงคะแนนอีก 22 เสียง[28] ดังนั้น ในระยะเวลาต่อมาจึงมีการตั้งคณะทำงานที่เรียกว่า 'The European Data Protection Board หรือ EDPB' ขึ้นในวันที่ 15 มิถุนายน ค.ศ. 2015 โดยจะทำหน้าที่แทนคณะทำงานเดิม (Article 29 Working Party) เพื่อตรวจตราและพิจารณาการบังคับใช้ GDPR กับประเทศสมาชิกของสหภาพยุโรป

ภายหลังการพิจารณาของคณะทำงานข้างต้น ปัจจุบันกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรปจึงมีผลใช้บังคับแทนที่หลักเกณฑ์ฉบับเดิมเมื่อวันที่ 24 พฤษภาคม 2016 แต่การบังคับใช้กับประเทศสมาชิกจะยังไม่มีผลจนกว่าจะถึงระยะเวลาที่กำหนดไว้ คือ วันที่ 25 พฤษภาคม 2018[29] ซึ่งภายหลังที่ GDPR มีผลใช้บังคับกับประเทศสมาชิกแล้ว ประเทศสมาชิกแต่ละประเทศจะต้องนำ GDPR มาใช้บังคับกับประเทศของตนโดยอัตโนมัติ อย่างไรก็ตาม แต่ละประเทศอาจออกกฎหมายภายในว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเพื่อระบุรายละเอียดเพิ่มเติมตามที่ GDPR เปิดช่องไว้ได้ ทั้งนี้ GDPR มีหลักการหลายประการที่เสริมและเพิ่มเติมจาก Directive 95/46/EC ซึ่งจะได้ศึกษาโดยละเอียดดังนี้

---

[28] European Data Protection Supervisor, "The History of the General Data Protection Regulation" สืบค้นเมื่อวันที่ 24 กุมภาพันธ์ 2560, จาก https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[29] Aysem Diker Vanberg and Mehmet Bilal Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?," EJLT European Journal of Law and Technology, Vol 8, No.1, p.1, (2017).

4.2.3.2 เจตนารมณ์

Directive 95/46/EC[30] และ GDPR[31] มีเจตนารมณ์ที่คล้ายคลึงกัน ดังต่อไปนี้[32]

1. คุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูล
2. เปิดโอกาสให้ข้อมูลส่วนบุคคลสามารถส่งผ่านได้อย่างเสรีภายในสหภาพยุโรป
3. ส่งเสริมเศรษฐกิจ กระบวนการทางสังคมและการค้า
4. ระบุตำแหน่งของการประมวลผลข้อมูลส่วนบุคคลในกระบวนการทางเทคโนโลยี

อย่างไรก็ตาม GDPR ได้กำหนดเจตนารมณ์เพิ่มเติมจาก Directive 95/46/EC โดยมุ่งหมายที่จะผสมผสานระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกภายในสหภาพยุโรปให้เป็นอันหนึ่งอันเดียวกันโดยยึด GDPR เป็นหลักซึ่งจะเป็นประโยชน์ต่อองค์กรหรือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามกฎหมายภายในสหภาพยุโรป

---

[30] Article 1 of Directive 95/46/EC

In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

[31] Article 1 of GDPR

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

[32]Christopher Kuner, *supra note 32*, p.17.

ทั้งนี้ หากพิจารณาเจตนารมณ์ของ GDPR เชื่อมโยงกับยุคเศรษฐกิจดิจิทัลในปัจจุบัน จะพบว่า GDPR มุ่งที่จะส่งเสริมการค้าในรูปแบบใหม่ในตลาดดิจิทัลซึ่งรวมถึงระบบการประมวลผลแบบคลาวด์ด้วย

4.2.3.3 ขอบเขตการใช้บังคับ

Directive 95/46/EC และ GDPR มีขอบเขตการใช้บังคับโดยตรงต่อข้อมูล ระบบ และบุคคล ดังต่อไปนี้

(1) ข้อมูลที่อยู่ภายใต้บังคับของ Directive 95/46/EC และ GDPR

ภายใต้ Directive 95/46/EC[33] และ GDPR[34] กำหนดให้ใช้บังคับกับข้อมูลส่วนบุคคลของบุคคลธรรมดาแต่ไม่รวมถึงผู้ที่ถึงแก่กรรม ดังนั้น ข้อมูลที่ไม่มีลักษณะเป็นข้อมูลส่วนบุคคล เช่น ข้อมูลความลับทางการค้า ข้อมูลทั่วๆ ไปหรือ Big Data จะไม่อยู่ภายใต้บังคับของทั้ง Directive 95/46/EC และ GDPR แต่อาจตกอยู่ภายใต้บังคับของกฎหมายอื่น ซึ่งไม่อยู่ในขอบเขตของการศึกษาในครั้งนี้ ซึ่งในกรณีของข้อมูลความลับทางการค้าจะตกอยู่ภายใต้บังคับของ Directive of the European Parliament and of the Council on the protection of undisclosured know-how and business information (trade secrets) againt their

---

[33] Article 2(a) of Directive 95/46/EC

2. For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

[34] Article 1(1)-(2) of Directive 95/46/EC

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

unlawful acquisition, use and disclosure แต่สำหรับข้อมูลทั่วๆ ไปหรือ Big Data นั้น ขณะนี้สหภาพยุโรปกำลังอยู่ในระหว่างการศึกษาเพื่อสร้างกฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล (Non-personal data) โดยเรียกชื่อว่า “A framework for the free flow of non-personal data in the EU”

อนึ่ง GDPR กำหนดเพิ่มเติมจาก Directive 95/46/EC ให้ประเทศสมาชิกจัดให้มีกฎเกณฑ์เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้ที่ถึงแก่กรรมด้วยเช่นกัน

(2) ระบบที่อยู่ภายใต้บังคับของ Directive 95/46/EC และ GDPR

Directive 95/46/EC[35] และ GDPR[36] กำหนดระบบที่จะอยู่ภายใต้บังคับเช่นเดียวกัน กล่าวคือ Directive 95/46/EC และ GDPR จะใช้บังคับกับการประมวลผลข้อมูล

---

[35] Article 3 of Directive 95/46/EC

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

[36] Article 2(1) of GDPR

1.This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

ส่วนบุคคลโดยวิธีการอัตโนมัติหรือโดยวิธีการอื่นใด โดยยึดหลักความเป็นกลางทางเทคโนโลยี (Technology Neutrality) และไม่ขึ้นอยู่กับเทคนิคที่ใช้

(3) บุคคลที่อยู่ภายใต้บังคับของ Directive 95/46/EC และ GDPR

Directive 95/46/EC[37] และ GDPR[38] กำหนดบุคคลที่อยู่ภายใต้บังคับเช่นเดียวกัน กล่าวคือ Directive 95/46/EC และ GDPR บังคับใช้ทั้งกับบุคคลธรรมดาและนิติบุคคล รวมทั้งหน่วยงานของรัฐและหน่วยงานอื่นๆ ที่ประมวลผลข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม บุคคลที่อยู่ภายใต้บังคับของ Directive 95/46/EC โดยตรง คือ ผู้ควบคุมข้อมูล ซึ่งแตกต่างจาก GDPR ที่กำหนดเพิ่มให้ผู้ประมวลผลข้อมูลจะต้องอยู่ภายใต้บังคับของ GDPR โดยตรงด้วย ดังนั้น บุคคลที่อยู่ภายใต้บังคับของ GDPR ได้แก่ ผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผล (Processor)

อย่างไรก็ตาม หลักเกณฑ์ทั้งสองข้างต้นมิได้ใช้บังคับเฉพาะเวลาที่ผู้ควบคุมข้อมูลจัดตั้งอยู่ภายในประเทศใดประเทศหนึ่งของสหภาพยุโรปเท่านั้น แต่ยังมีขอบเขตในการใช้บังคับรวมถึงกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลตั้งอยู่ภายนอกสหภาพยุโรปแต่มีการขายสินค้าหรือให้บริการ หรือ monitor ข้อมูลส่วนบุคคลของบุคคลที่อยู่ในสหภาพยุโรปแล้ว ผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวก็จะต้องปฏิบัติตามกฎข้อบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR ด้วยเช่นกัน ซึ่งการกำหนดเช่นนี้อาจเป็นไปได้ว่ากฎหมาย

---

[37] Article 2(d) of Directive 95/46/EC

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

[38] Article 4(7) of GDPR

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

คุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปพิจารณาคำนึงการซื้อขายหรือให้บริการผ่านระบบเทคโนโลยีที่ลักษณะทางกายภาพอาจจะไม่ปรากฏอยู่ในดินแดนของสหภาพยุโรป

(4) ข้อยกเว้นของขอบเขตการใช้บังคับ Directive 95/46/EC[39] และ GDPR[40] จะไม่ใช้บังคับกับกรณีดังต่อไปนี้

- การดำเนินการใดๆ ที่นอกเหนือไปจากขอบเขตของกฎเกณฑ์ของสหภาพยุโรป อาทิ การดำเนินการของประเทศสมาชิกที่เกี่ยวเนื่องกับกฎหมายอาญา
- การดำเนินการใดๆ ของประเทศสมาชิกเพื่อวัตถุประสงค์บางประการ เช่น รักษาความปลอดภัย ปกป้องเศรษฐกิจของประเทศ หรือเพื่อผลประโยชน์ทางการเงินของประเทศ เป็นต้น
- การดำเนินการใดๆ ของบุคคลธรรมดาเพื่อตนเองหรือครอบครัวโดยเฉพาะ

---

[39] Article 3(2) of Directive 95/46/EC

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

[40] Article 2(2) – (3) of GDPR

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

ทั้งนี้ ภายใต้ GDPR จะเพิ่มข้อยกเว้นเพิ่มเติมจาก Directive 95/46/EC ได้แก่ การดำเนินการใดๆ ของสหภาพยุโรปเอง และการดำเนินการใดๆ ของหน่วยงานของรัฐเพื่อวัตถุประสงค์เกี่ยวกับความมั่นคงของชาติ (National Security) การป้องกันประเทศ (Defence) ความปลอดภัยของสาธารณะ (Public Security) การป้องกัน (Prevention) การสืบสวน (Investigation) การสอบสวน (Detection) การดำเนินคดีอาญา (Prosecution of criminal offences) การดำเนินการเกี่ยวกับการพิจารณาคดี (Performance of judicial functions) เป็นต้น

4.2.3.4 บทนิยามที่สำคัญ

ภายใต้ Directive 95/46/EC และ GDPR มีบทนิยามที่สำคัญที่ต้องพิจารณา ได้แก่

(1) ข้อมูลส่วนบุคคล

Directive 95/46/EC	GDPR
ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใดๆ ที่สามารถระบุตัวหรืออาจจะระบุตัวตนของบุคคลนั้นได้ (เจ้าของข้อมูล) ซึ่งบุคคลที่อาจระบุตัวตนได้ไม่ว่าโดยทางตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะตัวของบุคคลหรือจากปัจจัยอื่นๆ ที่มีลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสภาพสังคมของบุคคลนั้น เป็นต้น[41]	ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใดๆ ที่สามารถระบุตัวหรืออาจจะระบุตัวตนของบุคคลนั้นได้ (เจ้าของข้อมูล) ซึ่งบุคคลที่อาจระบุตัวตนได้ไม่ว่าโดยทางตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากสิ่งบ่งชี้หรือระบุตัวตน เช่น ชื่อ หมายเลขเฉพาะตัวของบุคคล ที่อยู่ของข้อมูล สิ่งระบุตัวตนออนไลน์ หรือจากปัจจัยอื่นๆ ที่มีเป็นจำนวนหนึ่งหรือมากกว่าหนึ่งปัจจัยที่มีลักษณะเฉพาะทางร่างกาย สรีระ พันธุกรรม

[41] Article 2(a) of Directive 95/46/EC

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Directive 95/46/EC	GDPR
	จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสภาพสังคมของบุคคลนั้น[42]

หมายเหตุ: จากบทนิยามข้างต้นจะเห็นได้ว่าข้อมูลส่วนบุคคลมีความหมายที่แคบกว่าข้อมูลทั่วๆ ไป และข้อมูลที่เป็นความลับทางการค้า ซึ่งข้อมูลทั่วๆ ไปและข้อมูลที่เป็นความลับทางการค้าไม่อยู่ในขอบเขตการให้ความคุ้มครองของ GDPR

(2) ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive data)

Directive 95/46/EC	GDPR
ข้อมูลส่วนบุคคลที่อ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่เปิดเผยเชื้อชาติ ที่มาของชาติพันธุ์ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อทางปรัชญา สมาชิกภาพของสหภาพแรงงาน และข้อมูลที่เกี่ยวกับสุขภาพหรือเพศ[43]	ข้อมูลส่วนบุคคลที่อ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่เปิดเผยเชื้อชาติ ที่มาของชาติพันธุ์ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อทางปรัชญา สมาชิกภาพของสหภาพแรงงาน

[42] Article 4(1) of GDPR

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[43] Article 8(1) Directive 95/46/EC

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Directive 95/46/EC	GDPR
	และข้อมูลที่เกี่ยวกับสุขภาพ เพศ ข้อมูลทางพันธุกรรม ข้อมูลทางชีวภาพ[44]

(3) ข้อมูลนิรนาม (Anonymous data) หรือข้อมูลที่ผ่านการ Anonymization

Directive 95/46/EC	GDPR
ไม่พบบทบัญญัติเรื่องข้อมูลนิรนาม	ไม่พบบทบัญญัติที่กำหนดบทนิยามเรื่องข้อมูลนิรนามโดยตรงแต่จาก Rectical 26 สามารถเข้าใจโดยปริยายได้ว่า ข้อมูลนิรนาม หมายถึง ข้อมูลที่ลบสิ่งเชื่อมโยงบุคคลออกอย่างถาวรทำให้ไม่สามารถบ่งชี้ตัวบุคคลผู้เป็นเจ้าของข้อมูลได้

(4) ข้อมูลแฝง (Pseudonymous data)

Directive 95/46/EC	GDPR
ไม่พบบทบัญญัติเรื่องข้อมูลแฝง	ไม่พบบทบัญญัติที่กำหนดบทนิยามของข้อมูลแฝงโดยตรงแต่จากบทบัญญัติมาตรา 4(5), 6(4)(e), 25(1), 32(1)(a), 40(2)(d) และ 89(1) ทำให้สามารถเข้าใจได้ว่า ข้อมูลแฝงเป็นข้อมูลที่สามารถบ่งชี้ลักษณะเฉพาะของตัวบุคคลได้โดยผ่านข้อมูลอีกชุดหนึ่ง ซึ่งข้อมูลอีกชุด

[44] Article 9(1) of GDPR

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Directive 95/46/EC	GDPR
	ดังกล่าวจะถูกเก็บแยกต่างหากจากข้อมูลส่วนบุคคล

(5) การประมวลผล

Directive 95/46/EC	GDPR
การประมวลผล หมายความถึง การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึก การจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การส่งผ่าน การใช้ การเปิดเผย การเผยแพร่ หรือโดยวิธีการอื่นๆ ที่ทำให้เข้าถึงข้อมูลได้[45]	การประมวลผล หมายความถึง การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึก การจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การส่งผ่าน การใช้ การเปิดเผย การเผยแพร่ หรือโดยวิธีการอื่นๆ ที่ทำให้เข้าถึงข้อมูลได้[46]

[45] Article 2(b) of Directive 95/46/EC

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

[46] Article 4(2) of GDPR

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(6) ผู้ควบคุมข้อมูล

Directive 95/46/EC	GDPR
ผู้ควบคุมข้อมูล หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใดที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพังหรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป[47]	ผู้ควบคุมข้อมูล หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใดที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพังหรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป[48]

(7) ผู้ประมวลผลข้อมูล

Directive 95/46/EC	GDPR
ผู้ประมวลผลข้อมูล หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือ	ผู้ประมวลผลข้อมูล หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือ

[47]Article 2(d) of Directive 95/46/EC

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

[48] Article 4(7) of GDPR

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Directive 95/46/EC	GDPR
องค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล[49]	องค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล[50]

4.2.3.5 การประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลตาม Directive 95/46/EC และ GDPR จะต้องเป็นการประมวลผลที่ชอบด้วยกฎหมายเท่านั้น[51] ทั้งนี้ การประมวลผลที่ชอบด้วยกฎหมาย

---

[49] Article 2(e) of Directive 95/46/EC

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

[50] Article 4(8) of GDPR

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

[51] Article 7 of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

หมายถึง การประมวลผลที่กฎหมายให้อำนาจให้สามารถกระทำได้ซึ่งตั้งอยู่บนหลักการที่จะได้กล่าวดังต่อไปนี้ อย่างไรก็ตาม GDPR บัญญัติให้ประเทศสมาชิกสามารถกำหนดหลักการอื่นเพิ่มเติมภายในกฎหมายภายในของตนได้ตามหลักการพื้นฐานที่กำหนดไว้ใน GDPR[52]

Article 6(1) of GDPR

Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks

[52] Article 6 (2) of GDPR

(2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

(1) ได้รับความยินยอมจากเจ้าของข้อมูล

ข้อมูลส่วนบุคคลจะสามารถประมวลผลโดยชอบด้วยกฎหมายได้ก็ต่อเมื่อเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยอิสระสำหรับการประมวลผลข้อมูลส่วนบุคคลนั้น[53] ทั้งนี้ ความยินยอมดังกล่าวจะต้องเป็นความยินยอมที่เจ้าของข้อมูลได้ให้ไว้โดยได้รับแจ้งข้อมูลที่เกี่ยวข้องที่เพียงพอสำหรับการให้ความยินยอมดังกล่าวด้วย[54] นอกจากนี้ ภายใต้ GDPR ความยินยอมดังกล่าวจะต้องเป็นความยินยอมที่แสดงออกโดยชัดแจ้งด้วยไม่ว่าจะเป็นลายลักษณ์อักษรหรือการกระทำการที่แสดงออกซึ่งความยินยอม หรือ

---

[53] Article 7(a) of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

Article 6(1)(a) of GDPR

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

[54] Article 2(h) of Directive 95/46/EC

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 4(11) of GDPR

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Article 7(1) of GDPR

(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(2) มีข้อตกลงหรือสัญญาระหว่างกัน

ข้อมูลส่วนบุคคลจะสามารถประมวลผลโดยชอบด้วยกฎหมายภายใต้ Directive 95/46/EC และ GDPR ก็ต่อเมื่อการประมวลผลนั้นมีการเข้าทำข้อตกลงหรือสัญญากับเจ้าของข้อมูล[55] หรือ

(3) จำเป็นต้องกระทำเพื่อปฏิบัติตามหน้าที่ที่กฎหมายกำหนด

การประมวลผลข้อมูลส่วนบุคคลที่จะสามารถกระทำได้โดยชอบด้วยกฎหมายภายใต้ Directive 95/46/EC และ GDPR จะต้องเป็นการประมวลผลที่ผู้ที่มีหน้าที่ตามที่กฎหมายกำหนดจำเป็นต้องกระทำเพื่อที่จะได้ปฏิบัติตามหน้าที่ที่กฎหมายกำหนดให้ถูกต้องครบถ้วน[56] หรือ

---

[55] Article 7(b) of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

Article 6(1)(b) of GDPR

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

[56] Article 7(c) of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

Article 6(1)(c) of GDPR

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(4) จำเป็นต้องกระทำเพื่อรักษาผลประโยชน์เกี่ยวกับชีวิตร่างกาย

การประมวลผลข้อมูลส่วนบุคคลที่จะสามารถกระทำได้โดยชอบด้วยกฎหมายภายใต้ Directive 95/46/EC และ GDPR จะต้องเป็นการประมวลผลที่จำเป็นต้องกระทำเพื่อปกป้องผลประโยชน์เกี่ยวกับชีวิตร่างกายของเจ้าของข้อมูล อย่างไรก็ตาม GDPR ขยายความรวมไปถึงผลประโยชน์เกี่ยวกับชีวิตร่างกายของบุคคลธรรมดารายอื่นด้วยเช่นกัน[57] หรือ

(5) จำเป็นต้องกระทำเพื่อรักษาผลประโยชน์สาธารณะ

การประมวลผลข้อมูลส่วนบุคคลที่จะสามารถกระทำได้โดยชอบด้วยกฎหมายภายใต้ Directive 95/46/EC และ GDPR จะต้องเป็นการประมวลผลที่จำเป็นต้องกระทำเพื่อปกป้องผลประโยชน์สาธารณะ หรือ เป็นการดำเนินการของหน่วยงานราชการในฐานะของผู้ควบคุมข้อมูล[58] หรือ

---

[57] Article 7(d) of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(d) processing is necessary in order to protect the vital interests of the data subject; or

Article 6(1)(d) of GDPR

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[58] Article 7(e) of Directive 95/46/EC

Member States shall provide that personal data may be processed only if:

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(6) กฎหมายบัญญัติโดยชัดแจ้งให้สามารถกระทำได้โดยชอบ

การประมวลผลข้อมูลส่วนบุคคลที่จะสามารถกระทำได้โดยชอบด้วยกฎหมายภายใต้ Directive 95/46/EC และ GDPR จะต้องเป็นการประมวลผลที่กฎหมายบัญญัติโดยชัดแจ้งให้สามารถกระทำได้โดยผู้ควบคุมข้อมูลหรือบุคคลอื่นที่ถูกเปิดเผยข้อมูลส่วนบุคคล แต่หากผลประโยชน์ของผู้ควบคุมข้อมูลขัดหรือแย้งกับผลประโยชน์หรือสิทธิของเจ้าของข้อมูล การประมวลผลดังกล่าวข้างต้นจะไม่สามารถกระทำได้

อย่างไรก็ตาม GDPR ให้ขยายความเพิ่มเติมให้ชัดเจนขึ้นสำหรับกรณีที่ผลประโยชน์ของผู้ควบคุมข้อมูลขัดหรือแย้งกับผลประโยชน์หรือสิทธิของเจ้าของข้อมูลที่เป็นเด็กและข้อยกเว้นข้างต้นจะไม่ใช้บังคับกับการประมวลผลที่ดำเนินการโดยหน่วยงานของรัฐหรือหน่วยงานสาธารณะที่ปฏิบัติตามหน้าที่ตามกฎหมายของตน

อนึ่ง การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการกระทำความผิด การพิสูจน์ความผิดในทางอาญา หรือมาตรการเกี่ยวกับความปลอดภัยนั้นจะสามารถประมวลผลได้เฉพาะภายใต้เงื่อนไขที่กฎหมายกำหนดไว้เท่านั้น ได้แก่ เป็นการประมวลผลโดยหน่วยงานของรัฐและมีกฎหมายอนุญาตให้สามารถทำได้ เป็นต้น ซึ่งเป็นไปในทำนองเดียวกับการประมวลผลข้อมูลที่อ่อนไหวซึ่ง Directive 95/46/EC และ GDPR กำหนดให้ห้ามประมวลผล ยกเว้นว่าจะปรากฏเหตุการณ์ ต่อไปนี้

- เจ้าของข้อมูลได้ให้ความยินยอมไว้อย่างชัดแจ้ง
- จำเป็นต้องมีการประมวลผลข้อมูลภายใต้กฎหมายแรงงาน ทั้งนี้ GDPR กำหนดขยายความเพิ่มต่อไปอีกว่า จำเป็นต้องมีการประมวลผลภายใต้กฎหมายเกี่ยวกับประกันสังคมหรือกฎหมายคุ้มครองแรงงาน

Article 6(1)(e) of GDPR

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- จำเป็นต้องมีการประมวลผลข้อมูลเพื่อปกป้องผลประโยชน์เกี่ยวกับชีวิตร่างกายของเจ้าของข้อมูลหรือบุคคลอื่นในกรณีที่เจ้าของข้อมูลไม่อยู่ในสภาวะที่สามารถให้ความยินยอมได้
- เป็นการประมวลผลขององค์กรที่ไม่แสวงหากำไรภายใต้วัตถุประสงค์ของกฎหมาย
- เป็นการประมวลผลข้อมูลที่ได้รับการเปิดเผยอย่างชัดแจ้งสู่สาธารณะโดยเจ้าของข้อมูล
- เป็นการประมวลผลที่จำเป็นต้องกระทำเพื่อการก่อตั้ง การแสดงออกหรือการโต้แย้งสิทธิเรียกร้องตามกฎหมาย ทั้งนี้ GDPR กำหนดขยายเพิ่มเติมถึงกรณีที่เป็นการแสดงออกของศาลในการตัดสินคดีด้วย
- จำเป็นต้องมีการประมวลผลเพื่อผลประโยชน์สาธารณะที่สำคัญและเพื่อเป็นการปกป้องสิทธิของเจ้าของข้อมูลตามส่วน
- เป็นการประมวลผลที่จำเป็นเพื่อวัตถุประสงค์ในการรักษาพยาบาลของผู้เชี่ยวชาญทางด้านสุขภาพ ทั้งนี้ GDPR ยกตัวอย่างเพิ่มเติมได้แก่ การประเมินความสามารถในการทำงานของลูกจ้าง การบริหารจัดการสุขภาพหรือระบบประกันสุขภาพ เป็นต้น[59]

---

[59] Article 8(3) of Directive 95/46/EC

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Article 9(2)(h) of GDPR

(2) Paragraph 1 shall not apply if one of the following applies:

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

- เป็นการประมวลผลที่จำเป็นต้องกระทำเพื่อรักษาผลประโยชน์สาธารณะที่เกี่ยวเนื่องกับสาธารณะสุข เช่น การตรวจสอบความปลอดภัยของสินค้าที่มีคุณสมบัติเป็นยา[60]
- เป็นการประมวลผลที่จำเป็นต้องกระทำเพื่อบรรลุวัตถุประสงค์ของผลประโยชน์สาธารณะ ประวัติศาสตร์ วิทยาศาสตร์ การค้นคว้าวิจัย หรือ เพื่อวัตถุประสงค์เชิงสถิติ เป็นต้น[61]

ทั้งนี้ GDPR ให้อำนาจแก่ประเทศสมาชิกของสหภาพยุโรปในการกำหนดเงื่อนไขอื่นๆ เพิ่มเติมจากที่กำหนดไว้ใน GDPR ได้ ตามมาตรา 9(4)[62] ของ GDPR

นอกจากนี้ Directive 95/46/EC และ GDPR ยังเปิดช่องให้ข้อมูลส่วนบุคคลสามารถถูกประมวลผลเพื่อวัตถุประสงค์ใหม่ที่แตกต่างไปจากวัตถุประสงค์เดิมได้ หาก

---

[60] Article 9(2)(i) of GDPR

2. Paragraph 1 shall not apply if one of the following applies:

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides fir suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

[61] Article 9(2)(j) of GDPR

2. Paragraph 1 shall not apply if one of the following applies:

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

[62] Article 9(4) of GDPR

4. Member states may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

วัตถุประสงค์ที่กำหนดขึ้นใหม่นั้นไม่ขัดหรือแย้งกับวัตถุประสงค์เดิม ซึ่งแต่เดิม Directive 95/46/EC ไม่ได้กำหนดอย่างชัดแจ้งว่าบุคคลใดจะทำหน้าที่พิจารณาว่าว่าวัตถุประสงค์ใหม่นั้นขัดหรือแย้งกับวัตถุประสงค์เดิมหรือไม่ ดังนั้น GDPR จึงได้บัญญัติในส่วนนี้โดยชัดแจ้งคือ ให้ผู้ควบคุมข้อมูลเป็นผู้มีหน้าที่ในการพิจารณา โดยผู้ควบคุมข้อมูลอาจพิจารณาจากปัจจัยต่างๆ ตามที่ได้ยกตัวอย่างไว้ในมาตรา 6(4) แห่ง GDPR ประกอบ

4.2.3.6 สิทธิของเจ้าของข้อมูล

ภายใต้ Directive 95/46/EC และ GDPR เจ้าของข้อมูลมีสิทธิต่างๆ ตามที่กฎหมายกำหนด ทั้งนี้ GDPR ได้กำหนดบทบัญญัติเพิ่มเติมเพื่อเป็นการรองรับสิทธิของเจ้าของข้อมูลด้วยว่า ผู้ควบคุมข้อมูลมีหน้าที่ตามกฎหมายที่จะทำให้สิทธิของเจ้าของข้อมูลสามารถเกิดขึ้นได้จริง ทั้งนี้ ตามมาตรา 12(2) แห่ง GDPR[63] และเมื่อเจ้าของข้อมูลร้องขอข้อมูลที่เกี่ยวข้องตามสิทธิของตน ผู้ควบข้อมูลจะต้องจัดหาข้อมูลดังกล่าวให้แก่เจ้าของข้อมูลภายในระยะเวลา 1 เดือน นับตั้งแต่ได้รับคำร้องขอดังกล่าว (หากเจ้าของข้อมูลร้องขอในรูปแบบอิเล็กทรอนิกส์ ผู้ควบคุมข้อมูลต้องจัดหาให้ในรูปแบบอิเล็กทรอนิกส์ด้วย) แต่หากผู้ควบคุมข้อมูลไม่สามารถจัดหาข้อมูลดังกล่าวให้ได้ภายในระยะเวลาที่กำหนดเนื่องจากผู้ควบคุมข้อมูลได้รับคำร้องขอเป็นจำนวนมากหรือคำร้องขอที่ได้รับเป็นคำร้องขอที่มีความยุ่งยากซับซ้อน ผู้ควบคุมข้อมูลสามารถขอขยายระยะเวลาดังกล่าวได้อีก 2 เดือน ซึ่งเมื่อครบเวลาที่กำหนดแล้ว หากเจ้าของข้อมูลยังไม่ได้รับข้อมูลที่ตนร้องขอ เจ้าของข้อมูล

---

[63] Article 12(2) of GDPR

2. The controller shall facilitate the exercise of data subject rights under Article 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

สามารถร้องเรียนไปยังหน่วยงานที่มีหน้าที่รับผิดชอบตาม GDPR ได้แก่ หน่วยงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Authority: DPA) ได้ ทั้งนี้ ตามมาตรา 12(3)-(4) แห่ง GDPR[64]

อนึ่ง เพื่อเป็นการคุ้มครองสิทธิของเจ้าของข้อมูลและเพื่อจำกัดความเสี่ยงที่บุคคลอื่นจะเข้าถึงสิทธิของเจ้าของข้อมูลโดยไม่ได้รับอนุญาตและไม่ชอบด้วยกฎหมาย GDPR ได้เพิ่มบทบัญญัติที่กำหนดให้ผู้ควบคุมข้อมูลสามารถกำหนดให้เจ้าของข้อมูลต้องแสดงหลักฐานเพื่อเป็นการยืนยันตัวตนในฐานะเจ้าของข้อมูลก่อนการใช้สิทธิดังต่อไปนี้ในฐานะเจ้าของข้อมูลได้ ตามมาตรา 12(2) และ (6)[65] ทั้งนี้ หากเจ้าของข้อมูลไม่สามารถยืนยันตัวตนของตนเองเพื่อแสดงความ

---

[64] Article 12(3)-(4) of GDPR

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two futher months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

[65] Article 12(6) of GDPR

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

เป็นเจ้าของข้อมูลดังกล่าวได้ ผู้ควบคุมข้อมูลย่อมได้รับยกเว้นไม่ต้องปฏิบัติตามสิทธิของเจ้าของข้อมูลตามที่กำหนดไว้ในกฎหมายนี้ได้ อย่างไรก็ตาม บทบัญญัติในส่วนนี้เป็นเพียงการเปิดช่องให้ผู้ควบคุมข้อมูลสามารถดำเนินการได้เพื่อป้องกันความเสี่ยงที่จะเกิดขึ้น แต่บทบัญญัติแห่งกฎหมายไม่ได้กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ที่จะต้องปฏิบัติตามโดยเคร่งครัดแต่อย่างใด

(1) สิทธิได้รับข้อมูล (กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง)

เนื่องจาก Directive 95/46/EC และ GDPR ต้องการให้เจ้าของข้อมูลแน่ใจว่าข้อมูลส่วนบุคคลจะถูกประมวลผลโดยชอบ ดังนั้น Directive 95/46/EC และ GDPR จึงกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่สื่อสารกับเจ้าของข้อมูลอย่างโปร่งใสเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลนั้น เมื่อผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง โดยต้องบอกกล่าวข้อมูลอย่างน้อยดังต่อไปนี้ให้แก่เจ้าของข้อมูลทราบ กล่าวคือ ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลคือใคร วัตถุประสงค์ของการประมวลผลข้อมูลที่จัดเก็บไปและข้อมูลอื่นๆ เช่น ผู้รับโอนข้อมูลหากมีการโอนข้อมูล สิทธิของเจ้าของข้อมูล เป็นต้น[66]

อย่างไรก็ตาม GDPR ได้แก้ไขเพิ่มเติมบทบัญญัติจากที่กำหนดไว้ใน Directive 95/46/EC โดยกำหนดให้ข้อมูลที่จะต้องบอกกล่าวแก่เจ้าของข้อมูลนั้นจะต้องเป็นการบอกกล่าวอย่างครบถ้วน โปร่งใส เข้าใจได้โดยง่ายโดยอาศัยรูปแบบที่เจ้าของข้อมูลสามารถเข้าถึงได้

---

[66] Article 10 of Directive 95/46/EC

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him

In so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

โดยง่าย ใช้ภาษาที่ชัดเจนและใช้อยู่เป็นการทั่วไปด้วย[67] นอกจากนี้ ข้อมูลใดๆ ที่บอกกล่าวแก่เจ้าของข้อมูลซึ่งเป็นเด็กจะต้องมีความชัดเจนและใช้ภาษาที่ใช้อยู่เป็นการทั่วไปเพื่อที่จะทำให้เด็กสามารถเข้าใจข้อมูลดังกล่าวได้โดยง่ายด้วยเช่นกัน

(2) สิทธิได้รับข้อมูล (กรณีได้รับข้อมูลจากแหล่งอื่น ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง)

ในกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้รับข้อมูลส่วนบุคคลมาจากแหล่งอื่น ซึ่งไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง เจ้าของข้อมูลย่อมมีสิทธิที่จะได้รับข้อมูลเกี่ยวกับลักษณะเฉพาะของผู้ควบคุมข้อมูล เหตุผลประกอบในการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล และข้อมูลอื่นๆ ที่เกี่ยวข้องเพื่อแสดงให้เห็นถึงการประมวลผลโดยชอบด้วยกฎหมาย

---

[67] Article 5(1) of GDPR

1. Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparecy’);

Article 12(1) of GDPR

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

และโปร่งใส ทั้งนี้ ตามมาตรา 10[68] และ 11(1)[69] ของ Directive 95/46/EC และมาตรา 13(1)[70] และ 14(1)[71] ของ GDPR

---

[68] Article 10 of Directive 95/46/EC

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him

In so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

[69] Article 11(1) of Directive 95/46/EC

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him

In so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

[70] Article 13(1) of GDPR

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

[71] Article 14(1) of GDPR

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information;

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(3) สิทธิเข้าถึงข้อมูลส่วนบุคคลของตน

เพื่อที่จะให้เจ้าของข้อมูลสามารถบังคับสิทธิของตนตามกฎหมายกับผู้ควบคุมข้อมูลได้ และเพื่อให้สามารถตรวจสอบได้ว่าผู้ควบคุมข้อมูลหรือผู้ประมวลผลได้ประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายหรือไม่ มาตรา 12(a) ของ Directive 95/46/EC[72] และ

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

[72] Article 12 of Directive 95/46/EC Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

มาตรา 15(1) ของ GDPR[73] จึงได้กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลดำเนินการให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลส่วนบุคคลได้และให้ได้รับข้อมูลดังต่อไปนี้

- ข้อมูลยืนยันว่าผู้ควบข้อมูลได้ประมวลผลข้อมูลส่วนบุคคลหรือไม่
- ข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
- ข้อมูลเกี่ยวกับประเภทของข้อมูลที่จะได้รับการประมวลผล
- สำเนาข้อมูลที่ได้รับการประมวลผลและข้อมูลเกี่ยวกับแหล่งที่มาของข้อมูลนั้น

---

[73] Article 15(1) of GDPR

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the signigicance and the envisaged consequences of such processing for the data subject.

- คำอธิบายเกี่ยวกับหลักการเกี่ยวกับการประมวลผลโดยอัตโนมัติซึ่งส่งผลกระทบโดยตรงต่อเจ้าของข้อมูล

ทั้งนี้ ภายหลังการแก้ไข Directive 95/46/EC มาเป็น GDPR บทบัญญัติดังกล่าวได้เพิ่มเติมข้อมูลที่เจ้าของข้อมูลมีสิทธิได้รับ ดังนี้

- ข้อมูลเกี่ยวกับระยะเวลาที่ข้อมูลส่วนบุคคลจะถูกจัดเก็บ
- ข้อมูลที่ว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะลบ แก้ไข ยับยั้งหรือคัดค้านการประมวลผล
- ข้อมูลที่ว่าเจ้าของข้อมูลมีสิทธิที่จะร้องเรียนไปยังหน่วยงานที่รับผิดชอบตามกฎหมายได้
- ในกรณีที่ข้อมูลไม่ได้ถูกจัดเก็บจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลจะต้องแจ้งข้อมูลของแหล่งที่มาที่เจ้าของข้อมูลนั้นถูกจัดเก็บด้วย

(4) สิทธิแก้ไขข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลมีหน้าที่ต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลที่จัดเก็บนั้นเป็นข้อมูลที่ถูกต้อง สมบูรณ์ ซึ่งหากข้อมูลดังกล่าวไม่ถูกต้องหรือไม่สมบูรณ์ เจ้าของข้อมูล

ย่อมมีสิทธิแก้ไขข้อมูลดังกล่าวให้ถูกต้องได้ ทั้งนี้ ตามมาตรา 6(1)(d)[74] และมาตรา 12(b)[75] แห่ง Directive 95/46/EC และมาตรา 5(1)(d)[76] และ มาตรา 16[77] ของ GDPR

(5) สิทธิในการลบข้อมูลส่วนบุคคล

ภายใต้ มาตรา 12(b) แห่ง Directive 95/46/EC เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะลบข้อมูลส่วนบุคคลได้ถ้าผู้ควบคุมข้อมูลไม่สามารถปฏิบัติตาม Directive 95/46/EC ได้

---

[74] Article 6(1) of Directive 95/46/EC

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

[75] Article 12(b) of Directive 95/46/EC

Member States shall guarantee every data subject the right to obtain from the controller:

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

[76] Article 5(1) of GDPR

1. Personal data shall be:

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

[77] Article 16 of GDPR

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

ส่วนมาตรา 17(1)[78] แห่ง GDPR กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะลบข้อมูลส่วนบุคคลได้ ซึ่งเรียกว่า ‘สิทธิที่จะถูกลืม หรือ Right to be forgotten’ หากปรากฏข้อเท็จจริงดังต่อไปนี้

1) ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับการประมวลผลตามวัตถุประสงค์ที่กำหนดไว้เดิมอีกต่อไป (รวมทั้งไม่มีวัตถุประสงค์ใหม่โดยชอบด้วยกฎหมายด้วย) หรือ
2) เจ้าของข้อมูลถอนความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลนั้น ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นกระทำอยู่บนฐานแห่งความยินยอมของเจ้าของข้อมูล ซึ่งทำให้ผู้ควบคุมข้อมูลไม่มีอำนาจในการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายได้
3) เจ้าของข้อมูลส่วนบุคคลใช้สิทธิที่จะคัดค้านและผู้ควบคุมข้อมูลไม่มีอำนาจในการประมวลผลข้อมูลส่วนบุคคลต่อไปโดยชอบด้วยกฎหมายได้
4) ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย

---

[78] Article 17 of GDPR

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is cased according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Artic;e 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

5) การลบข้อมูลส่วนบุคคลดังกล่าวเป็นสิ่งที่จำเป็นต้องกระทำเพื่อปฏิบัติตามกฎหมายของสหภาพยุโรปหรือกฎหมายภายในที่เกี่ยวข้องของประเทศสมาชิก

สิทธิที่จะถูกลืมหรือ Right to be forgotten นี้เคยได้รับการตัดสินจากศาลยุโรป (European Court of Justice) ในปี 2014 ระหว่าง Google และ AEPD and Gonzáles[79] โดยที่ Gonzáles ร้องขอต่อศาลให้ Google ลบข้อมูลที่บ่งบอกว่า Gonzáles เป็นบุคคลที่อยู่ในกระบวนการพิจารณาล้มละลายซึ่งไม่เป็นความจริงในปัจจุบัน ดังนั้น Google ในฐานะผู้ควบคุมข้อมูลย่อมมีหน้าที่จะต้องลบข้อมูลดังกล่าวซึ่งไม่ถูกต้องหรือไม่ครบถ้วนตามความเป็นจริง หากข้อมูลเช่นว่านั้นสามารถนำไปประมวลผลได้ แต่เมื่อข้อเท็จจริงปรากฏว่า Google เพิกเฉยต่อหน้าที่นี้ย่อมถือว่า Google ละเมิดกฎหมายสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม ในบางกรณีเจ้าของข้อมูลอาจไม่มีสิทธิในการขอให้ผู้ควบคุมข้อมูลลบข้อมูลส่วนบุคคลตามบทบัญญัติดังกล่าวข้างต้นได้ ดังนั้น GDPR จึงกำหนดบทบัญญัติมาตรา 18(1)[80] ให้เจ้าของข้อมูลสามารถจำกัดวัตถุประสงค์ที่ผู้ควบคุมข้อมูลส่วนบุคคล

---

[79] Eleni Frantziou, “Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos,” สืบค้นเมื่อวันที่ 18 กันยายน 2559, จาก https://academic.oup.com/hrlr/article/14/4/761/644686/Further-Developments-in-the-Right-to-be-Forgotten

[80] Article 18 of GDPR 1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

สามารถประมวลผลข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย ซึ่งจะส่งผลให้ผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลได้ภายใต้วัตถุประสงค์ที่จำกัด ทั้งนี้ กรณีที่เจ้าของข้อมูลจะสามารถจำกัดวัตถุประสงค์ได้จะต้องปรากฏข้อเท็จจริงดังต่อไปนี้

- มีการโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล
- การประมวลผลข้อมูลส่วนบุคคลไม่ชอบด้วยกฎหมายและเจ้าของข้อมูลร้องขอให้มีการจำกัดวัตถุประสงค์ในการประมวลผล
- ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลตามวัตถุประสงค์เดิมอีกต่อไป แต่ข้อมูลดังกล่างยังคงมีความจำเป็นสำหรับการก่อตั้งแสดงออกหรือป้องกันสิทธิตามกฎหมายของผู้ควบคุมข้อมูล
- ในกรณีที่มูลฐานแห่งการประมวลผลข้อมูลอยู่ในระหว่างการพิสูจน์ความถูกต้องในบริบทที่เจ้าของข้อมูลใช้สิทธิเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลของตน

อนึ่ง ในกรณีที่ผู้ควบคุมข้อมูลเปิดเผยข้อมูลของเจ้าของข้อมูลให้แก่บุคคลอื่นหรือเปิดเผยสู่สาธารณะและเจ้าของข้อมูลมีความประสงค์จะใช้สิทธิแก้ไข ลบ หรือจำกัดวัตถุประสงค์ดังกล่าวข้างต้น ผู้ควบคุมข้อมูลจะมีหน้าที่ต้องแจ้งบุคคลภายนอกที่ได้รับการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวให้ทราบถึงการใช้สิทธิของเจ้าของข้อมูลด้วย ซึ่งหากการดำเนินการเช่นว่านั้นไม่สามารถกระทำการได้อย่างแน่แท้หรือการกระทำเช่นว่านั้นจะต้องใช้ความพยายามเป็นอย่างมาก ผู้ควบคุมข้อมูลอาจได้รับยกเว้นจากหน้าที่ในการแจ้งบุคคลภายนอกได้[81] ในประเด็นเรื่องการแจ้งบุคคลภายนอกนี้ GDPR ได้เพิ่มรายละเอียดสำหรับหน้าที่ดังกล่าวเพิ่มเติมโดยกำหนดให้กรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลออกสู่บุคคลภายนอกหรือสาธารณะ เจ้าของข้อมูลมีสิทธิที่จะร้องขอข้อมูลเกี่ยวกับบุคคลที่ได้รับการเปิดเผยข้อมูลส่วนบุคคลของตนจากผู้ควบคุมข้อมูลได้ และกรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลสู่สาธารณะ ผู้ควบคุมข้อมูลจะต้องแจ้งการใช้สิทธิ

---

[81] Article 12(c) of Directive 95/46/EC

Member States shall guarantee every data subject the right to obtain from the controller:

(c) notification to third parties to whom the data have been disclosed of any retification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

ของเจ้าของข้อมูลโดยรับภาระค่าใช้จ่ายด้วยตนเองเช่นกัน ทั้งนี้เป็นไปตามมาตรา 17(2)[82] และมาตรา 19[83] ของ GDPR

(6) สิทธิในการโอนข้อมูลส่วนบุคคล (Data Portability)

สิทธิในการโอนข้อมูลส่วนบุคคลเป็นสิทธิที่เจ้าของข้อมูลมีสิทธิที่จะโอนข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองหรือดูแลของผู้ควบคุมข้อมูลรายหนึ่งไปยังผู้ควบคุมข้อมูลอีกรายหนึ่งได้ สิทธิในการโอนข้อมูลส่วนบุคคลนี้ถือเป็นสิทธิที่กำหนดเพิ่มเติมขึ้นในมาตรา 20[84] ของ GDPR ซึ่งนอกจากเจ้าของข้อมูลจะมีสิทธิในการโอนข้อมูลส่วนบุคคลแล้ว เจ้าของข้อมูล

---

[82] Article 17(2) of GDPR

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erasue the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

[83] Article 19 of GDPR

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

[84] Article 20 of GDPR

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

ยังมีสิทธิขอสำเนาข้อมูลส่วนบุคคลของตนในรูปแบบไฟล์ที่สามารถอ่านได้กับอุปกรณ์อิเล็กทรอนิกส์แต่ละประเภทด้วย

(7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

เจ้าของข้อมูลย่อมมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนโดยเป็นหน้าที่ของผู้ควบคุมข้อมูลที่จะต้องแจ้งสิทธิดังกล่าวให้แก่เจ้าของข้อมูลทราบโดยไม่ชักช้าตามมาตรา 21(4) ของ GDPR[85] ทั้งนี้ แม้ว่าการประมวลผลดังกล่าวจะเป็นไปเพื่อประโยชน์สาธารณะหรือเพื่อประโยชน์ตามกฎหมายของผู้ควบคุมข้อมูล และในกรณีเช่นว่านี้ผู้ควบคุมข้อมูลจะต้องหยุดการประมวลผลข้อมูลส่วนบุคคลดังกล่าวตามมาตรา 14(a)[86] ของ Directive 95/46/EC

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right sall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedons of others.

[85] Article 21(4) of GDPR

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

[86] Article 14(a) of Directive 95/46/EC

Member States shall grant the data subject right:

อย่างไรก็ตาม มาตรา 21(1)[87] ของ GDPR ได้เพิ่มข้อยกเว้นเพิ่มเติมว่า กรณีที่เจ้าของข้อมูลใช้สิทธิคัดค้านดังกล่าวข้างต้น ผู้ควบคุมข้อมูลอาจประมวลผลข้อมูลส่วนบุคคลต่อไปได้หากผู้ควบคุมข้อมูลสามารถแสดงให้เห็นว่ากรณีดังกล่าวจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเนื่องจากมีกฎหมายกำหนดให้ทำ ซึ่งกฎหมายดังกล่าวมีศักดิ์ที่สูงกว่าสิทธิ ผลประโยชน์และเสรีภาพของเจ้าของข้อมูล หรือหากกฎหมายบังคับให้ผู้ควบคุมข้อมูลจะต้องประมวลผลข้อมูลดังกล่าวเพื่อที่จะก่อ ดำเนินการหรือโต้แย้งซึ่งสิทธิตามกฎหมาย

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

[87] Article 21(1) of GDPR

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demostates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

นอกจากนี้ มาตรา 14(b)[88] ของ Directive 95/46/EC และมาตรา 21(2),(3)[89] ของ GDPR ยังขยายสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลไปถึงกรณีที่ผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อการตลาดโดยตรง (Direct marketing) รวมถึงการคัดค้านการประมวลผลที่มีวัตถุประสงค์เกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ และสถิติศาสตร์ได้ตามมาตรา 21(6)[90] ของ GDPR

---

[88] Article 14(b) of Directive 95/46/EC

Member States shall grant the data subject the right:

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or uses.

[89] Article 21(2)-(3) of GDPR

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

[90] Article 21(6) of GDPR

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

4.2.3.7 หน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

แต่เดิมภายใต้ Directive 95/46/EC เฉพาะผู้ควบคุมข้อมูลเท่านั้นที่มีหน้าที่ต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม เนื่องจากในปัจจุบันผู้ประมวลผลข้อมูลมักจะเป็นบุคคลคนละคนกับผู้ควบคุมข้อมูล อีกทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลยังมีบทบาทที่แตกต่างกันอีกด้วย ดังนั้น เมื่อ GDPR มีผลใช้บังคับจึงกำหนดหน้าที่ของผู้ประมวลผลข้อมูลเพิ่มเติมขึ้นมา โดยภายใต้ Directive 95/46/EC และ GDPR ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะมีหน้าที่ดังต่อไปนี้

<u>หน้าที่ของผู้ควบคุมข้อมูล</u>

(1) หน้าที่ตรวจสอบว่าการประมวลผลดังกล่าวอยู่ภายใต้หลักการประมวลผลที่ชอบด้วยกฎหมาย

ผู้ควบคุมข้อมูลจะต้องทำให้แน่ใจว่าการประมวลผลข้อมูลส่วนบุคคลนั้นอยู่ภายใต้หลักการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายหรือภายใต้ข้อกำหนดตามที่บัญญัติไว้ใน Directive 95/46/EC และ GDPR ทั้งนี้ ตามมาตรา 6(2)[91] ของ Directive 95/46/EC และมาตรา 24[92] ของ GDPR นอกจากนี้ GDPR ยังกำหนดเพิ่มเติมต่อไปให้ผู้ควบคุมข้อมูลต้อง

---

[91] Article 6(2) of Directive 95/46/EC

2. It shall be for the controller to ensure that paragraph 1 is complied with.

[92] Article 24 of GDPR

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

สามารถแสดงให้เห็นด้วยว่าการประมวลผลดังกล่าวชอบด้วยกฎหมายอย่างไร อาทิ มีการปรับใช้วิธีการทางเทคนิคและแนวทางการจัดการข้อมูลส่วนบุคคลที่เหมาะสม เป็นต้น

(2) หน้าที่จัดเตรียมข้อตกลงเกี่ยวกับผู้ควบคุมข้อมูลร่วมกัน (joint controller) ให้เจ้าของข้อมูลสามารถเข้าถึงได้

เนื่องจากในการประมวลผลข้อมูลส่วนบุคคลในทางปฏิบัตินั้นย่อมมีความเป็นไปได้ที่ผู้ควบคุมข้อมูลจะเป็นบุคคลตั้งแต่สองคนขึ้นไป ทั้งนี้ เพราะการตัดสินใจเกี่ยวกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล (ได้แก่ การกำหนดจุดมุ่งหมายของการประมวลผล วิธีการประมวลผล เป็นต้น) สามารถร่วมกันตัดสินใจกับบุคคลหลายฝ่ายได้ ดังนั้น ในทางปฏิบัติจึงปรากฏกรณีที่ผู้ควบคุมข้อมูลมีหลายคนได้ อย่างไรก็ตาม หลักการว่าด้วยผู้ควบคุมข้อมูลร่วมกันกลับไม่ปรากฏเป็นบทบัญญัติเฉพาะใน Directive 95/46/EC แต่เมื่อถึงคราวการยกร่าง GDPR จึงได้กำหนดบทบัญญัติเฉพาะว่าด้วยผู้ควบคุมข้อมูลร่วมกันในมาตรา 26(1)[93] ซึ่งกำหนดให้ผู้ควบคุมข้อมูลร่วมกันจะต้องแบ่งส่วนในการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลอีกรายหนึ่ง ซึ่งรายละเอียดของการแบ่งส่วนการปฏิบัติตามข้างต้นจะต้องจัดให้เจ้าของข้อมูลสามารถเข้าถึงได้ด้วยเช่นกัน

---

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstate compliance with the obligations of the controller.

[93] Article 26(1) of GDPR

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

การแบ่งส่วนในการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลนี้ส่งผลโดยตรงต่อความรับผิดระหว่างผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูลร่วมกัน โดยมาตรา 23(2)[94] ของ Directive 95/46/EC กำหนดไว้ว่าผู้ควบคุมข้อมูลอาจหลุดพ้นจากความรับผิดทั้งหมดหรือบางส่วน ถ้าสามารถพิสูจน์ได้ว่าตนไม่มีหน้าที่ต้องรับผิดสำหรับเหตุการณ์ดังกล่าวที่ก่อให้เกิดความเสียหายเกิดขึ้น นอกจากนี้มาตรา 26(3)[95] และมาตรา 82(3)-(5)[96] ของ GDPR ยังกำหนดเพิ่มเติมไปในกรณีที่ผู้ควบคุมข้อมูลร่วมกันคนใดหนึ่งชดใช้ความเสียหายไป บุคคลดังกล่าวย่อมมีสิทธิเรียกร้องให้ผู้ควบคุมข้อมูลรายอื่นชดใช้ความเสียหายที่ตนได้เสียแทนไปได้ตามสัดส่วนแห่งความรับผิดของตน

---

[94] Article 23(2) of Directive 95/46/EC

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to damage.

[95] Article 26(3) of GDPR

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

[96] Article 82(3)-(5) of GDPR

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraph 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

(3) หน้าที่แต่งตั้งผู้แทนในกรณีที่ผู้ควบคุมข้อมูลก่อตั้งอยู่ภายนอกสหภาพยุโรป

ในกรณีที่ผู้ควบคุมข้อมูลอยู่ภายนอกสหภาพยุโรปนั้น มาตรา 4(2)[97] ของ Directive 95/46/EC กำหนดให้ผู้ควบคุมข้อมูลจะต้องแต่งตั้งผู้แทนของตนเองภายในสหภาพยุโรปเพื่อทำหน้าที่เป็นผู้ติดต่อกับเจ้าของข้อมูลและหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) นอกจากนี้ มาตรา 4(17)[98] และมาตรา 27(1)[99] ของ GDPR ยังกำหนดเพิ่มเติมให้ครอบคลุมถึงผู้ประมวลผลข้อมูลด้วยโดยเพิ่มเติมไปว่ากรณีที่จะต้องมีการแต่งตั้งผู้ที่ทำหน้าที่แทนตน ได้แก่ กรณีที่ผู้ควบคุมข้อมูลให้บริการ ขายสินค้าหรือสอดส่องควบคุมบุคคลที่อยู่อาศัยอยู่ภายในสหภาพยุโรป (EU Residents) ยกเว้นแต่ว่าการประมวลผลดังกล่าวเป็นการประมวลผลเป็นครั้งคราวและจำนวนไม่มากซึ่งต้องไม่ใช่การประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหวง่าย (Sensitive Personal Data) ผู้ควบคุมข้อมูลอาจไม่ต้องตั้งผู้แทนของตนก็ได้

ทั้งนี้ ภายหลังที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแต่งตั้งผู้แทนของตนแล้ว ผู้แทนที่ได้รับการแต่งตั้งให้ทำหน้าที่แทนอาจจะตกอยู่ภายใต้การบังคับของหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ให้กระทำการใดๆ ในกรณีที่ผู้ควบคุมข้อมูลไม่ปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลก็ได้

---

[97] Article 4(2) of Directive 95/46/EC

2. In circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

[98] Article 4(17) of GDPR

For the purposes of this Regulation:

(17). ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

[99] Article 27(1) of GDPR

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

(4) หน้าที่ปฏิบัติตามเงื่อนไขในกรณีที่มีการแต่งตั้งผู้ประมวลผลข้อมูล

มาตรา 17(2)-(3)[100] ของ Directive 95/46/EC และมาตรา 28(1) – (3)[101] ของ GDPR อนุญาตให้บุคคลที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลสามารถมอบหมายให้ผู้ให้บริการ

---

[100] Article 17(2)-(3) of Directive 95/46/EC

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

[101] Article 28(1) – (3) of GDPR

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, this is binding on the processor with

regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an internation organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragrapgh 2 and 4 for engaging another processor;

(e) taking into account the nature of processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down un this Article and allow for

รายอื่นประมวลผลข้อมูลส่วนบุคคลในนามตนเองโดยการทำข้อตกลงหรือสัญญาเป็นลายลักษณ์อักษรได้ อย่างไรก็ตาม การดำเนินการเช่นว่านั้นจะต้องอยู่ภายใต้เงื่อนไขที่กำหนดไว้ในกฎหมาย กล่าวคือ ผู้ให้บริการและผู้ควบคุมข้อมูลจะต้องจัดข้อตกลงหรือสัญญาเป็นลายลักษณ์อักษรโดยมีรายละเอียด ดังต่อไปนี้

1. ผู้ให้บริการรายดังกล่าวจะต้องรับรองว่าตนเองได้ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
2. ผู้ให้บริการรายดังกล่าวจะต้องรับรองความปลอดภัยของข้อมูลส่วนบุคคลที่ได้รับการประมวลผล
3. ผู้ให้บริการรายดังกล่าวจะต้องกำหนดหน้าที่ให้แก่บุคคลภายใต้การกำกับดูแลของตนซึ่งทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้ชัดเจน
4. ผู้ให้บริการรายดังกล่าวจะต้องปฏิบัติตามข้อตกลงเกี่ยวกับการแต่งตั้งผู้ประมวลผลข้อมูลอีกทอดหนึ่งอย่างเคร่งครัดด้วย
5. ผู้ให้บริการรายดังกล่าวจะต้องจัดเตรียมมาตรการในการช่วยเหลือผู้ควบคุมข้อมูลในการที่จะปฏิบัติตามสิทธิของเจ้าของข้อมูล
6. ผู้ให้บริการรายดังกล่าวจะต้องให้ความช่วยเหลือผู้ควบคุมข้อมูลให้ได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ในกรณีที่หน่วยงานดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลจะต้องได้รับอนุญาตจากตน
7. ผู้ให้บริการรายดังกล่าวจะต้องกำหนดให้ผู้ควบคุมข้อมูลมีสิทธิที่จะเลือกว่าจะให้ตนส่งคืนข้อมูลส่วนบุคคลหรือทำลายข้อมูลส่วนบุคคลนั้นเมื่อความสัมพันธ์ตามข้อตกลงหรือสัญญาสิ้นสุดลงด้วย
8. ผู้ให้บริการรายดังกล่าวจะต้องจัดหาข้อมูลที่สำคัญให้แก่ผู้ควบคุมข้อมูลสำหรับการแสดงให้เห็นถึงการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของตน

---

and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion an instruction infringes this Regulation or other Union or Member State data protection provisions.

(5) หน้าที่เก็บรวบรวมบันทึกการประมวลผลข้อมูลส่วนบุคคล

มาตรา 30[102] ของ GDPR บัญญัติให้ผู้ควบคุมข้อมูลหรือผู้แทนที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลจะต้องจัดเก็บบันทึกของการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยผู้ควบคุมข้อมูลและบันทึกดังกล่าวจะต้องปรากฏรายละเอียดอย่างน้อย ดังต่อไปนี้

---

[102] Article 30 of GDPR

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the catagories of personal data;

(d) the categories of recipient to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organization security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

1. รายละเอียดข้อตกลงหรือสัญญาของผู้ควบคุมข้อมูลหรือผู้แทนที่ได้รับจากแต่งตั้งจากผู้ควบคุมข้อมูล
2. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
3. ประเภทของเจ้าของข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่ถูกประมวลผล
4. ประเภทของผู้รับหรือผู้ที่ข้อมูลส่วนบุคคลจะถูกเปิดเผยด้วย
5. รายละเอียดเกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศ เป็นต้น

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

บันทึกการประมวลผลข้างต้น GDPR กำหนดให้ผู้ควบคุมข้อมูลหรือผู้แทนจะต้องจัดเก็บเพื่อที่จะเปิดเผยให้แก่หน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ในกรณีที่หน่วยงานดังกล่าวได้ร้องขอด้วย

นอกจากนี้ในบทบัญญัติเดียวกันนั้น แต่เดิมมาตรา 18[103] ของ Directive 95/46/EC กำหนดให้ก่อนการประมวลผลข้อมูลส่วนบุคคลทุกครั้ง ผู้ควบคุมข้อมูลจะต้อง

---

[103] Article 18 of Directive 95/46/EC

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to

แจ้งการประมวลผลดังกล่าวให้แก่หน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ทราบทุกครั้ง ซึ่งก่อให้เกิดความไม่คล่องตัวในการให้บริการ ดังนั้น GDPR จึงได้บัญญัติยกเลิกหน้าที่ดังกล่าวและกำหนดให้คงไว้เพียงหน้าที่เก็บบันทึกการประมวลผลข้อมูลส่วนบุคคลเพื่อส่งมอบให้แก่หน่วยงานข้างต้นเมื่อมีการร้องขอเท่านั้น

(6) หน้าที่ให้ความร่วมมือกับหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority)

หน้าที่ให้ความร่วมมือกับหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) นั้นจัดเป็นหน้าที่ที่ GDPR บัญญัติเพิ่มเติมจาก Directive 95/46/EC โดยกำหนดให้ผู้ควบคุมข้อมูลและผู้แทนที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลมีหน้าที่ต้องให้ความร่วมมือกับหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ทั้งนี้ ตามมาตรา 31[104] ของ GDPR

(7) หน้าที่จัดหามาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล

เนื่องจากหลักการที่กำหนดให้ผู้ควบคุมข้อมูลจะต้องจัดหามาตรการที่จะทำให้แน่ใจว่าข้อมูลส่วนบุคคลจะได้รับความปลอดภัยนั้นถือเป็นหลักการที่สำคัญของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ดังนั้น Directive 95/46/EC และ GDPR จึงกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดหามาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล ซึ่งมาตรา

---

consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification

[104] Article 31 of GDPR

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

32(1)[105] แห่ง GDPR ได้ยกตัวอย่างมาตรการสำหรับรักษาความปลอดภัยของข้อมูลส่วนบุคคลไว้ด้วย อาทิเช่น เทคโนโลยีการเข้ารหัสข้อมูล (Encryption) การสำรองข้อมูล (Back-up) การทดสอบความปลอดภัยของระบบ เป็นต้น

(8) หน้าที่รายงานการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) โดยไม่ชักช้า

หน้าที่รายงานการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ของผู้ควบคุมข้อมูลเป็นหน้าที่ที่ถูกบัญญัติเพิ่มเติมขึ้นในมาตรา 33(1)[106] ของ GDPR โดยกำหนดให้ผู้ควบคุมข้อมูลจะต้องรายงานการละเมิดข้อมูลส่วน

---

[105] Article 32(1) of GDPR

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and serverity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

[106] Article 33(1) of GDPR

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the

บุคคลไปยังหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) ภายในระยะเวลา 72 ชั่วโมง อย่างไรก็ตาม ผู้ควบคุมข้อมูลอาจได้รับยกเว้นจากหน้าที่ดังกล่าวได้หากการละเมิดข้อมูลส่วนบุคคลนั้นไม่ก่อให้เกิดอันตรายแก่สิทธิและเสรีภาพของเจ้าของข้อมูล

นอกจากการรายงานการละเมิดข้อมูลส่วนบุคคลให้แก่หน่วยงานที่รับผิดชอบตามกฎหมาย (SUppervisory Authority) แล้ว ผู้ควบคุมข้อมูลยังมีหน้าที่ต้องรายงานเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าเช่นกัน ทั้งนี้ ตามมาตรา 34(1)[107] แห่ง GDPR

<u>หน้าที่ของผู้ประมวลผลข้อมูล</u>

(1) หน้าที่แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูล

หน้าที่แจ้งคำสั่งที่ขัดหรือแย้งให้แก่ผู้ควบคุมข้อมูลนี้เป็นหน้าที่ที่ไม่ปรากฏใน Directive 95/46/EC มาก่อน โดย GDPR ได้กำหนดเพิ่มเติมไว้ในมาตรา 28(3)(h) กล่าวคือ ในกรณีที่คำสั่งของผู้ควบคุมข้อมูลขัดหรือแย้งกับบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ผู้ประมวลผลข้อมูลย่อมมีหน้าที่ต้องแจ้งคำสั่งที่ขัดหรือแย้งดังกล่าวให้แก่ผู้ควบคุมข้อมูลทราบโดยทันที

(2) หน้าที่ไม่แต่งตั้งผู้ประมวลผลข้อมูลช่วงโดยปราศจากความยินยอม

แต่เดิม Directive 95/46/EC ไม่ได้กำหนดบทบัญญัติที่ชัดเจนว่าด้วยการแต่งตั้งผู้ประมวลผลข้อมูลช่วง เนื่องจากมาตรา 16[108] ของ Directive 95/46/EC กำหนดไว้แต่

---

supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

[107] Article 34(1) of GDPR

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

[108] Article 16 of Directive 95/46/EC

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not

เพียงว่าผู้ประมวลผลข้อมูลช่วงสามารถประมวลผลข้อมูลส่วนบุคคลได้เฉพาะตามคำสั่งของผู้ควบคุมข้อมูลหรือตามที่กฎหมายกำหนดให้สามารถกระทำได้เท่านั้น ดังนั้น มาตรา 28(2) และ 28(4)[109] ของ GDPR จึงได้บัญญัติเพิ่มเติมให้ชัดเจนว่าผู้ประมวลผลข้อมูลไม่สามารถแต่งตั้งผู้ประมวลผลข้อมูลช่วงโดยปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลได้ นอกจากนี้ เมื่อผู้ควบคุมข้อมูลยินยอมให้มีการแต่งตั้งผู้ประมวลผลข้อมูลช่วงแล้ว ผู้ประมวลผลข้อมูลช่วงจะต้องตกอยู่ภายใต้บังคับของสัญญาหรือข้อตกลงระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลด้วยเช่นกัน

(3) หน้าที่รักษาความลับของข้อมูลส่วนบุคคล

เดิมมาตรา 16 ของ Directive 95/46/EC กำหนดให้ผู้ประมวลผลข้อมูลจะต้องเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นความลับยกเว้นจะเป็นคำสั่งของผู้ควบคุมข้อมูลให้เปิดเผยได้ ซึ่งสอดคล้องกับมาตรา 28(3)(b) และมาตรา 29[110] ของ GDPR ที่กำหนดให้ผู้ประมวลผลข้อมูลมีหน้าที่ทำให้แน่ใจว่าข้อมูลส่วนบุคคลที่ตนได้ประมวลผลไว้นั้นจะถูกเก็บรักษาเป็นความลับ ทั้งนี้ ข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องกำหนดให้ผู้ที่อยู่

---

process them except on instructions from the controller, unless he is required to do so by law.

[109] Article 28(4) of GDPR

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligation as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

[110] Article 29 of GDPR

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

ภายใต้การกำกับดูแลของผู้ประมวลผลข้อมูลมีหน้าที่จัดเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวให้เป็นความลับด้วย

(4) หน้าที่ประมวลผลข้อมูลส่วนบุคคลภายในขอบวัตถุประสงค์

มาตรา 16 ของ Directive 95/46/EC และมาตรา 29 ของ GDPR กำหนดหลักการที่สำคัญของการประมวลผลข้อมูลในฐานะผู้ประมวลผลข้อมูล กล่าวคือ ผู้ประมวลผลข้อมูลจะต้องไม่ประมวลผลข้อมูลส่วนบุคคลยกเว้นจะมีคำสั่งของผู้ควบคุมข้อมูลให้สามารถประมวลผลข้อมูลส่วนบุคคลนั้นๆ ได้ ทั้งนี้ หากผู้ประมวลผลข้อมูลประมวลผลข้อมูลนอกเหนือไปจากคำสั่งที่ผู้ควบคุมข้อมูลกำหนดไว้ กรณีจะถือว่าผู้ประมวลผลเป็นผู้กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นๆ เองและผู้ประมวลผลย่อมมีสถานะเป็นผู้ควบคุมข้อมูลในเรื่องดังกล่าวด้วย ตามมาตรา 28(10)[111] แห่ง GDPR

(5) หน้าที่บันทึกการประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล

มาตรา 30(2) ของ GDPR ได้บัญญัติให้ผู้ประมวลผลข้อมูลมีหน้าที่ต้องบันทึกการประมวลผลข้อมูลแทนผู้ควบคุมข้อมูลด้วยโดยบันทึกดังกล่าวต้องมีรายละเอียดเช่นเดียวกับที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดทำบันทึกข้างต้น ทั้งนี้ หน้าที่บันทึกการประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูลนี้ไม่ปรากฏใน Directive 95/46/EC แต่อย่างใดเนื่องจาก Directive 95/46/EC ไม่ปรากฏบทบัญญัติใดๆ ที่เกี่ยวข้องกับผู้ประมวลผลข้อมูลโดยตรง

(6) หน้าที่ให้ความร่วมมือกับหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority)

เช่นเดียวกับหน้าที่ของผู้ควบคุมข้อมูล มาตรา 31 ของ GDPR กำหนดให้ผู้ประมวลผลข้อมูลมีหน้าที่จะต้องให้ความร่วมมือกับหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority)

---

[111] Article 28(10) of GDPR

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

(7) หน้าที่จัดหามาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล

เช่นเดียวกับหน้าที่ของผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูลย่อมมีหน้าที่ต้องจัดหามาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย โดยผู้ควบคุมข้อมูลควรกำหนดหน้าที่จัดหามาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลนี้ในสัญญาหรือข้อตกลงระหว่างตนและผู้ประมวลผลข้อมูลด้วย หากผู้ประมวลผลข้อมูลฝ่าฝืนหน้าที่ในการจัดหามาตรการรักษาความปลอดภัย ผู้ประมวลผลข้อมูลอาจต้องรับผิดในค่าปรับอาญา เบี้ยปรับ หรือเงินเพิ่มต่างๆ ตามที่กฎหมายกำหนดด้วย

(8) หน้าที่รายงานการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory AUthority) โดยไม่ชักช้า

เช่นเดียวกับหน้าที่ของผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูลย่อมมีหน้าที่ต้องรายงานการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่รับผิดชอบตามกฎหมาย (Supervisory Authority) โดยไม่ชักช้า ทั้งนี้ ตามที่กำหนดไว้ในมาตรา 33(2)[112] ของ GDPR

(9) หน้าที่ปฏิบัติตามหลักเกณฑ์ว่าด้วยการส่งหรือโอนข้อมูลระหว่างประเทศ

ภายใต้ GDPR ผู้ประมวลผลมีหน้าที่โดยตรงในการปฏิบัติตามบทบัญญัติว่าด้วยการส่งหรือโอนข้อมูลระหว่างประเทศด้วย

จากบทบัญญัติต่างๆ ข้างต้นที่กำหนดหน้าที่ให้แก่ผู้ประมวลผลข้อมูลจะเห็นได้ว่าผู้ประมวลผลข้อมูลเริ่มเข้ามามีบทบาทในสายตาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ดังนั้น หากข้อเท็จจริงปรากฏว่าเจ้าของข้อมูลได้รับความเสียหายใดๆ อันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลของตน เช่น มีการละเมิดข้อมูลส่วนบุคคลของตน เจ้าของข้อมูลย่อมสามารถเรียกร้องให้ผู้ประมวลผลข้อมูลรับผิดได้โดยตรง ทั้งนี้ ภายใต้เงื่อนไขที่ว่าความเสียหายดังกล่าวจะต้องเกิดจากการประมวลผลข้อมูลของผู้ประมวลผลโดยเป็นการประมวลผลที่ไม่ปฏิบัติตามบทบัญญัติของ GDPR ที่กำหนดไว้เกี่ยวกับผู้ประมวลผลโดยตรงหรือเป็นการประมวลผลที่ขัดแย้งกับคำสั่งของผู้ควบคุมข้อมูลหรือดำเนินการนอกเหนือไปจากคำสั่งตามกฎหมายของผู้ควบคุมข้อมูล

---

[112] Article 33(2) of GDPR

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

4.2.3.8 การส่งหรือโอนข้อมูลระหว่างประเทศ

โดยหลักตามมาตรา 25(1)-(5)[113] และมาตรา 26(1)-(2)[114] ของ Directive 95/46/EC และ มาตรา 44[115] และมาตรา 45(1)[116] ของ GDPR นั้น การส่งหรือโอนข้อมูล

---

[113] Article 25 of Directive 95/46/EC

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

[114] Article 26(1) – (2) of Directive 95/46/EC

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the

ส่วนบุคคลเพื่อการประมวลผลหรือเพื่อการอื่นไปยังประเทศที่มิได้เป็นสมาชิกของสหภาพยุโรป<u>ย่อมต้องห้าม</u> เว้นเสียแต่ว่า

(1) ประเทศที่รับโอนข้อมูลนั้นจะได้ให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (Adequate level) ทั้งนี้ หากประเทศที่รับโอนข้อมูลนั้นเข้าลักษณะเป็นประเทศที่คณะกรรมการได้ประกาศให้ประเทศดังกล่าวเป็นประเทศที่ถือว่าให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอแล้ว ผู้โอนหรือส่งข้อมูลย่อมสามารถโอนหรือส่งข้อมูลดังกล่าวได้โดยตรง เช่น ประเทศแคนาดา อาร์เจนตินา อิสลาเอล สวิตเซอร์แลนด์ นิวซีแลนด์ อุรุกวัย เป็นต้น สำหรับประเทศรอบๆ ประเทศไทย ขณะนี้คณะกรรมการกำลังอยู่ในระหว่างการพิจารณาประเทศญี่ปุ่นและประเทศเกาหลีใต้ ซึ่งคาดว่าการพิจารณาจะแล้วเสร็จในปี พ.ศ. 2561 ประเทศที่คณะกรรมการได้ประกาศให้เป็นประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอนั้นจะคงสถานะเช่นว่า

---

corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

[115] Article 44 of GDPR

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

[116] Article 45(1) of GDPR

1. A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

นั้นไว้เป็นระยะเวลาสูงสุดไม่เกินกว่า 4 ปี หมายความว่า ทุกๆ 4 ปี คณะกรรมการจะต้องพิจารณาความเห็นอีกครั้งว่าประเทศดังกล่าวยังคงเป็นประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอเช่นเดิมหรือไม่ ซึ่งหลักเกณฑ์นี้เป็นหลักเกณฑ์ที่กำหนดเพิ่มเติมมาไว้ในมาตรา 45(3)[117] ของ GDPR ทั้งนี้ ในการพิจารณาของคณะกรรมการว่าประเทศถือว่ามีมาตรฐานระดับที่เพียงพอหรือไม่ คณะกรรมการจะอาศัยหลักเกณฑ์ตามมาตรา 45(2)[118] ของ GDPR (ซึ่งแตกต่างไปจากที่กำหนดไว้ใน Directive 95/46/EC เดิม) ดังนี้

---

[117] Article 45(3) of GDPR

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organization ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organization. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

[118] Article 45 (2) of GDPR

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as

- บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน
- การเข้าถึงข้อมูลที่รับโอนโดยองค์กรหรือหน่วยงานสาธารณะ
- การมีอยู่และประสิทธิภาพของหน่วยงานคุ้มครองข้อมูลส่วนบุคคล
- หน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลของประเทศนั้นๆ

(2) ผู้ส่งหรือโอนข้อมูลส่วนบุคคลมีมาตรการรักษาความปลอดภัยที่เหมาะสม (Appropriate safeguard) ซึ่งสามารถปกป้องสิทธิของเจ้าของข้อมูลตามที่กำหนดไว้ในมาตรา 46 ซึ่งเป็นกรณี GDPR เปิดช่องให้ผู้ส่งหรือโอนข้อมูลสามารถส่งหรือโอนข้อมูลไปยังประเทศที่ไม่มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอตาม (1) ได้เพราะผู้ส่งหรือโอนข้อมูลส่วนบุคคลสามารถให้ความคุ้มครองข้อมูลส่วนบุคคลได้นั่นเอง มาตรการรักษาความปลอดภัยที่เหมาะสมนั้นสามารถจัดให้มีขึ้นได้โดยไม่ต้องได้รับการอนุมัติจากคณะกรรมการ โดยอาศัย

- ข้อตกลงระหว่างหน่วยงานภาครัฐซึ่งเป็นประเทศสมาชิกสหภาพยุโรปและไม่ใช่สมาชิกสหภาพยุโรป เช่น ข้อตกลง “Privacy Sheild” ระหว่างสหภาพยุโรปและสหรัฐอเมริกา
- นโยบายหรือหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules: BCRs) ซึ่งได้รับการอนุมัติจากหน่วยงานคุ้มครองข้อมูลส่วนบุคคล (Supervisory Authority) ด้วย โดยเป็นการอนุมัติเพียงครั้งเดียวสำหรับการส่งหรือโอนข้อมูล

---

well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

ระหว่างบริษัทในเครือในอนาคตโดยไม่ต้องขออนุมัติอีก สำหรับกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือซึ่งตั้งอยู่ในประเทศนอกสหภาพยุโรป

- ข้อความที่กำหนดมาตรฐานพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล (Standard Contractual Clause) ซึ่งได้รับการพิจารณาจากคณะกรรมการตาม GDPR หรือ Supervisory authority ของแต่ละประเทศซึ่งเป็นประเทศต้นทางของข้อมูล
- Code of conduct ที่ได้รับการอนุมัติและคำรับรองของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลในประเทศนอกสหภาพยุโรปที่รับโอนข้อมูลว่าได้ใช้มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่จะปกป้องสิทธิของเจ้าของข้อมูลแล้ว
- ใบรับรองที่ได้รับอนุมัติ (approved certification) และคำรับรองของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลในประเทศนอกสหภาพยุโรปที่รับโอนข้อมูลว่าได้ใช้มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่จะปกป้องสิทธิของเจ้าของข้อมูลแล้ว

และบางกรณีมาตรการรักษาความปลอดภัยที่เหมาะสม (Appropriate safeguard) ที่จัดให้มีขึ้นโดยอาศัยข้อสัญญาหรือข้อตกลงดังต่อไปนี้ จะต้องได้รับอนุมัติจาก Supervisory authority ก่อน

- ข้อสัญญา (Contractual clauses) ระหว่างผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล (ผู้ส่ง) และผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล ผู้รับโอนข้อมูลส่วนบุคคลในประเทศที่รับโอนข้อมูลซึ่งไม่มีมาตรฐานในระดับที่เพียงพอ หรือองค์กรระหว่างประเทศซึ่งเป็นผู้รับโอนข้อมูล
- ข้อกำหนดสำหรับการดำเนินการบริหารจัดการระหว่างองค์กรของรัฐหรือหน่วยงานใดๆ ซึ่งต้องระบุถึงสิทธิของเจ้าของข้อมูล

(3) กรณีมีเหตุการณ์พิเศษตามมาตรา 49 ให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้เป็นกรณีพิเศษแม้ว่าประเทศผู้รับโอนจะไม่มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอตามข้อ (1) และไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสมตามข้อ (2) ซึ่งได้แก่

- เจ้าของข้อมูลให้ความยินยอมให้สามารถกระทำได้อย่างชัดแจ้งภายหลังได้รับแจ้งความเสี่ยงที่อาจเกิดขึ้นได้อันเนื่องมาจากประเทศผู้รับโอนไม่มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอและไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสม
- การส่งหรือโอนข้อมูลส่วนบุคคลที่จำเป็นต้องกระทำเพื่อปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลและผู้ควบคุมข้อมูล เพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูล

และบุคคลอื่นซึ่งเป็นประโยชน์แก่เจ้าของข้อมูล เพื่อประโยชน์สาธารณะ เพื่อให้เป็นไปตามสิทธิเรียกร้องตามกฎหมาย เพื่อปกป้องชีวิตของเจ้าของข้อมูลหรือบุคคลอื่นในกรณีที่เจ้าของข้อมูลไม่อาจให้ความยินยอมได้ไม่ว่าโดยสภาพหรือโดยกฎหมาย เป็นต้น

ดังนั้น จะเห็นได้ว่าแม้ว่าโดยหลักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศซึ่งมิใช่สมาชิกของสหภาพยุโรปจะเป็นสิ่งที่ต้องห้ามก็ตาม แต่ GDPR ก็ได้เปิดช่องทางในการส่งหรือโอนข้อมูลส่วนบุคคลที่จะต้องได้รับอนุมัติจากหน่วยงานคุ้มครองข้อมูลส่วนบุคคลหลายช่องทางเพื่อให้ธุรกิจหรือการค้าระหว่างประเทศสามารถดำเนินต่อไปได้โดยไม่ก่อให้เกิดอุปสรรคจนเกินความจำเป็น ไม่ว่าจะเป็นการโอนหรือส่งข้อมูลโดยอาศัยความยินยอมของเจ้าของข้อมูลหรือโดยอาศัยข้อตกลงระหว่างผู้โอนข้อมูลและผู้รับข้อมูลซึ่งได้รับอนุมัติจากจากหน่วยงานคุ้มครองข้อมูลแล้ว (Ad hoc clauses) เป็นต้น

อย่างไรก็ตาม หากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลให้แก่ผู้รับในประเทศที่สามหรือองค์กรระหว่างประเทศที่ฝ่าฝืนต่อหลักเกณฑ์ข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีโทษปรับสูงสุด 20 ล้านยูโร หรือ 4% ของรายได้ประจำปีทั่วโลก แล้วแต่อย่างใดจะมากกว่ากัน

4.3 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศที่มีผลการประเมินความพร้อมในเกณฑ์ดี

4.3.1 ประเทศญี่ปุ่น

ดังที่ได้กล่าวไว้แล้วข้างต้นว่าประเทศญี่ปุ่นเป็นประเทศที่มีความพร้อมในการให้บริการระบบการประมวลผลแบบคลาวด์เป็นอันดับแรกจากการจัดอันดับของกลุ่มพันธมิตรธุรกิจซอฟต์แวร์ หรือบีเอสเอ ดังนั้น การศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นจึงเป็นประโยชน์ต่อการยกร่างกฎหมายของประเทศอื่นๆ รวมถึงประเทศไทยด้วยเช่นกัน ทั้งนี้ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น มีสาระสำคัญ ดังต่อไปนี้

4.3.1.1 ความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น

แต่เดิมประเทศญี่ปุ่นใช้ระบบการควบคุมตนเอง (self-regulation) ในการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชน ทำให้ปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลรุนแรงมากยิ่งขึ้นนับตั้งแต่ปี ค.ศ. 1990 เป็นต้นมา เช่น กรณีที่บริษัทเอกชนลักลอบทำการศึกษาวิจัยเกี่ยวกับการทดลองทางพันธุกรรมโดยการเก็บตัวอย่างเลือดจากประชาชนพันกว่าคนที่ได้บริจาคเลือดให้แก่สภากาชาดของประเทศญี่ปุ่น เป็นต้น[119] จนกระทั่งในปีค.ศ. 1999 (พ.ศ. 2542) รัฐบาลของประเทศญี่ปุ่นได้ให้ความสำคัญกับการละเมิดความเป็นส่วนตัว การขยายตัวของสังคมข้อมูลข่าวสาร เครือข่ายสารสนเทศนานาชาติและระบบพาณิชย์อิเล็กทรอนิกส์ทั้งในประเทศญี่ปุ่นเองและในขอบเขตทั่วโลก ดังนั้น รัฐบาลของประเทศญี่ปุ่นจึงได้ประกาศโครงการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาโดยอาศัยหลักการพื้นฐาน 5 ประการ ดังนี้

1. จะต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลให้ชัดเจนและจัดระบบข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ประกาศไว้
2. การจัดเก็บข้อมูลส่วนบุคคลจะต้องกระทำโดยชอบด้วยกฎหมายและใช้วิธีการที่เหมาะสม
3. ต้องเก็บรักษาและปรับปรุงข้อมูลให้ถูกต้องและทันสมัยอยู่เสมอ
4. ต้องจัดระบบรักษาความปลอดภัยให้แก่ข้อมูลส่วนบุคคลที่จัดเก็บ
5. ต้องจัดระบบการจัดเก็บและใช้ข้อมูลส่วนบุคคลภายใต้หลักความโปร่งใส

คณะรัฐมนตรีญี่ปุ่นได้พิจารณาร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเมื่อเดือนมีนาคม ค.ศ. 2000 (พ.ศ. 2543) และได้ส่งร่างนี้ให้แก่รัฐสภาพิจารณาในปีค.ศ.

---

[119] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 21*, น.189.

2001 (พ.ศ. 2544) อย่างไรก็ตามปรากฏว่ามีผู้คัดค้านร่างกฎหมายดังกล่าว โดยเฉพาะอย่างยิ่งจากพรรคการเมืองฝ่ายค้านในสมัยนั้น โดยให้เหตุผลว่าหลักการยกร่างทั้ง 5 ประการดังกล่าวข้างต้นมีความหมายที่กว้างจน เป็นเหตุให้เจ้าหน้าที่ของรัฐอาจใช้อำนาจควบคุมได้อย่างกว้างขวางและอาจมีผลกระทบต่อเสรีภาพในการแสดงความเห็นตามรัฐธรรมนูญของประเทศญี่ปุ่นได้ ส่งผลให้การพิจารณาร่างกฎหมายฉบับนี้ยืดเยื้อออกไปจนกระทั่งพ้นสมัยประชุมในเดือนธันวาคม ค.ศ. 2002 (พ.ศ. 2545) ดังนั้น คณะรัฐมนตรีในขณะนั้นจึงรับร่างที่ยังค้างการพิจารณากลับไปทบทวนอีกครั้งหนึ่งเพื่อปรับแก้ไขร่างในหลายประเด็นโดยปรับวิธีการยกร่างจากการกำหนดบทบัญญัติในรายละเอียดเป็นการกำหนดบทบัญญัติเป็นหลักการกว้างๆ แทน จนกระทั่งในเดือนมีนาคม ค.ศ. 2003 (พ.ศ. 2546) คณะรัฐมนตรีจึงได้นำร่างที่แก้ไขใหม่เสนอต่อรัฐสภาอีกครั้ง ต่อมาเมื่อวันที่ 23 พฤษภาคม ค.ศ. 2003 (พ.ศ. 2546) รัฐสภาของประเทศญี่ปุ่นได้พิจารณาร่างที่นำเสนอโดยคณะรัฐมนตรีและตราเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อใช้บังคับเป็นกฎหมายทั่วไปสำหรับทั้งภาครัฐและภาคเอกชนโดยเรียกชื่อว่า “The Act on the Protection of Personal Information (Law No. 57 of 2003)” หรือ “APPI” พร้อมกันกับการตรากฎหมายอื่นที่เกี่ยวข้องอีก 4 ฉบับ ได้แก่ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลของหน่วยงานฝ่ายปกครอง กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลขององค์กรอิสระและองค์การมหาชนอื่นๆ กฎหมายเกี่ยวกับการจัดตั้งคณะกรรมการวินิจฉัยการเปิดเผยและการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการตระเตรียมการบังคับการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในความครอบครองดูแลของหน่วยงานฝ่ายปกครอง[120]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นมีผลใช้บังคับเมื่อ ค.ศ. 2005 (พ.ศ. 2548) และใช้บังคับต่อมาจนกระทั่งในเมื่อวันที่ 9 กันยายน ค.ศ. 2015 (พ.ศ. 2558) จึงได้มีการตรากฎหมายออกมาปรับปรุงแก้ไขกฎหมายฉบับเดิมซึ่งพระราชบัญญัติที่ออกมาแก้ไขนี้มีผลใช้บังคับวันที่ 1 กุมภาพันธ์ ค.ศ. 2016 (พ.ศ. 2559) ทั้งนี้ การปรับปรุงแก้ไขกฎหมายดังกล่าวมีวัตถุประสงค์เพื่อรองรับการใช้งาน Big data และการจัดการข้อมูลข้ามพรมแดนระหว่างประเทศโดยเฉพาะอย่างยิ่งในระบบการประมวลผลแบบคลาวด์[121] รวมทั้งเพื่อกำหนดกฎเกณฑ์ว่า

---

[120]กิตติศักดิ์ ปรกติ, “กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น,” วารสารนิติศาสตร์, เล่มที่ 4, ปีที่ 34, น.514, (ธันวาคม 2547).

[121]DPL Piper, “New amendments to Japanese privacy law,” สืบค้นเมื่อวันที่ 28 กุมภาพันธ์ 2560, จาก https://www.dlapiper.com/en/japan/insights/publications/2015/09/new-amendments-to-japanese-privacy-law/

ด้วยการเปิดเผยข้อมูลส่วนบุคคลให้ชัดเจนอันเนื่องมาจากการเก็บข้อมูลส่วนบุคคลของบริษัทรถไฟตะวันออกของญี่ปุ่น (East Japan Railways Company: “JR”) ผ่านการใช้บัตรโดยรถไฟฟ้าที่เรียกว่า “Suica Card”

การปรับปรุงแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นนี้เป็นการปรับปรุงแก้ไขในหลายประเด็น ได้แก่ การปรับปรุงบทนิยามของข้อมูลที่จะได้รับความคุ้มครองภายใต้กฎหมายดังกล่าว พร้อมทั้งกำหนดข้อมูลที่จะได้รับความคุ้มครองเพิ่มขึ้นอีก 2 ประเภท คือ ข้อมูลที่อ่อนไหว (Sensitive Information) และข้อมูลนิรนาม (Anonymized Information) การปรับปรุงแก้ไขหลักการเรื่องการโอนหรือเปิดเผยข้อมูลต่อบุคคลที่สามโดยไม่ต้องได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลล่วงหน้าหากเป็นไปตามเงื่อนไขหรือพฤติการณ์ที่กำหนดไว้และการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ การเพิ่มโทษสำหรับผู้ที่ไม่ปฏิบัติตามกฎหมาย และการเพิ่มบทบัญญัติว่าด้วยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะได้ศึกษาโดยละเอียดต่อไป

4.3.1.2 สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นหรือ APPI แบ่งออกเป็น 6 ส่วนหลัก ได้แก่ บทบัญญัติทั่วไป หน้าที่ของรัฐบาลและองค์กรปกครองท้องถิ่น มาตรการในการคุ้มครองข้อมูลส่วนบุคคล หน้าที่ของผู้ประกอบการที่จัดการงานเกี่ยวกับข้อมูลส่วนบุคคล บทบัญญัติเบ็ดเตล็ด และบทลงโทษ

APPI มีขอบเขตการให้ความคุ้มครองเฉพาะข้อมูลส่วนบุคคลเท่านั้น ข้อมูลอื่นๆ เช่น ข้อมูลทั่วๆ ไป หรือข้อมูลความลับทางการค้าจะไม่อยู่ภายใต้บังคับของกฎหมายฉบับนี้ แต่อาจอยู่ภายใต้บังคับของกฎหมายอื่น ซึ่งไม่อยู่ในขอบเขตของการศึกษาในครั้งนี้ เช่น the Unfair Competition Prevention Act ที่ให้ความคุ้มครองข้อมูลทางการค้าโดยเฉพาะ เป็นต้น และ APPI จะบังคับใช้เฉพาะกับผู้ควบคุมข้อมูลที่ตั้งอยู่ในประเทศญี่ปุ่นซึ่งหมายถึงองค์กรที่ใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ในทางธุรกิจของตน แต่ไม่รวมถึงหน่วยงานของรัฐ องค์กรปกครองส่วนท้องถิ่น หน่วยงานอิสระหรือหน่วยงานที่ถือครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลไม่เกิน 5,000 คนในระยะเวลา 6 เดือนที่ผ่านและ APPI จะใช้เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ทั้งในความครอบครองของหน่วยงานรัฐและหน่วยงานเอกชน โดยมุ่งหมายจะวางหลักกฎหมายทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ โดยคำนึงถึงความจำเป็นในการเอื้ออำนวยให้การประกอบการค้าและธุรกิจในยุคข้อมูลข่าวสารสามารถดำเนินไปได้ รวมทั้งคำนึงถึงสิทธิและผลประโยชน์ของบุคคลประกอบด้วย เพื่อให้ประชาชนชาวญี่ปุ่นมีคุณภาพชีวิตที่ดีในการใช้งานแอพพลิเคชั่นต่างๆ

APPI มีหลักการจัดการข้อมูลส่วนบุคคลที่สำคัญ 4 ประการ คือ (1) กำหนดแนวคิดพื้นฐานของรัฐบาล (2) กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล (3) กำหนดรายละเอียดหน้าที่รับผิดชอบของบุคคลที่เกี่ยวเนื่องกับการคุ้มครองข้อมูลส่วนบุคคล และ (4) กำหนดความรับผิด[122]

ทั้งนี้ ภายใต้ APPI ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับการดำรงชีวิตของบุคคลซึ่งมีลักษณะประการใดประการหนึ่ง ดังต่อไปนี้[123]

---

[122] Article 1 of APPI

The purpose of this Act is to protect the rights and interests of individuals while taking consideration of the usefulness of personal information, in view of a remarkable increase in the utilization of personal information due to development of the advanced information and communications society, by clarifying the responsibilities of the State and local governments, etc. with laying down basic principle, establishment of a basic policy by the Government and the matters to serve as a basis for other measures on the protection of personal information, and by prescribing the duties to be observed by entities handling personal information, etc., regarding the proper handling of personal information.

[123] Article 2 (1) of APPI

(1) The term "personal information" as used in this Act means information about a living individual, and falls under one of the following items:

(i) information that can be used to identify that specific individual due to its inclusion of a name, date of birth, or other description contained (any and all matters (that excludes individual identification codes) written, recorded or otherwise expressed using voice, movement or other methods in documents, drawings or electromagnetic records (meaning records made by electromagnetic format (electronic, magnetic or any other format that cannot be recognized through the human senses; the same applies in next paragraph, item (ii)); the same applies in Article 18, paragraph (2); the same applies hereinafter) in such information (this includes any information that can be cross-checked against other information and thereby used to identify that specific individual).

1) ข้อมูลที่สามารถใช้ระบุบ่งตัวตนของบุคคลได้ เช่น ชื่อ วันเดือนปีเกิด หรือข้อมูลข่าวสารอื่นๆ ที่ถูกจัดเก็บเป็นลายลักษณ์อักษร บันทึก หรือเสียง หรือด้วยวิธีการอื่นใดในเอกสาร ภาพวาด สื่อบันทึกอิเล็กทรอนิกส์ เป็นต้น
2) ข้อมูลที่ระบุรหัสการบ่งตัวตนของบุคคลได้ ซึ่งหมายถึงคุณลักษณะ อักษร ตัวเลข สัญลักษณ์ หรือเครื่องหมายอื่นใดที่สามารถแปลงเป็นความหมายโดยอาศัยเครื่องคอมพิวเตอร์ได้ หรือข้อมูลอื่นใดที่สามารถบ่งตัวตนของบุคคลได้

ข้อมูลที่อ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่บรรจุลักษณะที่กำหนดไว้โดยคำสั่งของคณะรัฐมนตรีซึ่งจำเป็นพิเศษในการจัดการข้อมูลดังกล่าว เพื่อหลีกเลี่ยงความไม่เป็นธรรมหรือความเสียเปรียบของบุคคลทางด้านสัญชาติ เชื้อชาติ สถานะทางสังคม ประวัติการรักษา ประวัติอาชญากรรม ความเชื่อทางศาสนา เป็นต้น[124]

ฐานข้อมูลส่วนบุคคล หมายถึง ระบบข้อมูลข่าวสารที่เก็บรวบรวมข้อมูลต่างๆ ซึ่งมีข้อมูลส่วนบุคคลรวมอยู่ด้วย ไม่ว่าจะเป็นระบบที่สามารถเรียกดูข้อมูลส่วนบุคคลที่เจาะจงได้โดยใช้เครื่องคอมพิวเตอร์ หรือเป็นระบบที่อาจตรวจดูข้อมูลส่วนบุคคลที่เจาะจงได้โดยง่ายโดยวิธีอื่นใด ทั้งนี้ตามที่ประกาศในคำสั่งของคณะรัฐมนตรี[125]

(ii) Information that contains individual identification codes

[124] Article 2(3) of APPI

(3) The term “sensitive personal information” used in this Act means a personal informationthat contains descriptions that have been specified by Cabinet Order to require specialconsideration in handling so as to avoid any unfair discrimination, prejudice or other disadvantage to an individual based on person's race, creed, social status, medical history, criminal records or the fact that a person has incurred damages through an offense, etc.

[125] Article 2(4) of APPI

(4) The term “personal information database etc.” used in this Act means a set of information which includes personal information as set forth below (this excludes sets of information specified by Cabinet Order to have little possibility of harming the rights and interests of an individual considering the manner such personal information is used).

และการดำเนินการที่จะอยู่ภายใต้กฎหมายคุ้มครองส่วนบุคคลนี้ ได้แก่ การประมวลผลข้อมูลส่วนบุคคลใดๆ ที่รวมถึงการเก็บ รวบรวม ใช้หรือโอนข้อมูลส่วนบุคคลนั้นๆ อย่างไรก็ตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้จะไม่ใช้บังคับกับสื่อมวลชนที่ดำเนินการกับข้อมูลส่วนบุคคลเฉพาะเพื่อกิจการสื่อสารมวลชนต่างๆ เช่น หนังสือพิมพ์ เป็นต้น หรือบุคคลที่ใช้ข้อมูลส่วนบุคคลเพื่องานศิลปกรรมหรืองานวรรณกรรม เพื่อการศึกษา ศาสนา หรือการเมือง

(1) หลักการประมวลผลข้อมูลโดยผู้ควบคุมข้อมูล

ก่อนการดำเนินการใดๆ เพื่อประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลรับทราบ[126] หรือเปิดเผยวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลของตนเองโดยวิธีการสาธารณะโดยไม่จำต้องแจ้งให้หน่วยงานของรัฐหรือหน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลทราบแต่อย่างใด ทั้งนี้ การเปลี่ยนแปลงวัตถุประสงค์ในการประมวลข้อมูลส่วนบุคคลให้เกินขอบเขตไปกว่าที่บุคคลทั่วไปจะสามารถเข้าใจนั้นย่อมไม่สามารถกระทำได้ตาม APPI[127] อย่างไรก็ตาม เมื่อพิจารณาแนวทางการตีความบทบัญญัติดังกล่าวของกระทรวงเศรษฐกิจ การค้าและอุตสาหกรรมของประเทศญี่ปุ่น[128] จะพบว่าวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลสามารถเปลี่ยนแปลงได้แต่ต้องอยู่ภายในขอบเขตที่ไม่ยากเกินกว่าบุคคลธรรมดาจะเข้าใจได้ ซึ่งวัตถุประสงค์ที่เปลี่ยนแปลงไปนี้ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบหรือจะประกาศการเปลี่ยนแปลงดังกล่าวสู่สาธารณะ

---

[126] Article 18(1) of APPI

(1) Unless the Purpose of Use has already been disclosed to the public, a business operator handling personal information must promptly notify the person of that Purpose of Use or disclose this to the public once it has acquired personal information.

[127] Article 15(2) of APPI

(2) A business operator handling personal information must not change the Purpose of Usebeyond a scope that makes it reasonable to consider the Purpose of Use after the change to be related to what it was before the change.

[128] Ministry of Economy, Trade and Industry, “Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information,” สืบค้นเมื่อวันที่ 6 มีนาคม 2560, จาก http://www.meti.go.jp/policy/it_policy/privacy/0708english.pdf

ก็ได้เช่นกัน การเปลี่ยนแปลงวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่นอกเหนือไปจากขอบเขตที่มีการตกลงกันไว้จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเสมอ[129]

ดังนั้น จะเห็นได้ว่าหน้าที่ประการหนึ่งที่สำคัญของผู้ควบคุมข้อมูล คือ การแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ นอกจากหน้าที่ดังกล่าวนี้ ผู้ควบคุมข้อมูลยังมีหน้าที่อื่นๆ ได้แก่ หน้าที่เก็บรักษาข้อมูลส่วนบุคคลให้ปลอดภัย (มาตรา 20[130]) หน้าที่เปิดเผยข้อมูลให้แก่บุคคลที่สามเฉพาะเมื่อเจ้าของข้อมูลได้ให้ความยินยอม การเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่สามทราบ จะกระทำได้เฉพาะในกรณีที่กำหนดไว้เท่านั้น (มาตรา 23(1)[131]) หรือหน้าที่ปฏิบัติตามคำร้องขอของเจ้าของข้อมูลที่เกี่ยวเนื่องกับข้อมูลส่วนบุคคล

---

[129] Article 18(3) of APPI

(3) If a business operator handling personal information changes the Purpose of Use, it must notify the person of the altered Purpose of Use or disclose this to the public.

[130] Article 20 of APPI

A business operator handling personal information must take the necessary and appropriate measures to ensure the secure management of personal information, such measures to prevent leakage, loss or damage to the personal data it handles.

[131] Article 23(1) of APPI

(1) A business operator handling personal information must not provide a third party withpersonal data without in advance obtaining the person's consent to do so, except in thefollowing cases:

(i) the business operator provides the third party with personal data based on laws and regulations;

(ii) It is necessary for the business operator to provide the third party with the personal data in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person.

(iii) there is a special need for the business operator to provide the third party with the personal data in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

ของตน เนื่องจาก APPI ให้สิทธิเจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลแจ้งวัตถุประสงค์ในการใช้ข้อมูลของตน แก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลให้ถูกต้องทันสมัย ลบข้อมูลส่วนบุคคลของตน หากผู้ควบคุมข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลอย่างไม่เหมาะสม เป็นต้น

นอกจากนี้ในการประมวลผลข้อมูลส่วนบุคคลภายใต้ APPI นั้น ผู้ควบคุมข้อมูลยังมีหน้าที่ต้องจัดหามาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมด้วยเพื่อป้องกันการรั่วไหล สูญหายหรือความเสียหายของข้อมูลส่วนบุคคล ไม่ว่าจะเป็นมาตรการการรักษาความปลอดภัยในด้านของระบบ คน หรือเทคโนโลยี เป็นต้น

(2) หลักการเกี่ยวกับการเปิดเผยข้อมูลต่อบุคคลที่สาม

ภายใต้ APPI นั้น ผู้ควบคุมข้อมูลไม่สามารถเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สามซึ่งอาจเป็นบุคคลธรรมดาหรือนิติบุคคลที่อยู่ภายในประเทศหรือภายนอกประเทศญี่ปุ่นโดยปราศจากความยินยอมล่วงหน้าจากเจ้าของข้อมูลได้ ทั้งนี้ บุคคลที่สาม หมายความรวมถึงบริษัทในเครือของผู้ควบคุมข้อมูลด้วยเช่นกัน

อนึ่ง ผู้ควบคุมข้อมูลอาจเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลโดยปราศจากความยินยอมจากเจ้าของข้อมูลได้หากปรากฏข้อเท็จจริงดังต่อไปนี้[132]

1. **การเปิดเผยข้อมูลส่วนบุคคลดังกล่าวมีกฎหมายของประเทศญี่ปุ่นกำหนดให้สามารถดำเนินการได้** ตัวอย่างเช่น ผู้ค้าปลีกส่งผ่านข้อมูลส่วนบุคคลของผู้บริโภคให้แก่ผู้ผลิตเพื่อที่จะเยียวยาจากการเรียกคืนสินค้าตามกฎหมายว่าด้วยความปลอดภัยของสินค้าบริโภคของญี่ปุ่นที่เรียกว่า “Consumer Product Safety Law (Act No.31 of 1973) หรือ กรณีธนาคารรายงานข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการดำเนินธุรกรรมที่เข้าข่ายต้องสงสัยไปยังหน่วยงานทางการ

(iv) it is necessary for the business operator to provide the third party with the personal data in order to cooperate with a national government organ, local government, or an individual or a business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

[132] Eric Kosinski and Shino Asayama, “Transfer of Personal Data Under Japan's Amended Personal Information Protection Act,” สืบค้นเมื่อวันที่ 6 มีนาคม 2560, จาก https://www.whitecase.com/publications/article/transfer-personal-data-under-japans-amended-personal-information-protection-act

ของประเทศญี่ปุ่นที่ดูแลรับผิดชอบตามกฎหมายเกี่ยวกับการป้องกันอาชญากรรม เป็นต้น กรณีเช่นว่านี้ เมื่อมีกฎหมายกำหนดให้ผู้ควบคุมข้อมูลจำเป็นต้องดำเนินการตามกฎหมาย การเปิดเผยข้อมูลส่วนบุคคลเพื่อเป็นการปฏิบัติตามกฎหมายดังกล่าว ย่อมสามารถดำเนินการได้

2. **กรณีมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลเพื่อปกป้องชีวิต ร่างกาย ทรัพย์สินของบุคคลและกรณีเป็นการยากที่จะได้รับความยินยอมล่วงหน้าจากเจ้าของข้อมูลส่วนบุคคล** ตัวอย่างเช่น เมื่อมีการเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับบุคคลในครอบครัวแก่แพทย์เพื่อให้แพทย์ทำการรักษาโดยฉุกเฉิน เป็นต้น
3. **กรณีมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลเพื่อสุขอนามัยสาธารณะหรือเพื่อส่งเสริมการเจริญเติบโตของเด็กและกรณีเป็นการยากที่จะได้รับความยินยอมล่วงหน้าจากเจ้าของข้อมูลส่วนบุคคล** ตัวอย่างเช่น กรณีที่โรงเรียนแลกเปลี่ยนข้อมูลส่วนบุคคลของเด็กที่กระทำความผิดต่อศูนย์ดูแลควบคุมเด็กเพื่อประโยชน์ต่อการดูแลตัวเด็กนั้นๆ เป็นต้น
4. **กรณีที่รัฐบาลของประเทศญี่ปุ่นขอความร่วมมือให้เปิดเผยข้อมูลส่วนบุคคลและการได้รับความยินยอมจากเจ้าข้อมูลส่วนบุคคลจะเป็นการชักช้าไม่ทันการกับที่รัฐบาลจำเป็นต้องดำเนินการ** ตัวอย่างเช่น กรณีที่ผู้ควบคุมข้อมูลสมัครใจแบ่งปันข้อมูลส่วนบุคคลของลูกจ้างต่อกรมสรรพากรของประเทศญี่ปุ่นเพื่อประโยชน์ในการคำนวณภาษีเงินได้บุคคลธรรมดาของลูกจ้างและเพื่อประโยชน์ในการจัดเก็บภาษีของรัฐบาล เป็นต้น
5. **กรณีที่ผู้ควบคุมข้อมูลได้รับความยินยอมประเภท opt-out จากเจ้าของข้อมูลส่วนบุคคล** ความยินยอมประเภท opt-out เป็นความยินยอมในลักษณะที่เปิดโอกาสให้ผู้ควบคุมข้อมูลสามารถส่งผ่านข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ก่อนครั้งหนึ่ง ซึ่งหากเจ้าของข้อมูลส่วนบุคคลไม่ประสงค์จะให้มีการส่งผ่านข้อมูลดังกล่าวก็สามารถแจ้งหรือร้องขอให้มีการยกเลิกได้ ภายใต้ APPI นั้น กรณีที่จะถือว่าเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมประเภท opt-out ต่อผู้ควบคุมข้อมูลนั้น ผู้ควบคุมข้อมูลจะต้องลงทะเบียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น หรือ Japanese government's Personal Information Protection Committee (PIPC) เพื่อขอให้ตนมีสิทธิได้รับความยินยอมประเภทดังกล่าวจากเจ้าของข้อมูลก่อน ซึ่งภายหลังการลงทะเบียนดังกล่าว ผู้ควบคุมข้อมูลสามารถได้รับความยินยอมประเภท opt-out จากการประกาศบนหน้าเว็บไซต์หรือจดหมายอิเล็กทรอนิกส์ซึ่งระบุว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลอาจถูกส่งผ่านให้แก่บุคคลอื่นได้โดยต้องกำหนดประเภทของข้อมูล วิธีการและถ้อยคำสัญญาของผู้ควบคุมข้อมูลในการหยุดการเปิดเผยข้อมูลส่วนบุคคลเมื่อเจ้าของ

ข้อมูลร้องขอ รวมทั้งจะต้องระบุวิธีการที่เจ้าของข้อมูลสามารถติดต่อผู้ควบคุมข้อมูลด้วย[133] อย่างไรก็ตาม ความยินยอมประเภทนี้ไม่มีผลใช้บังคับกับข้อมูลที่อ่อนไหว เช่น เชื้อชาติ สัญชาติ หรือข้อมูลทางอาชญากรรม เป็นต้น ทั้งนี้ หน้าที่ของผู้ควบคุมข้อมูลในการลงทะเบียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นบทบัญญัติใหม่ที่กำหนดเพิ่มเติมขึ้นมา

6. **การเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่ได้รับความไว้วางใจ (A trustee)** ผู้ควบคุมข้อมูลอาจเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่ได้รับความไว้วางใจโดยปราศจากความยินยอมจากเจ้าของข้อมูลได้ เนื่องจากบุคคลที่ได้รับความไว้วางใจนั้นไม่ถือเป็นบุคคลที่สามภายใต้ APPI ทั้งนี้ บุคคลที่ได้รับความไว้วางใจดังกล่าว หมายถึง หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับการให้บริการของผู้ควบคุมข้อมูล ซึ่งหน่วยงานดังกล่าวจะต้องใช้ข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์ที่ผู้ควบคุมข้อมูลกำหนดอย่างเคร่งครัดโดยการใช้ข้อมูลดังกล่าวจะต้องเป็นไปเพื่อ

---

[133] Article 23(2) of APPI

(2) Notwithstanding the provisions of the preceding paragraph, if a business operator handling personal information agrees, at the request of a person, to stop providing a third party with any personal data it provides to third parties which can be used to identify the person, but then as prescribed by rules of the Personal Information Protection Commission, notifies the person of the following information in advance or makes that information readily accessible to the person in advance, and notifies the Personal Information Protection Commission in advance, the business operator may provide that personal data to a third party:

(i) the fact that providing the data to a third party constitutes the Purpose of Use;

(ii) the items of the personal data it will provide to the third party;

(iii) the means in which it will provide the data to a third party;

(iv) the fact that it will stop providing personal data that can be used to identify the person to a third party at the request of the person;

(v) the means to receive the request of the person.

วัตถุประสงค์ในการติดต่อสื่อสารกับเจ้าของข้อมูล[134] ตัวอย่างเช่น บริษัทที่ทำหน้าที่เก็บรวบรวมจดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ หรือ บริษัทที่รับขนส่งสินค้า เป็นต้น

7. **การเปิดเผยข้อมูลส่วนบุคคลอันเนื่องมาจากการควบรวมกิจการ** ผู้ควบคุมข้อมูลสามารถเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สามอันเนื่องจากกมาการรับช่วงต่อทางธุรกิจได้ เช่น การควบรวมกิจการ การโอนกิจการหรือการแยกกิจการ เป็นต้น (มาตรา 23(5)) ทั้งนี้ ข้อยกเว้นในการเปิดเผยข้อมูลกรณีนี้ใช้กับกรณีที่มีการเจรจาทางธุรกิจเป็นผลสำเร็จแล้วเท่านั้น การเปิดเผยข้อมูลส่วนบุคคลไม่สามารถดำเนินการได้ในขั้นตอนของการเจรจาต่อรองทางธุรกิจหรือขั้นตอนของการตรวจสอบวิเคราะห์สถานะของกิจการ (Due Diligence) ได้ อย่างไรก็ตาม หากบริษัทผู้ซื้อมีความประสงค์จะให้บริษัทผู้ขายเปิดเผยข้อมูลส่วนบุคคลในระหว่างขั้นตอนของการเจรจา บริษัทผู้ซื้อและผู้ขายย่อมมีหน้าที่ต้องเข้าผูกผันกันตามสัญญาเพื่อที่จะทำให้แน่ใจว่าบริษัทผู้ซื้อจะปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้ โดยที่สัญญาดังกล่าวจะต้องกำหนดเกี่ยวกับการใช้ข้อมูลส่วนบุคคลตลอดจนการจัดการข้อมูลส่วนบุคคลของบริษัทผู้ซื้ออย่างเคร่งครัด

---

[134] Article 23(5) of APPI

(5) In the following cases, the individual or business operator being provided with the personal data must not be deemed to be a third party as regards the application of the provisions of each preceding paragraph:

(i) if the business operator handling personal information entrusts with all or part of the handling of personal data within the scope necessary for achieving the Purpose of Use;

(ii) if the personal data is provided when a business operator succeeds to the business of the business operator due to a merger or other such circumstances;

(iii) if personal data which is used jointly with a specific individual or business operator is provided to the individual or business operator, and the individual or business operator notify the person of this in advance as well as notify the person of the items of the personal data of which the specific individual or business operator have joint use, the extent of the joint users, the user's purposes of use, and the name of the individual or business operator responsible for managing the personal data, or the individual or business operator make the foregoing information readily accessible to the person in advance.

รวมทั้งกำหนดแนวทางการดำเนินการและแนวทางการเยียวยาหากข้อมูลดังกล่าวรั่วไหลด้วย เป็นต้น

8. **การเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่มีลักษณะเป็นผู้ใช้บริการร่วม (Joint user)** การเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่สามที่ได้รับอนุญาตนั้น ผู้ควบคุมข้อมูลอาจกำหนดข้อมูลที่สามารถเปิดเผยให้แก่ผู้ใช้บริการร่วมกับเจ้าของข้อมูลได้ (มาตรา 25(3)) ตัวอย่างเช่น ชนิดของข้อมูลส่วนบุคคลที่สามารถใช้ร่วมกัน ขอบเขตของผู้ใช้บริการร่วม วัตถุประสงค์ของการใช้บริการข้อมูลส่วนบุคคลร่วมกัน และข้อมูลการติดต่อสำหรับบุคคลที่รับผิดชอบในการบริหารจัดการการใช้ข้อมูลส่วนบุคคลร่วมกันของผู้ใช้บริการร่วม เป็นต้น ข้อยกเว้นสำหรับการเปิดเผยข้อมูลส่วนบุคคลระหว่างผู้ใช้บริการร่วมนี้ถูกกำหนดขึ้นมาเพื่อรองรับการเปิดเผยข้อมูลส่วนบุคคลระหว่างกลุ่มบริษัทที่มีบริษัทแม่เป็นบริษัทเดียวกันนั่นเอง

ในกรณีที่ผู้ควบคุมข้อมูลมีสิทธิที่จะเปิดเผยข้อมูลส่วนบุคคลและได้เปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่สามแล้ว ผู้ควบคุมข้อมูลในฐานะผู้โอนหรือเปิดเผยข้อมูลจะต้องจัดทำเอกสารบันทึกการโอนโดยระบุรายละเอียด คือ (1) วันที่มีการโอน (2) ชื่อสกุลของผู้รับโอนข้อมูล และ (3) ข้อมูลอื่นๆ ของผู้รับโอนข้อมูลเพื่อประกอบการพิจารณาของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 25 (1)[135]) และผู้ควบคุมข้อมูลในฐานะผู้โอนจะต้องเก็บรักษา

---

[135] Article 25(1) of APPI

(1) A business operator handling personal information must, when providing personal data to a third party (this excludes business operators provided for in each item of Article 2, paragraph (5); the same applies hereinafter in this Article and the next Article), make a record of the matters as prescribed by rules of the Personal Information Protection Commission, regarding the date such personal data was provided, the name of the third party, as well as other matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision falling under any of the items of Article 23, paragraph (1) or paragraph (5) (any of the items of Article 23, paragraph (1) for the provision of personal data under the preceding Article).

เอกสารบันทึกดังกล่าวเป็นระยะเวลาที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 25(2)[136])

ในทางกลับกันหากผู้ควบคุมข้อมูลเป็นผู้ที่ได้รับข้อมูลส่วนบุคคลมาจากบุคคลที่สาม ผู้ควบคุมข้อมูลในฐานะผู้รับโอนจะต้องตรวจสอบหรือสืบสวนให้แน่ใจในรายละเอียดดังนี้ (1) ชื่อสกุลของผู้โอนหรือชื่อหน่วยงานของผู้โอน (2) ที่อยู่ของผู้โอน (3) ผู้โอนข้อมูลครอบครองข้อมูลส่วนบุคคลดังกล่าวได้อย่างไร (มาตรา 26(1)[137]) นอกจากนี้ผู้ควบคุมข้อมูลในฐานะผู้รับโอนจะต้องจัดทำเอกสารบันทึกวันที่ตนได้รับโอนข้อมูล ข้อเท็จจริงที่ได้ตรวจสอบข้างต้นตลอดจนข้อมูล

---

[136] Article 25(2) of APPI

(2) A business operator handling personal information must store records set forth in the preceding paragraph, from the day when the said records are created for a period of time prescribed by rules of the Personal Information Protection Commission.

[137] Article 26(1) of APPI

(1) A business operator handling personal information must, upon being provided personal data from a third party, confirm the following matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision fall under any of the items of Article 23, paragraph (1) or paragraph(5).

(i) The name and address of the third party, and the name of the representative (the representative or the manager for an association or foundation that are not juridical person) for juridical person;

(ii) The details of the acquisition of the personal data by the third party.

อื่นๆ ที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 26(3)[138]) ตามระยะเวลาที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 26(4)[139])

(3) หลักการเกี่ยวกับการโอนข้อมูลส่วนบุคคลจากประเทศญี่ปุ่นไปยังต่างประเทศ

แต่เดิม APPI ไม่ได้บัญญัติข้อกำหนดโดยเคร่งครัดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศแต่อย่างใด ซึ่งแตกต่างจากกฎเกณฑ์ของกลุ่มสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม ภายหลังการปรับปรุงแก้ไขดังกล่าว กฎหมายที่แก้ไขเพิ่มเติม APPI ได้เพิ่มบทบัญญัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ กล่าวคือ ถ้าผู้ควบคุมข้อมูลซึ่งดำเนินการอยู่ภายในประเทศญี่ปุ่นต้องการโอนข้อมูลส่วนบุคคลให้แก่หน่วยงานอื่นนอกประเทศญี่ปุ่น (แม้ว่าหน่วยงานดังกล่าวจะเป็นบริษัทในเครือเดียวกันก็ตาม) ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน เว้นเสียแต่ว่า จะเป็นกรณีตามที่กำหนดไว้ในมาตราก่อนว่าด้วยการเปิดเผยข้อมูลข้างต้น กรณีเช่นว่านี้ผู้ควบคุมข้อมูลสามารถเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนได้ (มาตรา 24[140])

---

[138] Article 26(3) of APPI

(3) When the business operator handling personal information carries out the confirmation under the paragraph (1), the business operator must, prescribed by rules of the Personal Information Protection Commission, make records of the date on which such personal data was provided, matters related to the confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

[139] Article 26(4) of APPI

(4) A business operator handling personal information must store such records beginning with the day on which the said records are created and for a period of time prescribes by rules of the Personal Information Protection Commission.

[140] Article 24 of APPI

A business operator handling personal information must, when providing personal data to a third party (this excludes individuals or business operators that put into place a system compliant with the standards prescribed by rules of the Personal Information Protection Commission as is necessary to continuously take of measures corresponding with measures that business operators

ทั้งนี้ กรณีการโอนข้อมูลส่วนบุคคลไปยังภายนอกประเทศ APPI ไม่ได้กำหนดให้ต้องจัดทำเอกสารหลักฐานหรือบันทึกการโอนข้อมูลแต่อย่างใด

4.3.2 สหพันธ์สาธารณรัฐเยอรมนี

ดังที่ได้กล่าวไว้แล้วในบทก่อนๆ ว่าประเทศเยอรมนีเป็นประเทศที่ได้รับการจัดอันดับให้เป็นประเทศที่มีความพร้อมในการบริการระบบการประมวลผลแบบคลาวด์ ซึ่งความพร้อมดังกล่าวได้รวมถึงการมีกฎหมายคุ้มครองข้อมูลบุคคลที่ทันสมัยและบังคับใช้ได้จริง ดังนี้

4.3.2.1 ความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี

กฎหมายรัฐธรรมนูญของสหพันธ์สาธารณรัฐเยอรมนี (Grundgesetz หรือ The Basic Law) ได้ให้ความคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลโดยถือเป็นสิทธิขั้นพื้นฐานประการหนึ่งภายใต้รัฐธรรมนูญฉบับดังกล่าว ดังนั้น สหพันธ์สาธารณรัฐเยอรมนีจึงมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เคร่งครัด ทั้งนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของสหพันธ์สาธารณรัฐเยอรมนีเกิดขึ้นในรัฐเฮสเซิน (Hessen)[141] ในปี ค.ศ. 1970 ซึ่งถือเป็นกฎหมายในระดับมลรัฐ และต่อมาในปีค.ศ. 1977 สหพันธ์สาธารณรัฐเยอรมนีจึงได้ตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับประเทศขึ้นโดยใช้ชื่อเรียกว่า ‘Bundesdatenschutzgesetz’ หรือ ‘BDSG’ ซึ่งในระยะเวลาต่อมาก็ได้รับการแก้ไขหลายครั้ง โดยการแก้ไขครั้งสำคัญเกิดขึ้นในปี ค.ศ. 2001 เพื่อให้

---

handling personal information ought to carry out pursuant to the provisions of this Section with regard to handling of personal data; the same applies in this Article hereinafter.) in a foreign country (any country or territory outside of the region of Japan; the same applies hereinafter) (excluding countries prescribed by rules of the Personal Information Protection Commission to be foreign countries possessing personal information protection systems recognized to be at the same level as Japan's in terms of protecting the rights and interests of individuals; the same applies hereinafter in this Article), obtain the prior consent of the person for the provision of such personal data to a third party in a foreign country, except in cases set forth in each item of paragraph (1) of the preceding Article. The provisions of that the preceding Article do not apply in this case.

[141] นคร เสรีรักษ์, *อ้างแล้ว เชิงอรรถที่ 21*, น.143.

สอดคล้องกับกฎหมายของสหภาพยุโรปในเรื่องการคุ้มครองข้อมูลส่วนบุคคล โดยมีสาระสำคัญเพื่อคุ้มครองข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม การประมวลผลและการใช้ข้อมูลส่วนบุคคลโดยหน่วยงานรัฐรวมทั้งการดำเนินการโดยเอกชนที่ใช้ระบบประมวลผลเพื่อการค้าและธุรกิจ และเพิ่มบทบัญญัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ การสอดส่องผ่านกล้องวิดีโอ การปกปิดชื่อและการใช้นามแฝง การใช้บัตรสมาร์ทการ์ด การเก็บรวบรวมข้อมูลที่มีลักษณะต้องห้ามหรือมีความอ่อนไหว เช่น สีผิว เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา การเข้าร่วมเป็นสมาชิกกลุ่ม ข้อมูลด้านสุขภาพ เป็นต้น ทั้งนี้ การแก้ไขนี้เป็นการให้สิทธิแก่เจ้าของข้อมูลในการปฏิเสธการอนุญาตให้เก็บข้อมูลนั้นได้และยังกำหนดให้บริษัทเอกชนที่เก็บรวบรวม ประมวลผลและใช้ข้อมูลส่วนบุคคลจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนเองด้วยต่างหากจากเจ้าหน้าที่ของรัฐ มิเช่นนั้นการประมวลผลข้อมูลทุกครั้งจะต้องจดทะเบียนต่อคณะกรรมการคุ้มครองข้อมูลของรัฐ (The Federal Commissioner for Data Protection and Freedom of Information หรือ Bundesbeauftragter fur den Datenschutz und die Informationsfreiheit) เป็นต้น ต่อมาในปี ค.ศ. 2005 ได้มีการแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลข้างต้นอีกครั้งโดยมีสาเหตุอันเนื่องมาจากคำแนะนำของผู้เชี่ยวชาญที่มีการจัดทำขึ้นตั้งแต่ปี ค.ศ. 2001 เพื่อใช้เป็นกฎหมายกลางของประเทศ

ต่อมาเมื่อวันที่ 27 เมษายน 2017 ที่ผ่านมา รัฐสภาแห่งสหพันธ์สาธารณรัฐเยอรมนีได้ลงมติรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ที่จะนำมาใช้แทนที่ฉบับเดิมควบคู่ไปกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR และกฎหมายอีกฉบับหนึ่งของสหภาพยุโรปได้แก่ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection (“Law Enforcement Directive”) ทั้งนี้ BDSG จะมีผลใช้บังคับพร้อมกับ GDPR ในวันที่ 25 พฤษภาคม 2018 ด้วย ซึ่งนับว่าสหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศแรกที่ได้รับเอา GDPR มาใช้บังคับเป็นกฎหมายภายในของประเทศ[142] นอกจากนี้

---

[142] Lennart Schüßler and Natallia Karniyevich, “Germany is the first EU Member State to enact new Data Protection Act to align with the GDPR,” สืบค้นเมื่อวันที่ 20 กรกฎาคม 2560, จาก https://www.twobirds.com/en/news/articles/2017/germany /germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr

เนื่องจาก GDPR เปิดโอกาสให้ประเทศสมาชิกสามารถออกกฎหมายภายในเพื่อบังคับใช้ภายในประเทศตนได้โดยอิสระแต่ต้องไม่ขัดกับ GDPR กว่า 70 เรื่อง ซึ่งเรียกว่า “Opening Clause” เช่น ความชอบด้วยกฎหมายของการประมวลผลข้อมูล การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer: DPO) หรือการประมวลผลข้อมูลในกรณีพิเศษ เช่น การประมวลผลข้อมูลของลูกจ้างที่มีวัตถุประสงค์เกี่ยวกับงานสื่อมวลชน เป็นต้น ดังนั้น ผู้ยกร่างกฎหมายของสหพันธ์สาธารณรัฐเยอรมนีจึงอาศัยบทบัญญัติที่เปิดช่องดังกล่าวในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนีให้มีความทันสมัยและสอดคล้องกับ GDPR มากยิ่งขึ้น ดังจะได้ศึกษาต่อไปนี้

4.3.2.2 สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี คือ ‘Bundesdatenschutzgesetz’ หรือ ‘BDSG’ ซึ่งมีชื่อภาษาอังกฤษว่า The Federal Data Protection Act แบ่งออกเป็น 4 ส่วน[143] ได้แก่

ส่วนที่ 1 ว่าด้วยหลักการทั่วไป (มาตรา 1 - มาตรา 21) บทบัญญัติที่บัญญัติไว้ในส่วนที่ 1 จะเป็นบทบัญญัติที่เกี่ยวกับหลักการทั่วไปซึ่งจะบังคับใช้กับบทบัญญัติที่เป็นการรับหลักการของ GDPR และ Law Enforcement Directive ได้แก่ ขอบเขตการใช้บังคับ บทนิยาม โครงสร้างและอำนาจหน้าที่ของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลกลางของเยอรมนี (Germany’s Federal Data Protection Authority) และการบังคับใช้ของ BDSG กับ มลรัฐทั้ง 16 มลรัฐ เป็นต้น

ทั้งนี้ BDSG จะบังคับใช้เฉพาะกับข้อมูลที่มีลักษณะเป็นข้อมูลส่วนบุคคลเท่านั้น ข้อมูลอื่นๆ เช่น ข้อมูลทั่วๆ ไป หรือ Big Data ข้อมูลความลับทางการค้า จะไม่อยู่ภายใต้บังคับของ BDSG แต่อาจอยู่ภายใต้บังคับของกฎหมายฉบับอื่น ซึ่งไม่อยู่ภายในขอบเขตของการศึกษาในครั้งนี้ เช่น กรณีของข้อมูลความลับทางการค้ามี The Act Against Unfair Competition ให้ความคุ้มครองโดยเฉพาะ เป็นต้น

---

[143] Alston & Bird, “An English-Language Primer on Germany’s GDPR Implementation Statute: Part 1 of 5,” สืบค้นเมื่อวันที่ 30 กันยายน 2560, จาก https://www.jdsupra.com/legalnews/an-english-language-primer-on-germany-s-59204/

ส่วนที่ 2 ว่าด้วยบทบัญญัติเกี่ยวกับการประมวลผลตาม GDPR (มาตรา 22 - มาตรา 44) ประกอบด้วยบทบัญญัติหลักการประมวลผลข้อมูลส่วนบุคคล การใช้ข้อมูลส่วนบุคคลซ้ำ (Secondary uses or data re-uses) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) สิทธิเจ้าของข้อมูล (Individual right) การประมวลโดยมีวัตถุประสงค์เกี่ยวกับวิทยาศาสตร์และการค้นคว้าวิจัย และบทกำหนดโทษ เป็นต้น ส่วนที่ 2 จะเป็นส่วนที่กระทบกับภาคเอกชนโดยเฉพาะ

ส่วนที่ 3 ว่าด้วยบทบัญญัติเกี่ยวกับการประมวลผลตาม Law Enforcement Directive (มาตรา 45 - มาตรา 84) ประกอบด้วยบทบัญญัติตามหลักการของ Law Enforcement Directive ที่จะใช้บังคับกับหน่วยงานของรัฐ (public authorities) ซึ่งประมวลผลข้อมูลโดยมีวัตถุประสงค์เพื่อป้องกัน สืบสวนสอบสวน ดำเนินคดีที่เกี่ยวกับการกระทำความผิดทางอาญา อาทิ หลักการพื้นฐานของการประมวลผล (มาตรา 47) สิทธิของเจ้าของข้อมูล (มาตรา 56-59) การใช้ข้อมูลซ้ำ (มาตรา 48-50) ผู้ประมวลผลหรือผู้ให้บริการ (มาตรา 62) ความปลอดภัยของข้อมูล (มาตรา 64) เป็นต้น ส่วนที่ 3 ผู้ที่จะได้รับผลกระทบ คือ บริษัทหรือภาคเอกชนที่เป็นคู่สัญญาของรัฐโดยเฉพาะ ดังนั้นบริษัทเอกชนโดยทั่วไปจึงไม่กระทบกับบทบัญญัติในส่วนที่ 3 มากนัก

ส่วนที่ 4 ว่าด้วยการประมวลผลที่ไม่ตกอยู่ภายใต้ขอบเขตของ GDPR และ Law Enforcement Directive (มาตรา 85) ประกอบด้วยบทบัญญัติเพียงมาตราเดียวที่จะกำหนดการประมวลผลข้อมูลส่วนบุคคลที่ไม่อยู่ในขอบเขตของทั้ง GDPR และ Law Enforcement Directive อาทิ การโอนข้อมูลเพื่อวัตถุประสงค์ของรัฐ ดังนั้น บริษัทซึ่งเป็นภาคเอกชนทั่วไปจึงไม่ได้รับผลกระทบจากบทบัญญัติในส่วนนี้

ทั้งนี้ เมื่อพิจารณาขอบเขตการใช้บังคับของ BDSG จะพบว่าโดยหลักหากกรณีใด GDPR สามารถใช้บังคับกับกรณีดังกล่าวได้ กฎหมายที่จะมีผลใช้บังคับ คือ GDPR แต่สำหรับกรณีใดที่ GDPR ไม่ได้กำหนดหลักการหรือไม่ได้กำหนดขอบเขตในการใช้บังคับไว้ BDSG จะมีผลใช้บังคับแทนสำหรับกรณีดังกล่าว ซึ่งเมื่อพิจารณาขอบเขตของ GDPR จะพบว่า GDPR กำหนดขอบเขตการใช้บังคับให้มีผลกับทั้งบริษัทที่จัดตั้งอยู่ในสหภาพยุโรปและบริษัทที่จัดตั้งนอกสหภาพยุโรปแต่เสนอขายสินค้าหรือบริการให้แก่ผู้ที่มีถิ่นที่อยู่ในสหภาพยุโรป (EU Residents) หรือควบคุมพฤติกรรมของผู้มีถิ่นที่อยู่ในสหภาพยุโรป BDSG จึงกำหนดขอบเขตการใช้บังคับไปในแนวทาง

เดียวกับ GDPR ตามที่ปรากฏในมาตรา 1(4) [144] ของ BDSG คือ บริษัทไม่ว่าอยู่ในสถานะของผู้ควบคุมข้อมูลหรือผู้ประมวลผลจะตกอยู่ภายใต้บังคับของ GDPR เมื่อ

- ประมวลผลข้อมูลส่วนบุคคลในสหพันธ์สาธารณรัฐเยอรมนี หรือ
- ประมวลผลข้อมูลส่วนบุคคลในบริบทของสถานประกอบการที่ตั้งอยู่ในสหพันธ์สาธารณรัฐเยอรมนี หรือ
- ไม่มีสถานประกอบการในสหภาพยุโรป แต่ตกอยู่ภายใต้บังคับตามขอบเขตที่ GDPR กำหนดไว้ คือ เสนอขายสินค้าหรือบริการให้แก่ผู้ที่มีถิ่นที่อยู่ในสหภาพยุโรป (EU Residents) หรือควบคุมพฤติกรรมของผู้มีถิ่นที่อยู่ในสหภาพยุโรป

อย่างไรก็ตาม GDPR ได้เปิดโอกาสให้ประเทศสมาชิกสามารถออกกฎหมายเพื่อใช้บังคับสำหรับเรื่องนั้นๆ โดยเฉพาะได้ (ที่เรียกว่า “Opening Clauses”) ดังนั้น BDSG จึงขยายขอบเขตการบังคับใช้ให้กว้างขึ้น โดยกำหนดว่า หากบริษัทซึ่งไม่ใช่บริษัทในสหภาพยุโรปตกอยู่ภายใต้บังคับของ GDPR แล้ว บริษัทดังกล่าวย่อมตกอยู่ภายใต้บังคับของ BDSG ยกตัวอย่างเช่น บริษัทที่ตั้งอยู่ในมลรัฐฟอลิด้า ประเทศสหรัฐอเมริกา ทำการตลาดให้แก่บริษัทในประเทศสเปน ซึ่งจะทำให้บริษัทในฟอลิด้าตกอยู่ภายใต้บังคับของ GDPR ดังนั้น บริษัทในฟอลิด้าจึงตกอยู่ภายใต้บังคับของ BDSG ด้วย แม้ว่าบริษัทนั้นจะไม่มีจุดเกาะเกี่ยวกับสหพันธ์สาธารณรัฐ

---

[144] Section 1(4) of BDSG

This act shall apply to public bodies. It shall apply to private bodies if

1. the controller or processor processes personal data in Germany,

2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany, or if,

3. although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it does fall within the scope of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the pro-cessing of personal data and on the free movement of such data, and repealing Di-rective 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4 May 2016, p. 1; L 314 of 22 November 2016, p. 72).

เยอรมนีเลยก็ตาม นอกเหนือจาก Opening Clauses เรื่องการขยายขอบเขตการใช้บังคับแล้ว BDSG ยังมี Opening Clauses อีกหลายประการ ดังนี้

<u>การประมวลผลข้อมูลประเภทพิเศษ (Special Categories)</u> ซึ่งกำหนดไว้ในมาตรา 22 และมาตรา 24(1) ของ BDSG คือ การประมวลผลข้อมูลประเภทพิเศษ หรือข้อมูลที่มีความอ่อนไหว เช่น การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง สมาชิกสหภาพแรงงาน เพศ สุขภาพ เป็นต้น จะกระทำได้ต่อเมื่อเป็นไปตามที่กำหนดไว้ในมาตรา 22[145] ได้แก่

(1) การประมวลผลที่จำเป็นต้องกระทำเพื่อแสดงออกซึ่งสิทธิในประกันสังคม (Right to social security) ความคุ้มครองทางสังคม (Right to social protection) หรือเพื่อเป็นการปฏิบัติตามหน้าที่ตามกฎหมาย
(2) การประมวลผลจำเป็นต้องกระทำเพื่อการคุ้มครองยา สุขภาพ เป็นต้น
(3) การประมวลผลจำเป็นต้องกระทำเนื่องจากเหตุผลเกี่ยวกับผลประโยชน์สาธารณะในบริบทของสุขภาพแห่งชาติ เช่น การป้องกันโรคติดต่อระหว่างประเทศ หรือการกระทำเพื่อมาตรฐานที่ดีเกี่ยวกับคุณภาพและความปลอดภัยของยาและอุปกรณ์ทางการแพทย์ เป็นต้น

ทั้งนี้ การประมวลผลข้างต้นจะต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมและเฉพาะเจาะจงเพื่อรักษาผลประโยชน์ของเจ้าของข้อมูล อาทิ
- มาตรการที่ทำให้การประมวลผลเป็นไปตามที่ Regulation (EU) 2016/679 กำหนด
- มาตรการที่เพิ่มความระมัดระวังของบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- มาตรการเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- มาตรการเกี่ยวกับการ Encryption ข้อมูลส่วนบุคคล เป็นต้น

---

[145] Section 22 of BDSG

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

นอกจากนี้ การประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากขอบวัตถุประสงค์ที่ข้อมูลส่วนบุคคลได้ถูกจัดเก็บสามารถดำเนินการได้ ภายใต้มาตรา 24(1)[146] ของ BDSG หากการประมวลผลดังกล่าวจำเป็นต้องกระทำเพื่อปกป้องภยันตรายของรัฐ ความปลอดภัยสาธารณะ หรือการดำเนินคดีอาญา หรือจำเป็นต้องกระทำเพื่อก่อตั้ง ดำเนินการ หรือโต้แย้งเกี่ยวกับสิทธิเรียกร้องตามกฎหมาย อย่างไรก็ตาม หากเจ้าของข้อมูลมีผลประโยชน์เหนือกว่าความจำเป็นข้างต้น การประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะสามารถประมวลผลได้

---

[146] Section 24(1) of BDSG

(1) Private bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected if

1. processing is necessary to prevent threats to state or public security or to prosecute criminal offences; or

2. processing is necessary for the establishment, exercise or defence of legal claims, unless the data subject has an overriding interest in not having the data processed.

<u>การประมวลผลข้อมูลส่วนบุคคลในบริบทของการจ้างแรงงาน</u>

(Processing in the context of employment) สืบเนื่องจากมาตรา 88(1)[147] ของ GDPR กำหนดให้ประเทศสมาชิกต้องรับผิดชอบในการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลในบริบทของการจ้างแรงงาน โดยกฎหมายของประเทศสมาชิกจะต้องประกอบไปด้วยมาตรการที่เฉพาะเจาะจงและมีความเหมาะสมในการที่จะคุ้มครองศักดิ์ศรีความเป็นมนุษย์ ผลประโยชน์ตามกฎหมาย และสิทธิขั้นพื้นฐานของลูกจ้าง ทั้งนี้ ตามมาตรา 88(2)[148] ของ GDPR ดังนั้น BDSG จึง

---

[147] Article 88(1) of GDPR

(1) Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

[148] Article 88(2) of GDPR

(2) Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

บัญญัติถึงการประมวลผลข้อมูลส่วนบุคคลของลูกจ้างไว้ในมาตรา 26[149] ซึ่งลูกจ้างในความหมายของ BDSG หมายความถึง ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้ที่ทำงานจากที่บ้าน (Home worker) ผู้ฝึกงาน (Trainee) ตลอดจนข้าราชการพลเรือน ผู้พิพากษาและทหาร ทั้งนี้ การประมวลผลจะสามารถกระทำได้โดยไม่ต้องได้รับความยินยอมเมื่อเป็นไปตามเงื่อนไขที่กำหนดไว้ดังนี้

(1) เป็นการประมวลผลเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการจ้างงานซึ่งจำเป็นต้องกระทำเพื่อประกอบการตัดสินใจจ้างงาน หรือภายหลังการจ้างงาน เพื่อระงับสัญญาจ้างแรงงาน หรือเพื่อแสดงออกซึ่งสิทธิหรือหน้าที่เพื่อให้เป็นไปตามที่กฎหมายรับรองหรือที่ได้ตกลงไว้ในสัญญา
(2) เป็นการประมวลผลเพื่อสืบหาการกระทำความผิดอาญาของลูกจ้าง ซึ่งมีเหตุผลเป็นลายลักษณ์อักษรที่แสดงให้เชื่อได้ว่าเจ้าของข้อมูลได้กระทำความผิดในขณะที่เป็นลูกจ้างและการประมวลผลจำเป็นต้องกระทำเพื่อสืบสวนสอบสวนการกระทำความผิดอาญา ทั้งนี้ จะต้องไม่ส่งผลกระทบกับผลประโยชน์ตามกฎหมายของเจ้าของข้อมูลจนเกินไปและได้สัดส่วน

กรณีเป็นการประมวลผลที่ได้รับความยินยอมจากเจ้าของข้อมูลซึ่งเป็นลูกจ้าง ความยินยอมดังกล่าวจะต้องเป็นความยินยอมที่ลูกจ้างได้ให้ไว้โดยอิสระ โดยอาจพิจารณาจากระดับความเป็นอิสระของลูกจ้างในความสัมพันธ์นั้นและเหตุการณ์ประกอบการให้ความยินยอม เป็นต้น ทั้งนี้ ความยินยอมดังกล่าวจะต้องเป็นความยินยอมที่ได้ให้ไว้เป็นลายลักษณ์อักษร (ยกเว้นจะมีสถานการณ์พิเศษที่การให้ความยินยอมในรูปแบบอื่นมีความเหมาะสมมากกว่า) และนายจ้าง

---

[149] Section 26 of BDSG

(1) Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' repre-sentation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

จะต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของลูกจ้างและสิทธิของลูกจ้างในการถอนความยินยอมให้ลูกจ้างทราบด้วย

นอกจากนี้ การประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ (Special Categories of Personal data) เพื่อวัตถุประสงค์สำหรับการจ้างแรงงานที่จำเป็นต้องกระทำตามสิทธิหรือเพื่อปฏิบัติตามกฎหมายแรงงาน กฎหมายประกันสังคม โดยไม่มีเหตุผลที่จะชวนให้เชื่อได้ว่าการประมวลผลดังกล่าวกระทบต่อผลประโยชน์ตามกฎหมายของลูกจ้าง ย่อมสามารถกระทำได้โดยต้องได้รับความยินยอมโดยระบุชัดว่าเป็นความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษและต้องอยู่ภายใต้เงื่อนไขการได้รับความยินยอมข้างต้นก่อนด้วย อย่างไรก็ตาม มาตรา 26(4) ของ BDSG ได้เปิดช่องให้การประมวลผลข้อมูลส่วนบุคคลได้แก่ การประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษเพื่อวัตถุประสงค์ในการจ้างแรงงาน สามารถกระทำได้โดยอาศัยการตกลงไว้ในข้อตกลงเกี่ยวกับสภาพการจ้างเช่นกัน แต่ทั้งนี้ทั้งนั้น ไม่ว่าจะเป็นการประมวลผลประเภทใดผู้ควบคุมข้อมูลจะต้องหามาตรการที่เหมาะสมในการตรวจทานให้แน่ใจว่าตนได้ปฏิบัติตามที่กฎหมายกำหนดอย่างครบถ้วน

<u>การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของการศึกษาวิจัยในทางวิทยาศาสตร์หรือประวัติศาสตร์และเพื่อวัตถุประสงค์ในทางสถิติ</u> (Data processing for purposes of scientific or historical research and for statistical purposes) สืบเนื่องจาก GDPR มีความเห็นว่าการศึกษาวิจัยในทางวิทยาศาสตร์หรือประวัติศาสตร์และสถิติมีความสำคัญเป็นอย่างมาก ดังนั้น มาตรา 89(2) ของ GDPR[150] จึงกำหนดข้อยกเว้นเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทนี้ไว้เป็นพิเศษ ด้วยเหตุนี้ BDSG จึงบัญญัติข้อยกเว้นเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทนี้ไว้ในมาตรา 27 และมาตรา 28 ของ BDSG โดยให้ผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษได้แม้จะไม่ได้รับความยินยอมจากเจ้าของข้อมูล หากเป็น

---

[150] Article 89(2) of GDPR

(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

การประมวลผลโดยมีวัตถุประสงค์เพื่อการศึกษาวิจัยในทางวิทยาศาสตร์หรือประวัติศาสตร์หรือเพื่อวัตถุประสงค์ในทางสถิติ ทั้งนี้ ก่อนการประมวลผลดังกล่าวผู้ควบคุมข้อมูลจะต้องพิจารณาผลประโยชน์ในกรณีที่ไม่มีการประมวลผลเปรียบเทียบก่อน โดยผลประโยชน์ของการศึกษาวิจัยจะต้องสูงกว่าผลประโยชน์ของเจ้าของข้อมูล ตามมาตรา 27(1) ของ BDSG[151] ไม่เช่นนั้นการประมวลผลข้อมูลส่วนบุคคลจะไม่สามารถกระทำได้

ภายหลังการพิจารณาผลประโยชน์ หากการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของการศึกษาวิจัยในทางวิทยาศาสตร์หรือประวัติศาสตร์และเพื่อวัตถุประสงค์ในทางสถิติสามารถดำเนินการได้ ข้อมูลส่วนบุคคลดังกล่าวจะต้องผ่านมาตรการในการลบหรือลดการเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลก่อนเสมอ เช่น อาศัยการลบการระบุตัวตน (Anonymized) หรือการแยกสิ่งเชื่อมโยงตัวบุคคลออกไปจัดเก็บไว้ต่างหาก เป็นต้น ตามมาตรา 27(3) ของ BDSG[152]

---

[151] Section 27(1) of BDSG

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research pur-poses or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sen-tence.

[152] Section 27(3) of BDSG

(3) In addition to the measures listed in Section 22 (2), special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They

นอกจากนี้มาตรา 28 ของ BDSG[153] ยังกำหนดข้อยกเว้นให้สิทธิของเจ้าของข้อมูลในการโอนย้ายข้อมูลส่วนบุคคล (Data Portability) อาจถูกกำจัดภายใต้ BDSG หากการจำกัดสิทธิดังกล่าวเป็นการดำเนินการเพียงวิธีการเดียวที่จะประสบผลสำเร็จในการศึกษาวิจัย แต่สำหรับสิทธิในการได้รับข้อมูลของเจ้าของข้อมูล (right to be informed) จะถูกกำจัดโดยสิ้นเชิงหากข้อเท็จจริงปรากฏว่าการปฏิบัติตามสิทธิของเจ้าของข้อมูลจะก่อให้เกิดค่าใช้จ่ายที่ไม่สมส่วนเมื่อเทียบกับค่าใช้จ่ายในการศึกษาวิจัยและการกำจัดสิทธิดังกล่าวมีความจำเป็นอย่างมากในการประสบความสำเร็จในการศึกษาวิจัย

---

may be combined with the information only to the extent required by the research or statistical purpose.

[153] Section 28 of BDSG

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.

(3) The right of the data subject to rectification according to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add this version to the files.

(4) The rights provided in Article 18 (1) (a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as these rights are likely to render impos-sible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes.

ส่วนการจำกัดสิทธิในการแก้ไขข้อมูล (Right to recitification) อาจกระทำได้เพื่อให้การศึกษาวิจัยประสบความสำเร็จ แต่อย่างไรก็ตาม เพื่อไม่ให้เจ้าของข้อมูลรู้สึกว่าการดำเนินการเช่นว่านั้นทำให้เจ้าของข้อมูลอยู่ในสถานะที่ไม่ได้รับความคุ้มครอง เจ้าของข้อมูลมีโอกาสที่จะโต้กลับได้โดยระบุว่าข้อมูลส่วนบุคคลดังกล่าวไม่ถูกต้อง ทั้งนี้ ตามมาตรา 28(3) ของ BDSG นอกจากนี้ข้อมูลส่วนบุคคลอาจเปิดเผยสู่สาธารณะเพื่อวัตถุประสงค์ของการศึกษาวิจัยหรือสถิติถ้าเจ้าของข้อมูลให้ความยินยอมหรือถ้าเป็นส่วนสำคัญในการนำเสนอผลงานการวิจัยในกรณีที่เป็นประวัติศาสตร์ปัจจุบันตามมาตรา 28(3) ของ BDSG

<u>การจำกัดสิทธิของเจ้าของข้อมูล</u> (Restriction of the Rights of Data Subjects) BDSG จำกัดสิทธิของเจ้าของข้อมูลในประเด็นดังต่อไปนี้

1. การจำกัดสิทธิได้รับข้อมูล (Right to be informed) โดยหลักผู้ควบคุมข้อมูลย่อมมีหน้าที่ต้องจัดหาข้อมูลที่เกี่ยวข้องกับการประมวลผลให้แก่เจ้าของข้อมูลตามที่ได้มีการร้องขอ อย่างไรก็ตาม มาตรา 29(1)[154] ของ BDSG กำหนดข้อยกเว้นให้ผู้ควบคุมข้อมูลไม่ต้อง

---

[154] Section 29(1) of BDSG

(1) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the ob-ligation to provide information to the data subject according to Article 14 (1) to (4) of Regu-lation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose in-formation which by its nature must be kept secret, in particular because of overriding legit-imate interests of a third party. The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from the exception pursuant to the third sentence, the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

จัดหาข้อมูลให้แก่เจ้าของข้อมูล หากข้อมูลดังกล่าวโดยลักษณะตามธรรมชาติเป็นข้อมูลที่ต้องเก็บเป็นความลับ เนื่องจากการเปิดเผยจะส่งผลกระทบต่อผลประโยชน์ตามกฎหมายของบุคคลภายนอก นอกจากนี้กรณีที่ผู้ควบคุมข้อมูลเป็นผู้ถือข้อมูลตามวิชาชีพ เช่น ทนายความ ผู้ตรวจสอบบัญชี แพทย์ เป็นต้น โดยหลักผู้ควบคุมข้อมูลดังกล่าวย่อมไม่มีหน้าที่ต้องเปิดเผยข้อมูลต่อเจ้าของข้อมูลแม้เจ้าของข้อมูลจะมีสิทธิได้รับข้อมูลก็ตาม ยกเว้นกรณีที่ผลประโยชน์ตามกฎหมายของเจ้าของข้อมูลสำคัญกว่า ทั้งนี้ ตามมาตรา 29(2)[155] ของ BDSG

การจำกัดสิทธิในการได้รับแจ้งข้อมูลในกรณีที่มีการเปลี่ยนวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลหากข้อมูลส่วนบุคคลดังกล่าวถูกจัดเก็บในลักษณะ ของ Analouge Form โดยวัตถุประสงค์ในการประมวลผลดังกล่าวยังอยู่ในขอบเขตของวัตถุประสงค์เดิม และการแจ้งให้เจ้าของข้อมูลทราบไม่สามารถทำโดยระบบดิจิทัล (มาตรา 32(1) ของ BDSG[156])

---

[155] Section 29(2) of BDSG

(2) If in the context of a client-lawyer relationship the data of third persons are trans-ferred to persons subject to a legal obligation of professional secrecy, the transferring body shall not be obligated to inform the data subject according to Article 13 (3) of Regu-lation (EU) 2016/679 unless the data subject has an overriding interest in being informed.

[156] Section 32(1) of BDSG

(1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the ob-ligation to provide information to the data subject according to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use

1. concerns the further processing of data stored in analogue form, for which the control-ler directly contacts the data subject through the further processing; the purpose is compatible with the original purpose for which the data were collected in accordance with Regulation (EU) 2016/679; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the infor-mation can be regarded as minimal, given the circumstances of the individual case, in particular with regard to the context in which the data were collected;

การจำกัดสิทธิในการได้รับแจ้งข้อมูลกรณีที่ข้อมูลดังกล่าวจะมีผลกระทบในทางลบต่อการยืนยัน การแสดงออก หรือการโต้แย้งข้อเรียกร้องตามสิทธิในทางแพ่งหรือก่อให้เกิดความเสี่ยงต่อความปลอดภัยสาธารณะ เป็นต้น (มาตรา 33(1) ของ BDSG[157])

---

2. would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;

3. would endanger public security or order or would otherwise be detrimental to the wel-fare of the Federation or a *Land*, and the controller's interests in not providing the in-formation outweigh the interests of the data subject;

4. would interfere with the establishment, exercise or defence of legal claims, and the controller's interests in not providing the information outweigh the interests of the data subject; or

5. would endanger a confidential transfer of data to public bodies.

[157] Section 33(1) of BDSG

(1) In addition to the exception in Article 14 (5) of Regulation (EU) 2016/679 and in Section 29 (1), first sentence, the obligation to provide information to the data subject ac-cording to Article 14 (1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if provid-ing information

1. in the case of a public body

a) would endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, or

b) would threaten the public security or order or otherwise be detrimental to the Federation or a *Land*,

and therefore the data subject's interest in receiving the information must not take prece-dence;

2. in the case of a private body

2. การจำกัดสิทธิเข้าถึงข้อมูล (Right to access) เช่นเดียวกับสิทธิได้รับข้อมูล โดยหลักผู้ควบคุมข้อมูลย่อมมีหน้าที่ต้องจัดให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลส่วนบุคคลได้ อย่างไรก็ตาม มาตรา 29(1) ของ BDSG[158] ได้จำกัดสิทธิประเภทนี้ไว้ หากข้อมูลที่จะเข้าถึงเป็นข้อมูล

---

a) would interfere with the establishment, exercise or defence of legal claims, or processing includes data from contracts under private law and is intended to pre-vent harm from criminal offences, unless the data subject has an overriding legit-imate interest in receiving the information; or

b) the responsible public body has determined with respect to the controller that dis-closing the data would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a Land; in the case of data pro-cessing for purposes of law enforcement, no determination pursuant to the first half-sentence shall be required.

[158] Section 29(1) of BDSG

(1) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the ob-ligation to provide information to the data subject according to Article 14 (1) to (4) of Regu-lation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose in-formation which by its nature must be kept secret, in particular because of overriding legit-imate interests of a third party. The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from the exception pursuant to the third sentence, the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

ที่ต้องเก็บรักษาไว้เป็นความลับ เนื่องจากการเปิดเผยจะกระทบต่อผลประโยชน์ตามกฎหมายของบุคคลภายนอกที่สำคัญกว่า

3. การจำกัดสิทธิได้รับแจ้งการละเมิดข้อมูลส่วนบุคคล (Right to be informed of a personal data breach) โดยหลักผู้ควบคุมข้อมูลย่อมมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคล แต่มาตรา 29(1) ของ BDSG ได้ยกเว้นหน้าที่ดังกล่าวของผู้ควบคุมข้อมูล หากการแจ้งการละเมิดดังกล่าวทำให้ผู้ควบคุมข้อมูลต้องเปิดเผยข้อมูลที่ต้องเก็บรักษาไว้เป็นความลับ ซึ่งหากเปิดเผยจะกระทบต่อผลประโยชน์ตามกฎหมายของบุคคลภายนอก

ทั้งนี้ แม้ว่า BDSG จะเปิดโอกาสให้มีการจำกัดสิทธิของเจ้าของข้อมูลได้ แต่มาตรา 34 ของ BDSG ก็กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องบอกเหตุผลในการปฏิเสธที่จะแจ้งข้อมูลดังกล่าวเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลทราบด้วย

4. การจำกัดสิทธิในการลบข้อมูลส่วนบุคคล (Right to erasure) ในกรณีที่เป็นการประมวลผลแบบ non-automated ในกรณีที่การลบข้อมูลส่วนบุคคลไม่สามารถกระทำได้หรือหากกระทำได้จะก่อให้เกิดภาระค่าใช้จ่ายเป็นจำนวนมาก แต่การประมวลผลข้อมูลก็จะต้องถูกจำกัดภายใต้กฎหมายเช่นกัน และหากการประมวลผลดังกล่าวเป็นการประมวลผลที่ผิดกฎหมายมาตั้งแต่ต้น ข้อจำกัดในการลบข้อมูลส่วนบุคคลนี้ย่อมไม่มีผลใช้บังคับ (มาตรา 35 ของ BDSG[159])

---

[159] Section 35 of BDSG

(1) If in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in ac-cordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure. The first and second sentences shall not apply if the personal data were processed unlaw-fully.

(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, subsection 1, first and second sentences shall apply accordingly in the case of Article

<u>การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล</u> (Data protection officer) มาตรา 37 ของ GDPR กำหนดให้องค์กรหรือหน่วยงานเอกชนที่ให้บริการระบบการประมวลผลแบบคลาวด์ในกรณีที่กำหนด เช่น กรณีการประมวลผลใน Scale ใหญ่ เป็นต้น ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม GDPR ได้เปิดช่องให้ประเทศสมาชิกสามารถบัญญัติเพิ่มเติมได้ว่ากรณีใดบ้างนอกเหนือจากที่กำหนดไว้ใน GDPR ที่องค์กรหรือหน่วยงานเอกชนมีหน้าที่ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนั้น BDSG จึงกำหนดไว้ในมาตรา 38[160] ของตนให้องค์กรหรือหน่วยงานเอกชนจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากมีการจ้างงานบุคคลซึ่งทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ (Automated processing of personal data) ตั้งแต่ 10 คนขึ้นไป อย่างไรก็ตาม หากการประมวลผลดังกล่าวมีลักษณะ

---

17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.

(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, subsection 1 shall apply accordingly in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

[160] Section 38 of BDSG

(1) In addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ as a rule at least ten persons dealing with the automated processing of personal data. If the control-ler or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process per-sonal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, they shall designate a data protection officer regardless of the number of persons employed in processing.

(2) Section 6 (4), (5), second sentence, and (6) shall apply, Section 6 (4) however shall apply only if designating a data protection officer is mandatory.

ดังต่อไปนี้ องค์กรหรือหน่วยงานเอกชนจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยไม่ต้องคำถึงจำนวนบุคคลที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ

(1) เป็นการประมวลผลที่อยู่ภายใต้บังคับเรื่องการประเมินผลกระทบของการคุ้มครองข้อมูล (Data protection impact assessment) ตามมาตรา 35 ของ GDPR หรือ

(2) เป็นการประมวลผลข้อมูลส่วนบุคคลในทางธุรกิจที่มีวัตถุประสงค์เพื่อการถ่ายโอนข้อมูล การวิจัยเชิงธุรกิจ หรือการสำรวจความเห็น (Opinion polling)

4.4 กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่รองรับระบบการประมวลผลแบบคลาวด์โดยเฉพาะ

ในระบบการคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศมองการให้บริการระบบการประมวลผลแบบคลาวด์ว่าเป็นระบบที่มีผลกระทบที่สำคัญต่อระบบการคุ้มครองข้อมูลส่วนบุคคล โดยมองว่าการให้บริการระบบการประมวลผลแบบคลาวด์ไม่ได้สร้างปัญหาใหม่ให้แก่ระบบการคุ้มครองข้อมูลส่วนบุคคล แต่กลับเพิ่มความซับซ้อนของประเด็นปัญหาในการคุ้มครองข้อมูลส่วนบุคคลให้ซับซ้อนมากยิ่งขึ้นกว่าเดิม โดยเฉพาะอย่างยิ่งในประเด็นเรื่องการส่งหรือโอนข้อมูลระหว่างประเทศ ดังนั้น ในช่วงระยะเวลาที่ผ่านมาจึงมีหลายประเทศพยายามยกร่างกฎหมายที่จะใช้บังคับคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บหรือประมวลผลในระบบการประมวลผลแบบคลาวด์โดยเฉพาะ อย่างไรก็ตาม ประเทศที่บัญญัติกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์โดยเฉพาะเป็นผลสำเร็จในขณะนี้ได้แก่ ประเทศแม็กซิโกและประเทศเกาหลีใต้ ซึ่งจะได้ศึกษาในรายละเอียดดังต่อไปนี้

4.4.1 ประเทศแม็กซิโก

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีการกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ไว้เป็นการเฉพาะของประเทศแม็กซิโกนั้น ได้แก่ กฎหมายทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ (The General Law for the Protection of Personal Data held by Regulated Subjects) ซึ่งเกิดขึ้นหลังจากการแก้ไข มาตรา 6 ของรัฐธรรมนูญแห่งประเทศแม็กซิโกในปีค.ศ. 2014 และภายหลังประกาศใน ราชกิจจานุเบกษา เมื่อวันที่ 26 มกราคม 2560 กฎหมายฉบับดังกล่าวก็มีผลใช้บังคับในวันถัดจากวันที่ประกาศในราชกิจจานุเบกษาทันที โดยหน่วยงานรัฐที่เกี่ยวข้องจะต้องรับหลักการตามกฎหมายฉบับนี้ไปปฏิบัติตามภายในระยะเวลา 6 เดือนนับตั้งแต่วันที่กฎหมายฉบับนี้มีผลใช้บังคับ[161] และกฎหมายสหพันธรัฐว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของเอกชน (The Federal Law on The Protection of Personal Data Held by Private Parties) ซึ่งเป็นรากฐานในการแก้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐข้างต้น ทั้งนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลในความครอบครองของเอกชนมีผลใช้

[161] Miguel Recio, “Mexico's new public-sector data protection law,” สืบค้นเมื่อวันที่ 30 กันยายน 2560, จาก https://iapp.org/news/a/mexicos-new-public-sector-data-protection-law/

บังคับเมื่อวันที่ 22 ธันวาคม 2554[162] ที่ผ่านมา โดยกฎหมายดังกล่าวมุ่งให้ความคุ้มครองสิทธิของเจ้าของข้อมูล ความปลอดภัยและการละเมิดบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ความยินยอม การส่งหรือโอนข้อมูล ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ ดังนั้น ข้อมูลอื่นๆ ที่ไม่ใช่ข้อมูลส่วนบุคคล เช่น ข้อมูลทั่วๆ ไป หรือ Big Data หรือข้อมูลความลับทางการค้า จะไม่อยู่ภายใต้บังคับของกฎหมายฉบับนี้ แต่อาจอยู่ภายใต้บังคับของกฎหมายฉบับอื่น ซึ่งไม่อยู่ในขอบเขตของการศึกษาในครั้งนี้

หลักการสำคัญที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ของกฎหมายทั้งสองฉบับข้างต้น มีรายละเอียดดังนี้

4.4.1.1 กฎหมายทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ (The General Law for the Protection of Personal Data held by Regulated Subjects)

กฎหมายฉบับนี้กำหนดบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการระบบการประมวลผลแบบคลาวด์ในภาครัฐจำนวนทั้งสิ้น 2 มาตรา โดยให้ความหมายของระบบการประมวลผลแบบคลาวด์ไว้ในมาตรา 3.VI ว่าระบบการประมวลผลแบบคลาวด์ หมายถึง รูปแบบการให้บริการประมวลผลตามความต้องการของผู้ใช้จากภายนอกซึ่งเกี่ยวข้องกับการให้บริการโครงสร้างพื้นฐาน แพลตฟอร์ม หรือซอฟต์แวร์ที่สามารถปรับแต่งได้และสามารถใช้งานร่วมกัน[163] บทนิยามที่ถูกกำหนดในกฎหมายฉบับนี้มีผู้ให้ความเห็น[164] ว่า ควรจะต้องบังคับใช้ในการพิจารณาบทนิยามของระบบการประมวลผลแบบคลาวด์ในกฎหมายอื่นของหน่วยงานของรัฐด้วยเช่นกัน ในกรณีที่กฎหมายดังกล่าวไม่ได้บัญญัติบทนิยามของระบบการประมวลผลแบบคลาวด์ไว้โดยเฉพาะ

---

[162] Privacy laws and business, “Mexico: DP regulations enter into force,” สืบค้นเมื่อวันที่ 29 กันยายน 2560, จาก https://www.privacylaws.com/Publictions/enews/International-E-news/Dates/2012/1/Mexico-DP-regulations-enter-into-force/

[163] “A model of external provision of computing services on-demand, involving the provision of infrastructure, platform or software, flexible provisioned, through virtual procedures, in dynamically shared resources”

[164] Miguel Recio, *supra note 166*.

นอกจากนี้ กฎหมายฉบับนี้ยังกำหนดให้ผู้ควบคุมข้อมูลที่เป็นหน่วยงานของรัฐสามารถเข้าทำสัญญาว่าจ้างหรือเข้าใช้บริการแอพพลิเคชั่นหรือโครงสร้างพื้นฐานของระบบการประมวลผลแบบคลาวด์ รวมทั้งเทคโนโลยีอื่นๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากระบบการประมวลผลแบบคลาวด์ได้ ทั้งนี้ เงื่อนไขของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ (มาตรา 63[165]) จะต้องเป็นไปตามที่กำหนดขึ้น เพื่อบังคับให้หน่วยงานของ

---

[165] มาตรา 63 เป็นมาตราที่มีบทบัญญัติเช่นเดียวกับมาตรา 52 ของ The Federal Law On the Protection of Personal Data held by Private Parties ดังนี้

Article 52 For the processing of personal data in services, applications, and infrastructure in what is called “cloud computing,” in which the data controller adheres to the same by general contractual conditions or clauses, such services may only be used when the provider:

I. Complies at least with the following:

a) Has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;

b) Makes transparent subcontracting that involves information about the service which is provided;

c) Abstains from including conditions in providing the service that authorize or permits it to assume the ownership of the information about which the service is provided, and

d) Maintains confidentiality with respect to the personal data about which it provides the service, and

II. Has mechanisms at least for:

a) Disclosing changes in its privacy policies or conditions of the service it provides;

b) Permitting the data controller to limit the type of processing of personal data about which it provides the service;

c) Establishing and maintaining adequate security measures to protect the personal data about which it provides the service;

รัฐที่อยู่ในสถานะของผู้ควบคุมข้อมูลสามารถเข้าใช้บริการระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการ เฉพาะในกรณีที่ผู้ให้บริการสามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสมเท่านั้น ซึ่งการพิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์รายใดจะสามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสมหรือไม่ ย่อมต้องพิจารณาว่าผู้ให้บริการรายดังกล่าวมีการปฏิบัติตามเงื่อนไขที่กำหนดไว้ในมาตรา 63 ซึ่งมีลักษณะเป็นเงื่อนไขขั้นต่ำที่จะต้องปฏิบัติตามหรือไม่ อาทิ ผู้ให้บริการมีนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ใกล้เคียงกับหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้กำหนดหรือไม่ เป็นต้น

4.4.1.2 กฎหมายทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชน (The Federal Law On the Protection of Personal Data held by Private Parties)

กฎหมายฉบับนี้กำหนดบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการระบบการประมวลผลแบบคลาวด์จำนวนทั้งสิ้น 1 มาตรา โดยเป็นบทบัญญัติที่ให้บทนิยามของระบบการประมวลผลแบบคลาวด์ไว้ว่า หมายถึง รูปแบบการให้บริการประมวลผลตามความต้องการของผู้ใช้จากภายนอกซึ่งเกี่ยวข้องกับการให้บริการโครงสร้างพื้นฐาน แพลตฟอร์ม หรือซอฟต์แวร์ที่สามารถปรับแต่งได้และสามารถใช้งานร่วมกัน ซึ่งเป็นการให้คำจำกัด

---

d) Ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it, and

e) Impeding access to personal data by those who do not have proper access or in the event of a request duly made by a competent authority, so inform the data controller.

In any case, the data controller may not use services that do not ensure the proper protection of personal data.

For purposes of these Regulations, cloud computing shall mean the model for the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared.

Regulatory agencies, within the scope of their authority, and assisting the Institute, shall issue guidelines for the proper processing of personal data in what is called “cloud computing.

ความที่เหมือนกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐข้างต้น

ภายใต้กฎหมายฉบับนี้ ระบบการประมวลผลแบบคลาวด์จะสามารถให้บริการได้ต่อเมื่อผู้ให้บริการปฏิบัติตามเงื่อนไขขั้นต่ำที่กฎหมายกำหนดไว้ดังต่อไปนี้

- กำหนดและใช้นโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปในทำนองเดียวกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้ภายใต้กฎหมายฉบับนี้
- มีความโปร่งใสในกรณีที่จะให้บุคคลอื่นทำหน้าที่ประมวลผลแทนตน
- รักษาความลับของข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์
- ละเว้นการกำหนดเงื่อนไขในการให้บริการเกี่ยวเนื่องกับความเป็นเจ้าของในข้อมูล

นอกจากนี้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะต้องมีกระบวนการหรือกลไกอย่างน้อยตามที่กำหนดดังต่อไปนี้ด้วย เช่น

- มีระบบหรือกลไกสำหรับการเปิดเผยการเปลี่ยนแปลงเรื่องนโยบายความเป็นส่วนตัวหรือเงื่อนไขของบริการของตน
- มีระบบหรือกลไกสำหรับการอนุญาตให้ผู้ควบคุมข้อมูลจำกัดประเภทของการประมวลผลข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ได้
- มีระบบหรือกลไกสำหรับการจัดให้มีมาตรการรักษาความปลอดภัยที่แม่นยำเพื่อที่จะคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์
- มีระบบหรือกลไกสำหรับรับรองการกู้คืนข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ในภายหลังที่มีการระงับการใช้บริการแล้ว
- มีระบบหรือกลไกสำหรับการแจ้งให้ผู้ควบคุมข้อมูลทราบ หากมีการเข้าถึงข้อมูลในลักษณะที่เป็นการคุกคามจากบุคคลที่ไม่ได้รับอนุญาตหรือหากมีการเข้าถึงข้อมูลโดยหน่วยงานที่มีอำนาจเข้าถึงได้

อนึ่ง เป็นดุลยพินิจของผู้ควบคุมข้อมูลว่าจะใช้บริการระบบการประมวลผลแบบคลาวด์ที่ไม่สามารถรับรองหรือพิสูจน์ให้เห็นถึงมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมได้หรือไม่ อย่างไรก็ตาม กฎหมายฉบับนี้ให้อำนาจแก่หน่วยงานที่มีหน้าที่รับผิดชอบในการออกระเบียบหรือประกาศที่เหมาะสมกับการประมวลผลข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ด้วย

4.4.2 ประเทศเกาหลีใต้

แต่เดิมในอดีตประเทศเกาหลีใต้ไม่ได้บัญญัติกฎหมายกลางที่ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ ดังนั้น ในระยะต่อมาจึงมีการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเกาหลีใต้ในลักษณะของกฎหมายทั่วไปขึ้นโดยใช้ชื่อว่า Personal Information Protection Act หรือ “PIPA” ซึ่งมีผลใช้บังคับเป็นกฎหมายทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเมื่อวันที่ 30 กันยายน 2554 อย่างไรก็ตาม โครงสร้างของระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเกาหลีใต้ยังประกอบไปด้วยกฎหมายเฉพาะอื่นๆ ที่ให้ความคุ้มครองข้อมูลส่วนบุคคลด้วย ได้แก่

1) The Act on Promotion of Information and Communication Network Utilisation and Information Protection หรือ “IT Network Act”
2) The Use and Protection of Credit Information Act หรือ “UPCIA”
3) The Act on Real Name Financial Transaction and Guarantee of Secrecy หรือ “ARNFTGS”

แต่อย่างไรก็ตาม กฎหมายฉบับดังกล่าวข้างต้นต่างก็มิได้กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ไว้โดยเฉพาะ ดังนั้น เมื่อวันที่ 3 มีนาคม 2558 รัฐสภาแห่งประเทศเกาหลีใต้ จึงได้ผ่านกฎหมายฉบับหนึ่งเกี่ยวกับการให้บริการระบบการประมวลผลแบบคลาวด์โดยตรง โดยเรียกชื่อว่า “An Act on the Development of Cloud Computing and Protection of Users” โดยกฎหมายฉบับนี้มีวัตถุประสงค์เพื่อเพิ่มความสามารถในการแข่งขันในอุตสาหกรรมของประเทศโดยการอนุญาตให้ภาครัฐสามารถใช้บริการระบบการประมวลผลแบบคลาวด์ของเอกชนได้และส่งเสริมการลงทุนในการวิจัยและสร้างระบบกฎหมายที่คุ้มครองข้อมูลของผู้ใช้งานระบบการประมวลผลแบบคลาวด์

หลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายฉบับข้างต้นนั้นปรากฏอยู่ในมาตรา 26 ว่าด้วยการเปิดเผยข้อมูลสำหรับการคุ้มครองผู้ใช้งาน (Disclosure of Information for Protection of Users, etc.) และมาตรา 27 ว่าด้วยการคุ้มครองข้อมูลของผู้ใช้งาน (Protection of User Information) โดยมีหลักการที่สำคัญ ดังต่อไปนี้

4.4.2.1 บทนิยามที่สำคัญ

ภายใต้มาตรา 2 ของกฎหมายดังกล่าว ระบบการประมวลผลแบบคลาวด์ หมายความถึง ระบบการประมวลผลข้อมูลที่ช่วยให้การเข้าใช้งานเป็นไปได้โดยง่ายและเป็น

ระบบที่มีการแชร์ทรัพยากรระหว่างกัน[166] ส่วนข้อมูลของผู้ใช้งาน หมายความถึง ข้อมูลที่ถูกจัดเก็บโดยผู้ใช้งานระบบการประมวลผลแบบคลาวด์ในทรัพยากรของผู้ให้บริการซึ่งผู้ใช้งานเป็นเจ้าของและเป็นผู้บริหารจัดการข้อมูลเหล่านั้น[167]

---

[166] Article 2 (1)-(3)

The terms used in this Act shall be defined as follows:

1. The term "cloud computing" means an information processing system that makes it possible to flexibly use integrated and shared resources for information and communications (hereinafter referred to as "resources for information and communications"), such as devices for information and communications, information and communications systems, and software, through information and communications networks in accordance with changes in users' requirements or demands;

2. The term "cloud computing technologies" means information and communications technologies specified by Presidential Decree as those for the establishment and use of cloud computing, including technologies for virtualization and distributed processing;

3. The term "cloud computing services" means the services specified by Presidential Decree as commercial services of providing resources for information and communications to others by utilizing cloud computing;

[167] Article 2(4)

4. The term "user information" means the information (referring to the information prescribed in subparagraph 1 of Article 3 of the Framework Act on National Informatization) stored by a user of cloud computing services (hereinafter referred to as "user") in the resources for information and communications of the person who provides the cloud computing services through a cloud computing system (hereinafter referred to as "cloud computing service provider") and owned or managed by the user.

4.4.2.2 การเปิดเผยข้อมูลเกี่ยวกับผู้ให้บริการเพื่อคุ้มครองผู้ใช้งาน

มาตรา 26 ว่าด้วยการเปิดเผยข้อมูลสำหรับการคุ้มครองผู้ใช้งาน บัญญัติให้ผู้ใช้งานระบบการประมวลผลแบบคลาวด์สามารถร้องขอให้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์แจ้งชื่อประเทศที่ข้อมูลของตนถูกจัดเก็บอยู่ได้[168] นอกจากนี้ หากรัฐมนตรีกระทรวงวิทยาศาสตร์ เทคโนโลยีและการวางแผนอนาคต (Ministrer of Science, ICT and Future Planning) เล็งเห็นว่า กรณีมีความจำเป็นที่จะต้องคุ้มครองผู้ใช้งาน รัฐมนตรีอาจแนะนำให้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์เปิดเผยชื่อของประเทศที่มีการจัดเก็บข้อมูลของผู้ใช้งาน

[168] Article 26(1)

1. Any user may request a cloud computing service provider to inform him/her of the name of the country where the relevant user information is stored.

ได้[169] โดยก่อนการแนะนำเช่นว่านั้นรัฐมนตรีจะต้องขอความเห็นจากคณะกรรมการการสื่อสารแห่งเกาหลี (The Korea Communications Commission) ก่อนเสมอ[170]

4.4.2.3 การคุ้มครองข้อมูลของผู้ใช้งาน

มาตรา 27 กำหนดหลักการคุ้มครองข้อมูลของผู้ใช้งานไว้ว่า ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ไม่สามารถเปิดเผยข้อมูลของผู้ใช้งานโดยปราศจากความยินยอมให้แก่บุคคลที่สามหรือใช้ข้อมูลของผู้ใช้งานเพื่อวัตถุประสงค์อื่นใดนอกเหนือจากการให้บริการแก่

---

[169] Article 26(2)-(3)

2.Any person who uses information and communications services (referring to the information and communications services defined by subparagraph 2 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.; hereinafter the same shall apply in paragraph (3)) may request an information and communications service provider (referring to the information and communications service provider defined by subparagraph 3 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.; hereinafter the same shall apply in paragraph (3)) to inform him/her as to whether it uses cloud computing services and the name of the country where the relevant user information is stored.

3. Where the Minister of Science, ICT and Future Planning deems it necessary for protecting users or the users of information and communications services, he/she may recommend that cloud computing service providers or information and communications service providers disclose the information referred to in paragraph (1) or (2).

[170] Article 26(4)

4. Where the Minister of Science, ICT and Future Planning intends to recommend the disclosure of information pursuant to paragraph (3), he/she shall seek opinions from the Korea Communications Commission thereon.

ผู้ใช้งานได้ เว้นแต่ศาลจะมีคำสั่งให้ดำเนินการเช่นว่านั้น[171] หมายความว่า หากผู้ให้บริการระบบการประมวลผลแบบคลาวด์ได้รับความยินยอมจากผู้ใช้งานให้สามารถเปิดเผยข้อมูลได้ หรือให้ใช้ข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากการให้บริการได้แล้ว ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ย่อมสามารถดำเนินการเช่นว่านั้นได้โดยจะต้องแจ้งข้อมูลอย่างน้อยดังต่อไปนี้[172] ให้แก่ผู้ใช้งานทราบด้วย

---

[171] Article 27(1)

1.No cloud computing service provider shall provide user any information to a third party or use user information for any purpose other than for the purpose of providing services, without the relevant user's consent, unless it is required by a court order to submit or a warrant issued by a judge. The foregoing shall also apply to a third party to whom a cloud computing service provider has provided user information.

[172] Article 27(2)

2. Where a cloud computing service provider intends to provide any user information to a third party or to use the user information for any purpose other than for the purpose of providing services, it shall notify the user of the following matters and shall obtain consent thereto. The same shall apply where a change occurs to any of the following matters:

(1) The person to whom the user information is to be provided;

(2) The purpose of use of the user information (referring to the purpose of use of the person to whom the information is provided, if it is provided);

(3) A list of user information used or provided;

(4) The period of holding and use of user information (referring to the period of possession and user information by the person to whom user information is provided, where such information is provided);

(5) A statement that the user has a right to refuse to give consent and the details of disadvantages in such cases, if disadvantages are given against refusal to give consent.

- บุคคลที่ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะเปิดเผยข้อมูลให้
- วัตถุประสงค์ของผู้ได้รับการเปิดเผยข้อมูลสำหรับการใช้ข้อมูลของผู้ใช้งานที่ได้รับการเปิดเผย
- รายการข้อมูลของผู้ใช้งานที่จะนำไปเปิดเผยหรือนำไปใช้งาน
- ระยะเวลาการครอบครองและระยะเวลาการใช้ข้อมูลของผู้ใช้งาน
- คำบอกกล่าวแก่ผู้ใช้งานว่าผู้ใช้งานมีสิทธิที่จะปฏิเสธที่จะให้ความยินยอมและรายละเอียดของผลเสียหายที่จะตามหากไม่ให้ความยินยอม

ทั้งนี้ ในกรณีที่สัญญาหรือข้อตกลงการให้บริการระบบการประมวลผลแบบคลาวด์สิ้นสุดลง ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะต้องส่งคืนข้อมูลของผู้ใช้บริการและทำลายข้อมูลที่ตนเองเก็บไว้ในระบบการประมวลผลแบบคลาวด์ด้วย (ในกรณีที่โดยสภาพข้อมูลดังกล่าวไม่สามารถส่งคืนได้อันเนื่องมาจากผู้ใช้งานไม่ยอมรับการส่งคืนนั้นหรือไม่ประสงค์จะให้ผู้ให้บริการส่งคืนข้อมูล)[173]

อนึ่ง หากผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประสงค์จะเลิกกิจการ ผู้ให้บริการรายดังกล่าวจะต้องแจ้งให้ผู้ใช้บริการแต่ละรายทราบพร้อมทั้งส่งคืนข้อมูลของผู้ใช้งานก่อนวันเลิกกิจการ แต่หากข้อมูลดังกล่าวไม่สามารถส่งคืนได้อันเนื่องมาจากผู้ใช้งานไม่ยอมรับการส่งคืนนั้นหรือไม่ประสงค์จะให้ผู้ให้บริการส่งคืนข้อมูล ผู้ให้บริการจะต้องทำลายข้อมูลของผู้ใช้งานก่อนวันเลิกกิจการแทน[174]

---

[173] Article 27(3) Where the contract made with a user terminates, the cloud computing service provider shall return the user information to the user and destroy the user information possessed by the cloud computing service provider: Provided, That the user information shall be destroyed, if it is actually impossible to return the user information, because the user does not accept the return of the user information or does not want to have the user information returned.

[174] Article 27(4) Where a cloud computing service provider intends to close its business, it shall notify each user of the closure of business, return the user information before the date of closure of business, and destroy the user information possessed by the cloud computing service provider: Provided, That the user information shall be destroyed, if it is actually impossible to return the user information, because the user does not accept the return of the user information or does not wish to have the user information returned.

บทที่ 5
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยและปัญหาที่เกิดขึ้นเมื่อบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์

ดังที่ได้กล่าวในบทก่อนว่าหลายประเทศให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล โดยหันมาออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อบังคับใช้กับประเทศของตนเอง ซึ่งสำหรับประเทศไทยเอง ก็มีแนวคิดที่จะออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกัน ทั้งนี้ แนวความคิดในการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ได้พัฒนาขึ้นมาควบคู่กันกับพัฒนาการทางด้านการเมืองของประเทศไทยตลอดมา โดยประเทศไทยได้มีการประกาศใช้กฎหมายที่มีเนื้อหาเกี่ยวเนื่องกับการคุ้มครองข้อมูลส่วนบุคคลมาแล้วหลายฉบับตั้งแต่ในช่วงแรกภายหลังการเปลี่ยนแปลงการปกครองปี พ.ศ. 2475 เช่น พระราชบัญญัติไปรษณีย์ พุทธศักราช 2477 ซึ่งให้ความคุ้มครองแก่ถุงไปรษณีย์และไปรษณีย์ภัณฑ์ในระหว่างขนส่งทางไปรษณีย์ โดยเจ้าพนักงานจะเปิดหรือยอมให้ผู้อื่นเปิดหรือกักหรือหน่วงเหนี่ยวไปรษณีย์ไม่ได้ พระราชบัญญัติโทรเลขและโทรศัพท์ พุทธศักราช 2477 ซึ่งให้ความคุ้มครองข้อมูลข่าวสารที่ส่งทางโทรเลขและโทรศัพท์เพื่อมิให้ผู้ใดเข้าไปล่วงรู้ข้อมูลรวมทั้งห้ามแพร่งพรายข้อมูลดังกล่าวแก่ผู้ที่ไม่มีสิทธิจะรับรู้ เป็นต้น[1] จะเห็นได้ว่าในยุคแรกเริ่มของการเปลี่ยนแปลงทางการเมือง การออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลจะคำนึงถึงเสรีภาพในการสื่อสารเป็นหลัก ดังที่ปรากฏใน มาตรา 46 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2517 ซึ่งกำหนดให้ บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางไปรษณีย์หรือทางอื่นที่ชอบด้วยกฎหมาย ทั้งนี้ การตรวจ การกักหรือการเปิดเผยจดหมาย โทรเลข โทรศัพท์ หรือสิ่งสื่อสารอื่นใดที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใด เพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกันจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อรักษาความมั่นคงของรัฐ เป็นต้น ต่อมาการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลจึงเริ่มปรากฏเป็นรูปธรรมมากขึ้นโดยผ่านการออกกฎหมายเพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ดังที่กำหนดไว้ในมาตรา 47 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2535 แก้ไขเพิ่มเติมฉบับที่ 5 พ.ศ. 2538 และเพื่อให้สิทธิในการรับรู้ข้อมูลข่าวสารที่อยู่ในความครอบครองของหน่วยงานราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจแก่เอกชน ดังที่กำหนดไว้ในมาตรา 48 ทวิ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.

---

[1] ชั่งทอง โอภาสศิริวิทย์, “การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในประเทศไทย: ปัจจุบันและอนาคต,” วารสารนิติศาสตร์, เล่มที่ 4, ปีที่ 34, น.613, (ธันวาคม 2547).

2535 แก้ไขเพิ่มเติมฉบับที่ 5 พ.ศ. 2538 ซึ่งหลักการดังกล่าวข้างต้นก็ได้ถูกบัญญัติเป็นบรรทัดฐานสำหรับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในรัฐธรรมนูญทุกฉบับจวบจนถึงปัจจุบันด้วยเช่นกัน

จากกฎหมายต่างๆ ข้างต้นจะเห็นได้ว่า แม้ประเทศไทยจะมีแนวคิดเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาเป็นระยะเวลานาน โดยเฉพาะอย่างยิ่งเมื่อมีการประกาศใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ยิ่งเป็นการแสดงให้เห็นถึงแนวคิดเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยที่ชัดเจนเป็นรูปธรรมมากขึ้น แต่อย่างไรก็ตาม แม้ว่าประเทศไทยจะประกาศใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่การให้ความคุ้มครองข้อมูลส่วนบุคคลก็ยังไม่ครอบคลุม เนื่องจากกฎหมายดังกล่าวยังให้ความคุ้มครองอย่างจำกัดโดยจะให้ความคุ้มครองเฉพาะข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานราชการหรืออรัฐวิสาหกิจเท่านั้น[2] นอกจากนี้ในระยะเวลาเดียวกัน รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 ก็มีผลใช้บังคับ และกำหนดห้ามมิให้มีการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบสิทธิส่วนบุคคลในครอบครัว เกียรติยศชื่อเสียง หรือความเป็นอยู่ส่วนตัว ซึ่งจากการประกาศใช้กฎหมายข้างต้นทำให้แนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่กระจัดกระจายของประเทศไทยเริ่มเป็นไปในแนวทางเดียวกันกับมาตรฐานระหว่างประเทศมากยิ่งขึ้น

อย่างไรก็ตาม แม้ว่าแนวคิดของประเทศไทยจะเริ่มคล้ายคลึงกับต่างประเทศ แต่เมื่อพิจารณาระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยเทียบกับระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ จะพบว่าประเทศไทยมีกฎหมายจำนวนมากที่บัญญัติคุ้มครองข้อมูลส่วนบุคคลในเรื่องต่าง ๆ ไว้ เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับต่าง ๆ ประมวลกฎหมายอาญา ประมวลกฎหมายแพ่งและพาณิชย์ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 พระราชบัญญัติคุ้มครองความลับของทางราชการ พ.ศ. 2483 พระราชบัญญัติโทรเลขและโทรศัพท์ พ.ศ. 2477 พระราชบัญญัติการสื่อสารแห่งประเทศไทย พ.ศ. 2519 พระราชบัญญัติองค์การโทรศัพท์แห่งประเทศไทย พ.ศ.

---

[2]อริยพร โพธิใส, “หลักการให้ความคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย,” จุลนิติ, ฉบับที่ 5, ปีที่ 11, น.137, (กันยายน – ตุลาคม 2557).

2497 เป็นต้น[3] ดังนั้น แม้ว่าประเทศไทยจะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีลักษณะคล้ายคลึงกับกฎหมายกลาง แต่กฎหมายดังกล่าวยังไม่สามารถใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของเอกชนได้ ทำให้ประเทศไทยจึงเป็นประเทศที่ใช้ระบบกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแบบผสม กล่าวคือ ใช้ระบบกฎหมายเฉพาะในกรณีที่มีกฎหมายบัญญัติเกี่ยวกับข้อมูลส่วนบุคคลในเรื่องใดเรื่องหนึ่งไว้แล้ว และใช้กฎหมายกลางในกรณีที่เรื่องนั้น ๆ ยังไม่มีกฎหมายบัญญัติเกี่ยวกับข้อมูลส่วนบุคคลเอาไว้

อนึ่ง หากในอนาคตประเทศไทยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลใช้บังคับประเทศไทยก็จะมีกฎหมายกลางที่ใช้บังคับควบคู่กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งจะส่งผลโดยตรงต่อการคุ้มครองข้อมูส่วนบุคคลของประเทศไทย กล่าวคือ การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะครอบคลุมทั้งข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานราชการ หรือรัฐวิสาหกิจ และหน่วยงานเอกชน ดังนั้น เพื่อศึกษาทำความเข้าใจการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์จึงมีความจำเป็นต้องพิจารณากฎหมายทั้งสองฉบับที่จะเป็นกฎหมายหลักในการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้

5.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการถือเป็นกฎหมายฉบับแรกที่ได้ให้การรับรองสิทธิได้รู้ (right to know) หรือสิทธิที่จะรับรู้ข้อมูลข่าวสารต่างๆ ที่เกี่ยวกับการดำเนินการของรัฐแก่ประชาชนและเป็นหลักประกันให้แก่ประชาชน โดยให้มีโอกาสในการรับรู้ข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐได้อย่างกว้างขวางมากขึ้น พร้อมกับการได้รับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมของรัฐด้วย ดังนั้น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงมีสถานะเสมือนมีสองกฎหมายในฉบับเดียวกัน[4] คือ กฎหมายคุ้มครองสิทธิรับรู้ข้อมูลข่าวสาร (Freedom Information Access law) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection law) ทั้งนี้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีรายละเอียดและสาระสำคัญ ดังต่อไปนี้

---

[3] เพชรรัตน์ จงปัญญาประพันธ์, “ความสำคัญเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล,” จุลนิติ, ฉบับที่ 4, ปีที่ 33, น.823, (ธันวาคม 2546).

[4] *เพิ่งอ้าง*, น.614.

5.1.1 แนวคิดและความเป็นมา

แนวคิดที่จะให้มีกฎหมายรับรองสิทธิของประชาชนในการรับรู้ข้อมูลข่าวสารของราชการนั้นเกิดขึ้นเป็นรูปธรรมในสมัยของรัฐบาล นายอานันท์ ปันยารชุน ดำรงตำแหน่งเป็นนายกรัฐมนตรี (พ.ศ. 2535)[5] ซึ่งได้ให้ความสำคัญกับหลักการในการบริหารงานที่โปร่งใส ดังนั้นรัฐบาลดังกล่าวจึงได้ให้ความเห็นชอบในการจัดตั้งคณะกรรมการเพื่อยกร่างกฎหมายว่าด้วยข้อมูลข่าวสารของราชการขึ้น โดยในระหว่างการศึกษาพิจารณาของคณะกรรมการดังกล่าว นายสุทิน นพเกตุและนายอาจอง ชุมสาย ณ อยุธยา สมาชิกสภาผู้แทนราษฎร พรรคพลังธรรม ได้นำร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. .... ที่ได้มีการจัดทำในสมัยรัฐบาลนายอานันท์ ปันยา-ราชุน ไปเสนอต่อสภาผู้แทนราษฎร ซึ่งรัฐบาลได้ขอรับร่างพระราชบัญญัติดังกล่าวไปพิจารณาก่อนรับหลักการ โดยรัฐบาลได้ส่งให้คณะกรรมการกฤษฎีกาพิจารณาร่างพระราชบัญญัติดังกล่าวอีกทอดหนึ่ง ซึ่งจากการพิจารณาของคณะกรรมการกฤษฎีกานั้น คณะกรรมการกฤษฎีกาได้ยกร่างพระราชบัญญัติขึ้นใหม่เป็นอีกหนึ่งฉบับโดยศึกษาเทียบเคียงจากกฎหมายของต่างประเทศ ได้แก่ ประเทศสหรัฐอเมริกา ฝรั่งเศส แคนาดา ออสเตรเลีย อังกฤษ นิวซีแลนด์ สวีเดน เป็นต้น และเรียกชื่อร่างดังกล่าวว่า ‘ร่างพระราชบัญญัติข่าวสารของราชการ พ.ศ. ....’[6]

ต่อมารัฐบาลในขณะนั้นได้เสนอร่างพระราชบัญญัติดังกล่าวต่อสภาผู้แทนราษฎร พิจารณาและสภาได้พิจารณาร่างพระราชบัญญัติของคณะกรรมการกฤษฎีกาควบคู่ไปกับร่างฉบับของนายสุทิน นพเกตุและนายอาจอง ชุมสาย ณ อยุธยา แล้วจึงมีมติรับหลักการและส่งให้คณะกรรมาธิการสามัญพิจารณา แต่ท้ายที่สุดร่างพระราชบัญญัติดังกล่าวได้ตกไป เนื่องจากการมีการยุบสภาผู้แทนราษฎรเสียก่อน

อย่างไรก็ตาม เมื่อรัฐบาลชุดใหม่เข้ามาบริหารประเทศต่อ (ได้แก่ รัฐบาลของนายบรรหาร ศิลปอาชา) ได้มีการแถลงนโยบายต่อรัฐสภาเมื่อวันที่ 26 กรกฎาคม 2538 ซึ่งมีเนื้อหาที่กล่าวถึงการผลักดันให้มีการตรากฎหมายข้อมูลข่าวสารของราชการในประเทศไทย[7] ดังนั้น ในระหว่างวาระการทำงานของรัฐบาลชุดนี้ จึงจัดให้มีการสัมมนาปรับปรุงร่างกฎหมายนี้หลายครั้ง ส่งผล

---

[5]บุญญรัตน์ โชคบันดาลชัย, กฎหมายสื่อสารมวลชน: การคุ้มครองสิทธิส่วนบุคคลและชื่อเสียงเกียรติคุณ, (พิษณุโลก: สำนักพิมพ์มหาวิทยาลัยนเรศวร, 2558), น.60.

[6] กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางแก้ไข,”(วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), น.309.

[7] *เพิ่งอ้าง*, น.310.

ทำให้แนวคิดและประโยชน์ของกฎหมายข้อมูลข่าวสารแพร่หลายออกไปสู่ประชาชนอย่างกว้างขวาง จนกระทั่งในสมัยของ พลเอกชวลิต ยงใจยุทธ ดำรงตำแหน่งเป็นนายกรัฐมนตรี (พ.ศ.2540) รัฐบาลจึงได้ส่งร่างพระราชบัญญัติข้อมูลข่าวสารของราชการให้สภาผู้แทนราษฎรพิจารณา และสภาได้มีมติรับหลักการและให้ตั้งคณะกรรมาธิการวิสามัญเพื่อพิจารณาร่างพระราชบัญญัติอีกครั้งในวันที่ 25 ธันวาคม 2539 จนกระทั่งต่อมา สภาได้มีมติเห็นชอบร่างพระราชบัญญัติดังกล่าว เมื่อวันที่ 23 กรกฎาคม 2540 และประกาศเป็นกฎหมายในราชกิจจานุเบกษาเมื่อวันที่ 10 กันยายน 2540 โดยกำหนดให้มีผลบังคับใช้เมื่อวันที่ 9 ธันวาคม 2540[8]

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีเจตนารมณ์หรือวัตถุประสงค์ในตราขึ้นเพื่อให้ประชาชนมีโอกาสรับรู้ข้อมูลข่าวสารของราชการมากยิ่งขึ้นและสามารถรักษาผลประโยชน์ของตน รวมทั้งให้ความคุ้มครองสิทธิส่วนบุคคลโดยเฉพาะอย่างยิ่งสิทธิในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการ ดังที่ปรากฏในหมายเหตุท้ายพระราชบัญญัติว่า “ในระบอบประชาธิปไตย การให้ประชาชนมีโอกาสกว้างขวางในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐเป็นสิ่งที่จำเป็น เพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความเป็นจริง อันเป็นการส่งเสริมให้มีความเป็นรัฐบาลโดยประชาชนมากยิ่งขึ้น สมควรกำหนดให้ประชาชนมีสิทธิได้รู้ข้อมูลข่าวสารของราชการ โดยมีข้อยกเว้นอันไม่ต้องเปิดเผยที่แจ้งชัดและจำกัดเฉพาะข้อมูลข่าวสารที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้ เพื่อพัฒนาระบอบประชาธิปไตยให้มั่นคงและจะยังผลให้ประชาชนมีโอกาสรู้ถึงสิทธิหน้าที่ของตนอย่างเต็มที่ เพื่อที่จะปกปักรักษาประโยชน์ของตนได้อีกประการหนึ่งด้วย ประกอบกับสมควรคุ้มครองสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อมกัน จึงจำเป็นต้องตราพระราชบัญญัตินี้” ซึ่งเมื่อพิจารณาพระราชบัญญัติดังกล่าวนับตั้งแต่ประกาศใช้บังคับในราชกิจจานุเบกษาจนกระทั่งถึงปัจจุบันนับเป็นระยะเวลากว่า 20 ปีแล้วที่พระราชบัญญัติดังกล่าวมีผลใช้บังคับโดยไม่ได้รับการปรับปรุงแก้ไขเพิ่มเติมแต่อย่างใด ดังนั้น ผู้ที่เกี่ยวข้องหลายฝ่ายจึงมีความพยายามในการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยกำหนดให้กฎหมายข้อมูลข่าวสารของราชการเป็นกฎหมายฉบับหนึ่งที่อยู่ในแผนนิติบัญญัติของรัฐบาลซึ่งจะต้องดำเนินการในช่วงปี พ.ศ. 2552 – 2554 โดยร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ (ฉบับที่ ..) พ.ศ. .. ได้ผ่านกระบวนการเสนอกฎหมายสู่การพิจารณาของรัฐสภาเมื่อวันที่ 18 ธันวาคม 2550 แต่ไม่สามารถเสนอผ่านสภานิติบัญญัติได้ เนื่องจากมีการเปลี่ยนแปลงรัฐบาลใหม่

---

[8] ศูนย์ข้อมูลข่าวสาร สป.ทส., “คู่มือการปฏิบัติงานตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ,” สืบค้นเมื่อวันที่ 5 มีนาคม 2560, จาก http://slc.mnre.go.th

ซึ่งในระหว่างนี้คณะกรรมการข้อมูลข่าวสารของราชการได้ประชุมพิจารณาเรื่องนี้หลายครั้ง โดยในวันที่ 1 พฤษภาคม 2552 คณะกรรมการข้อมูลข่าวสารของราชการได้จัดให้มีการประชุมประจำครั้งที่ 3/2552 โดยมีวาระการประชุม คือการพิจารณาร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ (ฉบับที่ ..) พ.ศ. .. ซึ่งในขณะนั้นคณะกรรมการข้อมูลข่าวสารของราชการมีร่างที่อยู่ในการพิจารณาด้วยกันทั้งสิ้น 2 ฉบับ ดังนี้

(1) ร่างฉบับที่ผ่านการพิจารณาของคณะกรรมการกฤษฎีกาและสภานิติบัญญัติแห่งชาติ แต่คณะรัฐมนตรีในขณะนั้นยังไม่ยืนยันร่างเนื่องจากเป็นช่วงปลายของรัฐบาลก่อน จึงทำให้ระยะเวลาไม่เพียงพอที่จะพิจารณาให้ทัน
(2) ร่างฉบับที่นายเธียรชัย ณ นครเป็นผู้ยกร่างซึ่งยังไม่ผ่านการพิจารณาของคณะกรรมการข้อมูลข่าวสารของทางราชการ

เพื่อเป็นการผลักดันร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. .... ฉบับใดฉบับหนึ่งที่ประชุมจึงจำเป็นต้องหารือว่าร่างพระราชบัญญัติฉบับใดจะถูกเลือกให้เป็นร่างหลักสำหรับการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อย่างไรก็ตาม เนื่องจากที่ประชุมไม่สามารถมีมติในประเด็นดังกล่าวได้ ณ ขณะนั้นจึงได้มีการแต่งตั้งคณะอนุกรรมการร่วมพิจารณาร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ (ฉบับที่ ..) พ.ศ. .. แต่ภายหลังคณะอนุกรรมการร่วมดังกล่าวได้ยุติหน้าที่ลง จนกระทั่งการประชุมคณะรัฐมนตรีในการพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ได้ตั้งข้อสังเกตว่ากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลน่าจะมีบางส่วนที่เกี่ยวเนื่องกับกฎหมายข้อมูลข่าวสารของราชการด้วย ประกอบกับกฎหมายข้อมูลข่าวสารของราชการยังไม่เป็นไปตามหลักสากลตามที่มีผู้ร้องเรียนมา จึงทำให้คณะกรรมการข้อมูลข่าวสารของทางราชการริเริ่มการพิจารณาร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ (ฉบับที่ ..) พ.ศ. .. อีกครั้ง

อย่างไรก็ตาม จากผลการพิจารณาร่างพระราชบัญญัติฯ ดังกล่าวอีกครั้ง ที่ประชุมเห็นว่าการแก้ไขกฎหมายยังมิใช่เรื่องเร่งด่วนเนื่องจากกฎหมายปัจจุบันสอดคล้องกับหลักสากลดีอยู่แล้ว แต่เสนอให้ตรากฎกระทรวง กำหนดให้หน่วยงานอิสระอยู่ภายใต้บังคับของ มาตรา 4 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ทั้งนี้ กรณีก็ยังคงไม่มีความคืบหน้าในประเด็นดังกล่าวเช่นเดิม แม้ว่าในการประชุมคณะรัฐมนตรีเมื่อวันที่ 4 มกราคม 2554 นายกรัฐมนตรีในขณะนั้นได้มอบหมายให้รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นายสาทิตย์ วงส์หนองเตย) และประธานกรรมการข้อมูลข่าวสารของราชการ (นายองอาจ คล้ามไพบูลย์) พิจารณาทบทวนปัญหาและ

อุปสรรคในการดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ว่าควรมีการปรับปรุงแก้ไขหรือไม่อย่างไร ซึ่งคณะกรรมการข้อมูลข่าวสารของราชการได้แต่งตั้งคณะอนุกรรมการเพื่อพิจารณาทบทวนปัญหาและอุปสรรค แต่ก็ยังมิได้มีข้อยุติที่ชัดเจนเช่นเดิม

ดังนั้น ต่อมาคณะกรรมการข้อมูลข่าวสารของราชการจึงได้พิจารณาให้แต่งตั้งคณะอนุกรรมการใหม่อีก 2 คณะ ซึ่งมีนายเธียรชัย ณ นคร เป็นประธานอนุกรรมการแก้ไขปัญหาและอุปสรรคในการดำเนินการตามพระราชบัญญัติและผู้ช่วยศาสตราจารย์ กิตติศักดิ์ ปรกติ เป็นประธานอนุกรรมการพิจารณาปรับปรุงพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่เนื่องจากมีการเปลี่ยนแปลงรัฐบาลในช่วงเวลาดังกล่าว คณะอนุกรรมการฯ ทั้งสองคณะจึงไม่ได้มีการประชุมแต่ประการใด และต่อมาในวันที่ 19 ตุลาคม 2554 คณะกรรมการข้อมูลข่าวสารจึงได้ประชุมหารืออีกครั้งและจึงมีมติให้เสนอร่างพระราชบัญญัติข้อมูลข่าวสารของราชการ (ฉบับที่...) พ.ศ. ... เพื่อเป็นส่วนหนึ่งของแผนนิติบัญญัติแห่งชาติต่อไป

อย่างไรก็ตาม นับเป็นระยะเวลากว่า 6 ปีแล้ว นับตั้งแต่การประชุมหารือของคณะกรรมการข้อมูลข่าวสาร แต่กรณีก็ยังไม่มีความคืบหน้าในการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่อย่างใด ดังนั้น พระราชบัญญัติฉบับปัจจุบันจึงยังคงมีผลใช้บังคับในฐานะกฎหมายกลางที่ให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐต่อไป

5.1.2 ขอบเขตการใช้บังคับ

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มิได้กำหนดขอบเขตการใช้บังคับไว้โดยชัดแจ้ง แต่จากบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 สามารถพิจารณาได้ว่าพระราชบัญญัติฉบับนี้ใช้บังคับกับประเภทของข้อมูลดังต่อไปนี้

(1) ข้อมูลข่าวสารทั่วไป ซึ่งหมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

(2) ข้อมูลข่าวสารของราชการ ซึ่งหมายถึง ข้อมูลข่าวสารที่อยู่ในความครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน

(3) ข้อมูลข่าวสารส่วนบุคคล ซึ่งหมายถึง ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์

นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่ายและให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมด้วย

อย่างไรก็ตาม ข้อมูลทั้ง 3 ประเภทข้างต้น จะได้รับความคุ้มครองตามพระราชบัญญัติฉบับนี้ก็ต่อเมื่อข้อมูลดังกล่าวอยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น ไม่รวมถึงข้อมูลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชนแต่อย่างใด

5.1.3 การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้น จะถูกบัญญัติไว้ในหมวด 3 ว่าด้วย“ข้อมูลข่าวสารส่วนบุคคล” เป็นจำนวนทั้งสิ้น 5 มาตรา ตั้งแต่มาตรา 21 ถึงมาตรา 25 ซึ่งมีรายละเอียดและสาระสำคัญ ดังต่อไปนี้

5.1.3.1 การกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลข่าวสารส่วนบุคคล (Identifying Purpose)

โดยหลักเมื่อหน่วยงานของรัฐจะจัดเก็บข้อมูลข่าวสารส่วนบุคคลของเอกชนนั้น หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกันกับการขอข้อมูลเพื่อมาจัดเก็บถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้และลักษณะการใช้ นอกจากนี้ หน่วยงานของรัฐมีหน้าที่จะต้องชี้แจงให้เจ้าของข้อมูลทราบด้วยเช่นกันว่า การให้ข้อมูลของเจ้าของข้อมูลเป็นการให้ข้อมูลโดยสมัครใจหรือเป็นกรณีที่มีกฎหมายบังคับให้ต้องให้ข้อมูลแก่หน่วยงานของรัฐ ทั้งนี้ ตามมาตรา 23 วรรคสอง แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

5.1.3.2 ความยินยอมของเจ้าของข้อมูล (Consent)

ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้น การจัดเก็บ การนำไปใช้และการนำไปเปิดเผยจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน ยกเว้นแต่กรณีที่มีกฎหมายกำหนดให้การจัดเก็บ การนำไปใช้หรือการนำไปเปิดเผยไม่จำต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน ทั้งนี้เป็นไปตามมาตรา 24 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

5.1.3.3 การจัดเก็บข้อมูลส่วนบุคคลให้กระทำได้เฉพาะเท่าที่จำเป็น (Limiting of collection)

โดยหลักการจัดเก็บข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติฉบับนี้นั้นให้จัดเก็บได้เฉพาะเท่าที่จำเป็นตามหน้าที่ขององค์กรหรือหน่วยงานของรัฐนั้นๆ ดังนั้น ในการดำเนินการจัดเก็บข้อมูลส่วนบุคคลของบุคคลหนึ่งบุคคลใดหรือเรื่องหนึ่งเรื่องใด จึงต้องพิจารณาก่อนว่าข้อมูล

ส่วนบุคคลนั้นมีความจำเป็นที่จะต้องจัดเก็บหรือไม่ ทั้งนี้ เพื่อให้การดำเนินการของหน่วยงานนั้นสามารถบรรลุผลได้ ตามมาตรา 23 วรรคแรก (1) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

5.1.3.4 การเก็บรักษาข้อมูลและการนำข้อมูลส่วนบุคคลไปใช้หรือไปเปิดเผยเท่าที่จำเป็น (Limiting use, Limiting disclosure and Limiting retention)

ดังที่ได้กล่าว ณ ข้างต้นว่าการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยนั้น หน่วยงานหรือองค์กรของรัฐจะกระทำได้เฉพาะตามขอบเขตวัตถุประสงค์และตามที่ได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้น โดยจะต้องมีการประกาศในราชกิจจานุเบกษาด้วยว่าข้อมูลส่วนบุคคลที่จัดเก็บไว้นั้นจะนำไปใช้ตามปกติในกรณีหรือเรื่องใด ทั้งนี้ แม้ว่าข้อมูลส่วนบุคคลดังกล่าวจะถูกนำไปใช้หรือเปิดเผยแล้ว หน่วยงานหรือองค์กรนั้นก็ยังคงมีหน้าที่ต้องเก็บรักษาไว้ในเวลาเท่าที่จำเป็นเท่านั้น เช่น เฉพาะระยะเวลาเท่าที่จำเป็นเพื่อให้เจ้าของข้อมูลมีโอกาสตรวจสอบ เป็นต้น ตามมาตรา 23 วรรคแรก แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ดังนั้น เมื่อหมดความจำเป็นแล้วองค์กรหรือหน่วยงานของรัฐจะต้องยกเลิกการจัดเก็บข้อมูลส่วนบุคคลนั้นทันที

5.1.3.5 ความถูกต้องครบถ้วนของข้อมูลข่าวสารส่วนบุคคล (Accuracy)

โดยหลักแล้วองค์กรหรือหน่วยงานที่จัดเก็บข้อมูลส่วนบุคคลนั้นจะต้องควบคุมดูแลให้ข้อมูลส่วนบุคคลนั้นมีความถูกต้องและเป็นปัจจุบัน ทั้งนี้ เพื่อให้การนำไปใช้หรือไปเปิดเผยตามอำนาจหน้าที่ หรือตามวัตถุประสงค์ไม่ก่อให้เกิดผลกระทบหรือความเสียหายต่อเจ้าของข้อมูล วิธีการหนึ่งในการจัดเก็บข้อมูลให้มีความถูกต้องคือการเก็บข้อมูลโดยตรงจากเจ้าของข้อมูลและตรวจสอบแก้ไขข้อมูลส่วนบุคคลที่จัดเก็บนั้นให้ถูกต้องอยู่เสมอ

5.1.3.6 มีระบบรักษาความปลอดภัย (Safeguards) ให้กับระบบข้อมูลส่วนบุคคล

หน่วยงานต่างๆ ที่มีการจัดเก็บข้อมูลส่วนบุคคลจะต้องมีระบบการควบคุมดูแลการเก็บรักษาหรือการนำข้อมูลส่วนบุคคลไปใช้ตามวัตถุประสงค์ของการจัดเก็บหรือนำไปใช้ตามขอบวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมไว้แล้ว ทั้งนี้ หน่วยงานดังกล่าวจะต้องมีมาตรการป้องกันหรือมาตรการในการรักษาความปลอดภัยในกรณีที่ข้อมูลดังกล่าวถูกนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูลด้วย โดยพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้กำหนดไว้ในมาตรา 23 วรรคแรก (5) และมาตรา 24 วรรคสอง ให้หน่วยงานราชการต่างๆ ต้องถือปฏิบัติ

5.1.3.7 มีระบบบริหารจัดการข้อมูลส่วนบุคคลที่โปร่งใส (Openness)

หลักการมีระบบบริหารจัดการข้อมูลส่วนบุคคลที่โปร่งใส ได้แก่ กรณีที่ทุกหน่วยงานจะต้องมีระบบบริหารจัดการข้อมูลส่วนบุคคลที่โปร่งใสและสามารถตรวจสอบได้ เพื่อที่เจ้าของข้อมูลหรือประชาชนทั่วไปสามารถรู้นโยบายหรือวิธีปฏิบัติในการจัดเก็บข้อมูลส่วนบุคคลของหน่วยงานของรัฐได้ ตามมาตรา 23 วรรคแรก (3) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

5.1.3.8 การให้สิทธิเข้าถึงข้อมูลส่วนบุคคลของตนเอง (Individual Access)

การให้สิทธิเจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตนเองถูกกำหนดไว้มาตรา 25 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยเจ้าของข้อมูลหรือผู้กระทำแทนบุคคลนั้นมีสิทธิขอตรวจดูหรือขอรับสำเนาข้อมูลส่วนบุคคลของตนได้ รวมทั้งยังมีสิทธิขอให้หน่วยงานของรัฐแก้ไขเปลี่ยนแปลงหรือลบข้อมูลส่วนบุคคลของตนที่ไม่ถูกต้องตามความเป็นจริงได้

5.1.3.9 การให้สิทธิร้องเรียนกรณีหน่วยงานปฏิบัติฝ่าฝืนกฎหมาย (Challenging Compliance)

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามบทบัญญัติแห่งกฎหมาย มาตรา 23 และมาตรา 25 วรรค 4 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงให้สิทธิแก่เจ้าของข้อมูลในการร้องเรียนหน่วยงานของรัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลของตนโดยไม่ปฏิบัติตามกฎหมายได้

5.1.3.10 หลักความรับผิดชอบของหน่วยงานในการปฏิบัติตามบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Accountability)

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้รองรับหลักการนี้โดยการกำหนดให้ทุกหน่วยงานของรัฐที่จัดเก็บข้อมูลส่วนบุคคลจะต้องกำหนดผู้รับผิดชอบอย่างชัดเจนในการดำเนินการบริหารจัดการระบบข้อมูลข่าวสารส่วนบุคคลขององค์กร เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลตามหลักการข้างต้นประสบผลสำเร็จ

5.2 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เป็นกฎหมายที่มีการยกร่างขึ้นมาช้านานแต่ยังไม่มีผลใช้บังคับเป็นกฎหมาย ทั้งนี้ ผู้ร่างและผู้ที่เกี่ยวข้องมุ่งหวังให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีสถานะเป็นกฎหมายกลางสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่

อยู่ในความครอบครองของหน่วยงานเอกชน ควบคู่ไปกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีข้อจำกัดในการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีสาระสำคัญ ดังนี้

5.2.1 แนวคิดและความเป็นมา

ประเทศไทยมีแนวคิดที่จะออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลมาตั้งแต่ปี พ.ศ. 2540 โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งในกลุ่มกฎหมายที่มีวัตถุประสงค์เพื่อรองรับการเติบโตด้านเทคโนโลยีสารสนเทศซึ่งเป็นนโยบายของรัฐบาลมานับตั้งแต่ปี พ.ศ. 2540 ทั้งนี้ เดิมศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center: NECTEC) ถือเป็นหน่วยงานที่เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นรายแรก ตั้งแต่ปี พ.ศ. 2540 โดยมีการจัดสัมมนา อภิปราย รับฟังความคิดเห็นและมีการแก้ไขร่างกฎหมายฉบับนี้อีกหลายครั้ง จนกระทั่งเดือน พฤศจิกายน 2552 ร่างพระราชบัญญัติดังกล่าวจึงได้ผ่านการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกาและคณะรัฐมนตรีสมัยนายอภิสิทธิ์ เวชชาชีวะ ดำรงตำแหน่งเป็นนายกรัฐมนตรี จึงได้ให้ความเห็นชอบและบรรจุเป็นระเบียบวาระในการพิจารณาของสภาผู้แทนราษฎรเมื่อวันที่ 17 พฤศจิกายน 2552 อย่างไรก็ตาม ร่างพระราชบัญญัติฉบับนี้ยังไม่ได้รับการพิจารณาในสภาผู้แทนราษฎรสมัยนั้น เนื่องจากได้มีการยุบสภาผู้แทนราษฎรเสียก่อน

นับว่าเป็นระยะเวลาที่ล่วงเลยมากว่า 12 ปี นับตั้งแต่พระราชบัญญัติฉบับข้างต้นถูกยกร่างขึ้น และบุคคลทุกภาคส่วนของประเทศไทยเริ่มให้ความสนใจและให้ความสำคัญกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยในระหว่างระยะเวลาดังกล่าว มีผู้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมเช่นกัน ดังนั้น ปัจจุบันประเทศไทยจึงมีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่รอการพิจารณาในกระบวนต่างๆ ที่แตกต่างกันไป รวมทั้งสิ้น 4 ฉบับ ดังนี้

5.2.1.1 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่ยกร่างโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ และเสนอโดยคณะรัฐมนตรีสมัยนางสาว ยิ่งลักษณ์ ชินวัตร ดำรงตำแหน่งเป็นนายกรัฐมนตรี

ในสมัยรัฐบาล นางสาวยิ่งลักษณ์ ชินวัตร ดำรงตำแหน่งเป็นนายกรัฐมนตรี ร่างพระราชบัญญัติฉบับที่ยกร่างโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในรัฐบาลของนายอภิสิทธิ์ เวชชาชีวะ ได้ถูกนำมาพิจารณาใหม่อีกครั้งเมื่อมีการเปิดประชุมสภาผู้แทนราษฎร อย่างไรก็ตาม เนื่องจากร่างพระราชบัญญัติดังกล่าวไม่ได้รับการหยิบยกขึ้นมาพิจารณาในฐานะที่เป็นร่างกฎหมายที่ค้างการพิจารณาจากสภาผู้แทนราษฎรในสมัยที่แล้ว ดังนั้น การ

พิจารณาร่างพระราชบัญญัติฉบับดังกล่าวจึงต้องเริ่มกระบวนการเสนอร่างพระราชบัญญัติใหม่ทั้งหมด โดยผู้ทำหน้าที่เสนอร่างพระราชบัญญัติฉบับนี้ คือ สำนักงานปลัดสำนักนายกรัฐมนตรี ซึ่งต่อมาคณะรัฐมนตรีในสมัยนั้น ได้มีมติเมื่อวันที่ 28 สิงหาคม 2555 เห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว ตามที่สำนักงานปลัดสำนักนายกรัฐมนตรีเสนอและให้ส่งคณะกรรมการประสานงานสภาผู้แทนราษฎรพิจารณา ก่อนนำเสนอสภาผู้แทนราษฎรพิจารณาต่อไป

กระทั่งในวันที่ 27 กุมภาพันธ์ 2556 คณะรัฐมนตรีในสมัยนั้น ได้ประชุมปรึกษาหารือและลงมติรับทราบสรุปผลการประชุมของคณะกรรมการประสานงานสภาผู้แทนราษฎรที่ได้จัดขึ้น ณ วันที่ 26 กุมภาพันธ์ 2556 โดยที่ประชุมของคณะกรรมการประสานงานสภาผู้แทนราษฎรได้มีมติให้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ต่อสภาผู้แทนราษฎรเพื่อบรรจุเป็นระเบียบวาระเรื่องด่วน

ดังนั้น ในระยะเวลาต่อ เมื่อวันที่ 27 กุมภาพันธ์ 2556 คณะรัฐมนตรีในสมัยนั้น จึงได้เสนอร่างพระราชบัญญัติฉบับดังกล่าวต่อประธานสภาผู้แทนราษฎรเพื่อให้สภาผู้แทนราษฎรพิจารณาตามบทบัญญัติรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 และได้บรรจุระเบียบวาระการประชุมสภาผู้แทนราษฎรในคราวประชุมสภาผู้แทนราษฎรชุดที่ 24 ปีที่ 2 ครั้งที่ 25 (สมัยสามัญนิติบัญญัติ) เมื่อวันที่ 27 มีนาคม 2556 ทั้งนี้ สภาผู้แทนราษฎรมีมติรับหลักการของร่างพระราชบัญญัติดังกล่าวในเดือนตุลาคม 2556 อย่างไรก็ตาม การพิจารณาร่างพระราชบัญญัติฉบับนั้นก็ยังคงไม่แล้วเสร็จ กล่าวคือ ยังไม่มีการพิจารณาเพื่อให้ความเห็นชอบต่อร่างพระราชบัญญัตินั้นแต่อย่างใด เนื่องจากมีการยุบสภาผู้แทนราษฎรอีกครั้ง

ต่อมาในสมัยที่พลเอกประยุทธ์ จันทร์โอชาดำรงตำแหน่งเป็นนายกรัฐมนตรี สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ (สขร.) จึงได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่ผ่านการพิจารณาจากคณะกรรมการกฤษฎีกา (เรื่องแล้วเสร็จที่ 515/2552) แก่สภานิติบัญญัติแห่งชาติอีกครั้ง เมื่อวันที่ 7 ตุลาคม 2557 ตามมติเห็นชอบของคณะกรรมการข้อมูลข่าวสารของราชการ เพราะร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลถือเป็นกฎหมายที่ต้องจัดให้มีขึ้นใหม่เพื่อให้การดำเนินงานตามแผนการบริหารราชการแผ่นดิน พ.ศ. 2555 – 2558 ประสบความสำเร็จ โดยร่างฉบับนี้ได้ถูกบรรจุเข้าไปในระเบียบวาระของสภานิติบัญญัติแห่งชาติ (สนช.) เป็นที่เรียบร้อยแล้ว แต่อย่างไรก็ตาม เมื่อวันที่ 8 กันยายน 2558 คณะรัฐมนตรีชุดที่มีพลเอก ประยุทธ์ จันทร์โอชา ดำรงตำแหน่งเป็นนายกรัฐมนตรี ได้มีมติให้ถอนร่างดังกล่าวออกจากการพิจารณาของสภานิติบัญญัติแห่งชาติแล้วเป็นที่เรียบร้อย ดังนั้น ร่างฉบับนี้จึงตกไป

5.2.1.2 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่เสนอโดยนายอภิชาต ศักดิเศรษฐ์ สมาชิกสภาผู้แทนราษฎร พรรคประชาธิปัตย์และคณะ

นายอภิชาต ศักดิเศรษฐ์เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ต่อประธานสภาผู้แทนราษฎรครั้งแรกเมื่อวันที่ 8 กันยายน 2552[9] และครั้งที่สองเมื่อวันที่ 15 กันยายน 2554 โดยร่างฉบับนี้ได้บรรจุไว้ในระเบียบวาระการประชุมสภาผู้แทนราษฎร ชุดที่ 24 ปีที่ 2 ครั้งที่ 25 (สมัยสามัญนิติบัญญัติ) เมื่อวันที่ 27 มีนาคม 2556 ซึ่งในปัจจุบันร่างพระราชบัญญัติฉบับนี้ก็ยังคงค้างการพิจารณาอยู่

5.2.1.3 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่เสนอโดยนายศุภชัย ใจสมุทร สมาชิกสภาผู้แทนราษฎร พรรคภูมิใจไทยและคณะ

นายศุภชัย ใจสมุทร สมาชิกสภาผู้แทนราษฎร พรรคภูมิใจไทยและคณะได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ต่อประธานสภาผู้แทนราษฎรเมื่อวันที่ 12 มีนาคม 2556 และร่างฉบับนี้ได้บรรจุในระเบียบวาระการประชุมสภาผู้แทนราษฎร ชุดที่ 24 ปีที่ 2 ครั้งที่ 27 (สมัยสามัญนิติบัญญัติ) เมื่อวันที่ 18 เมษายน 2556 อย่างไรก็ตาม ปัจจุบันร่างดังกล่าวก็ยังค้างการพิจารณาอยู่[10]

5.2.1.4 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับที่เสนอโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ฉบับความมั่นคงดิจิทัล (เดิม) /ฉบับคณะรัฐมนตรีอนุมัติหลักการ (ใหม่)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับความมั่นคงดิจิทัล (เดิม) เป็นหนึ่งในกฎหมายของชุดร่างกฎหมายดิจิทัลซึ่งประกอบไปด้วย ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ร่างพระราชบัญญัติคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. .... ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เป็นต้น ทั้งนี้กฎหมายในชุดกฎหมายความมั่นคงดิจิทัลถูกยกร่างขึ้นเพื่อรองรับการพัฒนาของเศรษฐกิจในยุคดิจิทัลโดยคณะรัฐมนตรีชุดที่พลเอก ประยุทธ์ จันทร์โอชา ดำรงตำแหน่งเป็นนายกรัฐมนตรีได้มีมติเห็นชอบ

---

[9]จุฬารัตน์ ยะปะนัน, “ร่างกฎหมายที่น่าสนใจ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....,” จุลนิติ, ฉบับที่ 3, ปีที่ 7, น.75, (พฤษภาคม – มิถุนายน 2553).

[10]ลันตา อุตมะโภคิน, “ร่างกฎหมายที่น่าสนใจ: ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....,” จุลนิติ, ฉบับที่ 3, ปีที่ 11, น.75, (พฤษภาคม – มิถุนายน 2557).

ในหลักการของร่างกฎหมายดังกล่าวเมื่อวันที่ 6 มกราคม 2558 ส่งผลให้ร่างกฎหมายฉบับดังกล่าวเข้าสู่กระบวนการตรวจพิจารณาของคณะกรรมการกฤษฎีกาในวันที่ 9 กุมภาพันธ์ 2558 โดยคณะกรรมการกฤษฎีกาได้ตรวจแก้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้วเสร็จในช่วงเดือนกรกฎาคม 2558 ดังนั้น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้นำเสนอร่างพระราชบัญญัติฉบับที่คณะกรรมการกฤษฎีกาตรวจแก้แล้วให้คณะรัฐมนตรีพิจารณาต่อไป

อย่างไรก็ตาม เมื่อวันที่ 8 กันยายน 2558 คณะรัฐมนตรีได้มีมติให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กลับไปทบทวนร่วมกับคณะกรรมการกฤษฎีกาอีกครั้งหนึ่ง ซึ่งคณะกรรมการกฤษฎีกาได้พิจารณาแล้วเสร็จและส่งกลับให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเมื่อช่วงปี 2559 ที่ผ่านมา และต่อมากระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงดำเนินการพิจารณาความเหมาะสมของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... โดยเปรียบเทียบกับกฎหมายต่างประเทศและบริบทของสังคมในปัจจุบัน ตลอดจนเปิดการรับฟังความคิดเห็นเกี่ยวกับร่างพระราชบัญญัติฉบับนี้ในระหว่างวันที่ 22 มกราคม 2561 ถึงวันที่ 2 กุมภาพันธ์ 2561 ผ่านทางเว็บไซต์ www.lawamendment.go.th ทั้งนี้คณะรัฐมนตรีได้มีมติเห็นชอบในหลักการของร่างพระราชบัญญัติคุ้มครองข้อมูลดังกล่าวเมื่อวันที่ 22 พฤษภาคม 2561 ที่ผ่านมาและจะนำเข้าสู่การพิจารณาของคณะกรรมการกฤษฎีกาและและพิจารณาสภานิติบัญญัติแห่งชาติตามลำดับ ซึ่งในเบื้องต้นคาดการณ์ว่าร่างพระราชบัญญัติฉบับนี้จะถูกเสนอให้สภานิติบัญญัติแห่งชาติพิจารณาภายในเดือนตุลาคม 2561 และหากสภานิติบัญญัติแห่งชาติเห็นชอบประเทศไทยก็จะมีกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่สามารถใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานเอกชนได้

เนื่องจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่คณะรัฐมนตรีมีมติรับหลักการเมื่อวันที่ 22 พฤษภาคม 2561 หรือ “ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)” เป็นร่างพระราชบัญญัติที่มีแนวโน้มจะได้รับการพิจารณาและประกาศใช้เป็นกฎหมายมากที่สุด ดังนั้น ในการศึกษาสาระสำคัญของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ผู้เขียนขอนำร่างพระราชบัญญัติฉบับดังกล่าวมาเป็นแนวทางในการศึกษาในประเด็นอื่นๆ ดังนี้

5.2.2 เจตนารมณ์ของกฎหมาย

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ยกร่างขึ้นโดยมีหลักการและเหตุผล คือ เนื่องจากปัจจุบันมีการล่วงละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของ

ข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยี ทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวสามารถทำได้โดยง่าย สะดวกและรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไกหรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น

5.2.3 ขอบเขตการใช้บังคับ

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ใช้บังคับกับกรณีนี้ดังต่อไปนี้

(1) การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรโดยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าบุคคลดังกล่าวจะอยู่ในหรือนอกราชอาณาจักร

(2) การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่กระทำนอกราชอาณาจักรที่แม้แต่ส่วนหนึ่งส่วนใดของการกระทำได้กระทำในราชอาณาจักร หรือกระทำนอกราชอาณาจักรที่ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักรหรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นนั้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักร ให้ถือว่าการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้กระทำในราชอาณาจักร

(3) การคุ้มครองข้อมูลส่วนบุคคลที่หากมีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใดหรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายนั้น เว้นแต่กรณีดังต่อไปนี้ แม้กฎหมายนั้นๆ จะบัญญัติไว้ ก็ให้บังคับตามพระราชบัญญัติฉบับนี้[11] หากบทบัญญัตินั้นเป็นบทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลและบทกำหนดโทษที่เกี่ยวข้อง แต่กรณีที่เป็นบทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจคณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้ใช้พระราชบัญญัตินี้แทนในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจ

---

[11] มาตรา 3 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

พิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อเจ้าของข้อมูลส่วนบุคคลแต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

นอกจากนี้ พระราชบัญญัตินี้จะไม่ใช้บังคับกับกรณีดังต่อไปนี้

(1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลต่อผู้อื่น

(2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภาหรือคณะกรรมาธิการ แล้วแต่กรณี

(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(5) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากนี้ กฎหมายฉบับนี้ยังเปิดช่องให้ไม่ต้องนำไปใช้บังคับกับกรณีอื่นๆ นอกเหนือจากกรณีข้างต้นได้ แต่ต้องจะต้องมีการตราเป็นพระราชกฤษฎีกามายกเว้นก่อนเสมอ จากขอบเขตการบังคับใช้ข้างต้น จะเห็นได้ว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้จะใช้บังคับกับเฉพาะข้อมูลส่วนบุคคลเท่านั้น และไม่ใช้บังคับกับข้อมูลอื่นใดที่ไม่เข้าลักษณะเป็นข้อมูลส่วนบุคคลตลอดจนข้อมูลที่เป็นความลับทางการค้า (ซึ่งไม่อยู่ในขอบเขตของการศึกษาครั้งนี้เช่นกัน) ดังนั้น ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจึงมีขอบเขตที่แคบกว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งจะบังคับใช้กับข้อมูลข่าวสารทุกประเภทที่อยู่ในความครอบครองของหน่วยงานของรัฐ

5.2.4 บทนิยามที่สำคัญ

ภายใต้มาตรา 6 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ปรากฏบทนิยามที่สำคัญที่จำเป็นต่อการพิจารณาร่างพระราชบัญญัติฉบับนี้ ดังต่อไปนี้

5.2.4.1 ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

5.2.4.2 ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

5.2.4.3 ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

5.2.4.4 เจ้าของข้อมูล

เจ้าของข้อมูล ให้หมายความรวมถึง

(1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ

(3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

5.2.5 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วย

ประธานกรรมการ ซึ่งคณะรัฐมนตรีจะแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้าน

เทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

<u>รองประธานกรรมการ</u> ซึ่งได้แก่ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

<u>กรรมการโดยตำแหน่ง</u> จำนวน 8 ท่าน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา อัยการสูงสุด เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้แทนสภาหอการค้าแห่งประเทศไทย ผู้แทนสภาอุตสาหกรรมแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

<u>กรรมการผู้ทรงคุณวุฒิ</u> จำนวน 5 ท่าน โดยคณะรัฐมนตรีจะแต่งตั้งกรรมการผู้ทรงคุณวุฒิจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านสังคมศาสตร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล อนึ่ง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะดำรงตำแหน่งคราวละ 3 ปี แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะมีความสำคัญในดำเนินการตามที่กำหนดไว้ในมาตรา 14 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ดังต่อไปนี้

ก. การจัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องตามนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว

ข. ส่งเสริมและสนับสนุนหน่วยงานของรัฐ ภาคเอกชนและภาคประชาชนในการดำเนินกิจกรรมตามแผนยุทธศาสตร์ข้างต้น รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามนโยบายและแผนยุทธศาสตร์ดังกล่าว เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

ค. กำหนดมาตรการ หรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

ง. ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

จ. ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลเพื่อที่ส่งหรือโอนไปยังต่างประเทศ

ฉ. ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ

ช. พิจารณากำหนดค่าปรับทางปกครองตามมาตรา 69 มาตรา 70 มาตรา 71 มาตรา 72 มาตรา 73 มาตรา 74 และมาตรา 75 รวมทั้งฟ้องคดีต่อศาลปกครอง ทั้งนี้ ในกรณีที่มีการบังคับทางปกครองเพื่อชำระค่าปรับทางปกครอง ให้คณะกรรมการเป็นผู้มีอำนาจออกคำสั่งยึด อายัด หรือขายตลอดตลาดทรัพย์สินในการบังคับทางปกครองและให้ประธานกรรมการเป็นผู้ลงนามแทนในคำสั่งดังกล่าว

ซ. เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ฌ. เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้

ญ. ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานทั้งภาครัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

ฎ. ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัตินี้

ฏ. ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

ฐ. ส่งเสริมและสนับสนุนการวิจัยเพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

5.2.6 การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ประกอบด้วยการดำเนินการ 2 ประเภท กล่าวคือ

5.2.6.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

ภายใต้มาตรา 21 แห่งร่างพระราชบัญญัติฉบับนี้ การเก็บรวบรวมข้อมูลส่วนบุคคลจะกระทำไม่ได้หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กรณีดังต่อไปนี้

ก. เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

ข. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

ค. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูล

ง. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนนเข้าทำสัญญานั้น

จ. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

ฉ. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

ช. เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

ซ. กรณีอื่นตามที่กำหนดไว้ในกฎกระทรวง

ดังนั้น จะเห็นได้ว่า ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) นั้น โดยหลัก การเก็บรวบรวมข้อมูลส่วนบุคคลย่อมไม่สามารถกระทำได้ ยกเว้นจะได้รับความยินยอมจากเจ้าของข้อมูลที่ให้ไว้ก่อนหรือในขณะที่จัดเก็บข้อมูลส่วนบุคคลหรือมีกรณีที่กฎหมายกำหนดให้สามารถกระทำได้เท่านั้น ทั้งนี้ ความยินยอมจะต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ และความยินยอมนี้เจ้าของข้อมูลมีสิทธิถอนความยินยอมเมื่อใดก็ได้ ยกเว้นจะมีข้อจำกัดสิทธิในการถอนความยินยอม

นอกจากนี้ โดยหลักการจัดเก็บข้อมูลส่วนบุคคลจะต้องจัดเก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรงด้วย การเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นย่อมไม่สามารถดำเนินการได้ ยกเว้นแต่กรณีที่กฎหมายกำหนด อาทิ ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้าแล้ว หรือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และการเปิดเผยที่ได้รับการยกเว้น หรือเป็นการเก็บรวบรวมข้อมูลที่เปิดเผยต่อสาธารณะ[12] เป็นต้น นอกเหนือจากข้อยกเว้นข้างต้นแล้ว ผู้ควบคุมข้อมูลซึ่งเป็นผู้เก็บข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดที่กำหนดต่อไปนี้ แต่หากไม่อาจดำเนินการได้ ผู้ควบคุมข้อมูลจะต้องแจ้งรายละเอียดดังกล่าวให้แก่เจ้าของข้อมูลทราบทันทีโดยไม่ชักช้า[13]

- วัตถุประสงค์ของการเก็บรวบรวม

---

[12] มาตรา 22 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[13] มาตรา 20 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

- ข้อมูลที่จะมีการเก็บรวบรวม
- ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล สถานที่ติดต่อและวิธีการติดต่อ
- สิทธิของเจ้าของข้อมูล

อนึ่ง ผู้ควบคุมข้อมูลไม่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพหรือข้อมูลอื่นใดที่กระทบความรู้สึกของผู้อื่นหรือของประชาชนโดยปราศจากความยินยอมจากเจ้าของข้อมูลดังกล่าวได้ ยกเว้น เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล หรือเป็นการปฏิบัติตามกฎหมาย[14]

5.2.6.2 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) นั้นการใช้หรือเปิดเผยข้อมูลส่วนบุคคลย่อมไม่สามารถกระทำได้หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นแต่เป็นข้อมูลที่เก็บรวบรวมได้โดยไม่ต้องได้รับความยินยอมตามที่กฎหมายกำหนดไว้ในมาตรา 21 หรือมาตรา 23 หรือเป็นข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้ว[15] ดังนั้น หลักการเกี่ยวกับการใช้หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัตินี้จะมีหลักการปกปิดเป็นหลักทั่วไป และการเปิดเผยเป็นข้อยกเว้น

ทั้งนี้ กรณีที่เข้าข้อยกเว้นแล้ว ผู้ที่ได้รับข้อมูลส่วนบุคคลจากการเปิดเผยดังกล่าวจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกจากวัตถุประสงค์ดั้งเดิมที่ได้ข้อมูลส่วนบุคคลนั้นมา นอกจากนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ยังกำหนดให้การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และจะต้อง

---

[14] มาตรา 23 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[15] มาตรา 24 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

เป็นไปตามหลักเกณฑ์การให้ความคุ้มครองที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะประกาศหากพระราชบัญญัตินี้มีผลใช้บังคับ ยกเว้นกรณีดังต่อไปนี้[16]

- เป็นการปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล
- เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้
- กรณีอื่นตามที่กำหนดในกฎกระทรวง

อนึ่ง หลักการเรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศข้างต้น เป็นการสะท้อนหลักดินแดนของการบังคับใช้กฎหมายของประเทศไทยซึ่งบัญญัติไปในแนวทางเดียวกับนานาประเทศ กล่าวคือ ตามหลักดินแดน กฎหมายของประเทศใดย่อมบังคับได้กับดินแดนของประเทศนั้นเท่านั้น ดังนั้น หากข้อมูลส่วนบุคคลของผู้ใช้บริการชาวไทยถูกโอนไปยังต่างประเทศ กฎหมายคุ้มครองข้อมูลส่วนบุคคลย่อมไม่สามารถใช้บังคับเหนือดินแดนของประเทศที่ข้อมูลถูกโอนไปได้ ด้วยเหตุนี้ นานาประเทศจึงได้กำหนดหลักเกณฑ์ให้ประเทศที่รับโอนข้อมูลส่วนบุคคลจากประเทศตนเองไปจะต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ต่ำกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศต้นทาง เพื่ออาศัยกฎหมายของประเทศปลายทางในการให้ความคุ้มครองข้อมูลส่วนบุคคลต่อไปตามหลักการของ Data Sovereignty นั่นเอง

5.2.7 สิทธิของเจ้าของข้อมูล

ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) เจ้าของข้อมูลมีสิทธิ 4 ประการ กล่าวคือ

5.2.7.1 สิทธิเข้าถึงข้อมูล

ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่อยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลหรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอมได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเปิดเผยภายใน 30 วันนับตั้งแต่วันที่ได้รับคำร้องขอ แต่อย่างไรก็ตาม สิทธิดังกล่าวไม่ใช่สิทธิเด็ดขาด เนื่องจากเจ้าของข้อมูลส่วนบุคคลอาจ

---

[16] มาตรา 25 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ถูกจำกัดไม่ให้เข้าถึงข้อมูลส่วนบุคคลของตนเองได้หากเป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมายอื่น คำสั่งศาล หรือมีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือการเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น ซึ่งกรณีเหล่านี้แม้ตนเองจะเป็นเจ้าของข้อมูลก็ไม่สามารถเข้าถึงได้[17] ทั้งนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องบันทึกการปฏิเสธนี้ด้วย

5.2.7.2 สิทธิในการลบ ทำลายหรือระงับการใช้ชั่วคราวหรือแปลงข้อมูล

ในกรณีที่ผู้ควบคุมข้อมูลไม่ปฏิบัติตามหลักเกณฑ์ต่างๆ ข้างต้นที่กำหนดไว้ในร่างพระราชบัญญัตินี้นั้น เจ้าของข้อมูลย่อมมีสิทธิขอให้ผู้ควบคุมข้อมูลดำเนินการลบ ทำลายหรือระงับการใช้ชั่วคราวหรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่ระบุชื่อก็ได้ ซึ่งหากผู้ควบคุมข้อมูลไม่ดำเนินการตามที่เจ้าของข้อมูลร้องขอ เจ้าของข้อมูลอาจร้องขอต่อคณะกรรมการเพื่อสั่งให้ผู้ควบคุมข้อมูลดำเนินการเช่นว่านั้นได้[18]

5.2.7.3 สิทธิในความถูกต้องหรือทันสมัยของข้อมูลส่วนบุคคล

โดยหลักนั้นผู้ควบคุมข้อมูลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องทันสมัย สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด อย่างไรก็ตาม ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ให้สิทธิแก่เจ้าของข้อมูลในการร้องขอให้ผู้ควบคุมข้อมูลดำเนินการข้างต้นได้ ทั้งนี้ หากผู้ควบคุมข้อมูลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลที่ให้ดำเนินการข้างต้นและเหตุที่ไม่ดำเนินการไว้กับบันทึกรายการข้อมูลส่วนบุคคลนั้นด้วย[19]

---

[17] มาตรา 26 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[18] มาตรา 27 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[19] มาตรา 28 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

5.2.7.4 สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ

เจ้าของข้อมูลย่อมมีสิทธิที่จะยื่นคำร้องต่อคณะกรรมการผู้เชี่ยวชาญ ซึ่งแต่งตั้งขึ้นโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้[20]

ภายหลังการพิจารณาคณะกรรมการดังกล่าวอาจมีคำสั่งให้ผู้ควบคุมข้อมูลดำเนินการ หรือห้ามดำเนินการใดๆ เพื่อบังคับให้เป็นไปตามสิทธิดังกล่าวได้[21]

5.2.8 หน้าที่และความรับผิด

ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งบังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล จะมีหน้าที่และความรับผิด ดังนี้

5.2.8.1 หน้าที่ของผู้ควบคุมข้อมูล

เนื่องจากผู้ควบคุมข้อมูลเป็นผู้ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลด้วย ดังนั้น ผู้ควบคุมข้อมูลจึงมีหน้าที่ดังต่อไปนี้[22]

- ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือนำไปใช้โดยมิชอบ
- ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลต้องดำเนินการเพื่อป้องกันมิให้บุคคลนั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาหรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นหรือที่เจ้าของข้อมูลได้เพิกถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ

---

[20] มาตรา 59 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[21] มาตรา 60 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[22] มาตรา 29 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

- แจ้งเหตุของการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

นอกเหนือจากหน้าที่พื้นฐานดังกล่าวข้างต้น ผู้ควบคุมข้อมูลยังมีหน้าที่ต้องจัดทำบันทึกรายการที่กฎหมายกำหนด ได้แก่ ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล ระยะเวลาการเก็บข้อมูลส่วนบุคคล สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคลรวมถึงเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น และการใช้และการเปิดเผยที่ได้รับยกเว้นไม่ต้องขอความยินยอมทั้งนี้ เพื่อให้เจ้าของข้อมูลสามารถตรวจสอบได้[23]

5.2.8.2 ความรับผิดของผู้ควบคุมข้อมูล

กรณีที่ปรากฏการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลด้วยประการใดๆ ที่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลนั้น ผู้ควบคุมข้อมูลจะต้องรับผิดทางแพ่ง ทางปกครอง และ/หรือทางอาญา แล้วแต่กรณีดังต่อไปนี้

(1) ความรับผิดทางแพ่ง

ผู้ควบคุมข้อมูลต้องชดใช้ค่าสินไหมทดแทนหากปรากฏการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลนั้น ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลหรือไม่ก็ตาม

อย่างไรก็ตาม ผู้ควบคุมข้อมูลอาจไม่ต้องรับผิดเช่นว่านั้น หากผู้ควบคุมข้อมูลสามารถพิสูจน์ได้ว่าการดำเนินการดังกล่าวเกิดจากกรณีดังต่อไปนี้

- เหตุสุดวิสัย หรือเกิดจากกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง
- การกระทำตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย
- การดำเนินการที่ครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลได้จัดทำขึ้นเพื่อกำหนดวิธีการคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

---

[23] มาตรา 31 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ทั้งนี้ ค่าสินไหมทดแทนที่ผู้ควบคุมข้อมูลจะต้องชดใช้ข้างต้นนั้น หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

(2) ความรับผิดทางปกครอง

ในกรณีที่ผู้ควบคุมข้อมูลไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมายดังต่อไปนี้ ผู้ควบคุมข้อมูลจะต้องระวางโทษปรับทางปกครองไม่เกิน 100,000 บาท[24]

- กรณีผู้ควบคุมข้อมูลไม่แจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดตามที่กำหนดไว้ในมาตรา 20 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลไม่ดำเนินการตามคำขอของเจ้าของข้อมูลให้ตนมีสิทธิเข้าถึงหรือให้เปิดเผยการได้มาซึ่งข้อมูลที่เจ้าของข้อมูลส่วนบุคคลไม่ยินยอม ตามมาตรา 26 วรรค 4 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลไม่จัดทำบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ตามมาตรา 31 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศหรือกำหนดตามมาตรา 17 วรรค 3 หรือไม่แจ้งผลกระทบจากถอนความยินยอมตามมาตรา 17 วรรค 5 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ในกรณีที่ผู้ควบคุมข้อมูลไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมายดังต่อไปนี้ ผู้ควบคุมข้อมูลจะต้องระวางโทษปรับทางปกครองไม่เกิน 300,000 บาท[25]

- กรณีผู้ควบคุมข้อมูลไม่เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 19 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

---

[24] มาตรา 69 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

[25] มาตรา 70 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

- กรณีผู้ควบคุมข้อมูลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 21 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง ตามมาตรา 22 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยหรือใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามมาตรา 24 วรรคแรก แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่เป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการกำหนด ตามมาตรา 25 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ในมาตรา 29 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)
- กรณีผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนเก็บรวบรวม (มาตรา 23) ใช้หรือเปิดเผย (มาตรา 24) โอนไปยังต่างประเทศ (มาตรา 25) ซึ่งข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการกำหนดโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลต้องระวาง<u>โทษปรับทางปกครองไม่เกิน 500,000 บาท</u>

5.2.8.3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

มาตรา 30 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่ คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

5.2.8.4 ความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลรายใด ไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ในมาตรา 30 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) โดยไม่มีเหตุอันควร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องระวางโทษปรับทางปกครองไม่เกิน 300,000 บาท

5.3 ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเมื่อบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์

เมื่อระบบการประมวลผลแบบคลาวด์เริ่มได้รับความนิยมเป็นอย่างมากในประเทศไทย ผู้เขียนจึงสังเกตว่าข้อมูลของผู้ใช้บริการจำนวนมาก (ไม่ว่าจะเข้าลักษณะเป็นข้อมูลส่วนบุคคลหรือไม่ก็ตาม) ถูกเก็บไว้ในระบบการประมวลผลแบบคลาวด์ โดยบางครั้งผู้ใช้บริการระบบการประมวลผลแบบคลาวด์ยังไม่อาจทราบได้ว่าปัจจุบันข้อมูลของตน โดยเฉพาะอย่างยิ่งข้อมูลที่มีลักษณะเป็นข้อมูลส่วนบุคคลได้ถูกจัดเก็บไว้ ณ ที่ใด ในประเทศไทยหรือในต่างประเทศ ดังนั้น จากการสังเกตดังกล่าวจึงนำมาสู่ข้อสงสัยว่ากฎหมายใดจะให้ความคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ได้บ้าง ซึ่งจากการศึกษาผ่านความเห็นของหน่วยงานที่เกี่ยวข้องในประเทศไทย เช่น กระทรวงวิทยาศาสตร์และเทคโนโลยี และหน่วยงานระดับสากลอย่างบีเอสเอ ผู้เขียนพบว่า ประเทศไทยกำลังประสบปัญหาเกี่ยวกับกฎหมายที่บังคับใช้กับการคุ้มครองข้อมูลส่วนบุคคลทั่วๆ ไป ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ที่ให้บริการโดยภาคเอกชน ดังนี้

5.3.1 ปัญหาการขาดแคลนกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้เป็นการทั่วไปกับภาคเอกชนและบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์ที่ให้บริการโดยภาคเอกชน

แม้ว่าประเทศไทยจะมีกฎหมายเฉพาะซึ่งบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งบัญญัติหลักการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการของการคุ้มครองข้อมูลส่วนบุคคลของสากลแล้วก็ตาม แต่เนื่องจาก

ขอบเขตการบังคับใช้ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จำกัดอยู่ที่ข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น ไม่รวมถึงข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชนแต่อย่างใด ดังนั้น กรณีย่อมทำให้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่สามารถใช้บังคับข้อมูลส่วนบุคคลที่จัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์ของภาคเอกชนได้ ทั้งนี้ เพราะผู้ให้บริการระบบการประมวลผลแบบคลาวด์ของประเทศไทยในปัจจุบัน ล้วนแต่เป็นรูปแบบการให้บริการที่ดำเนินการโดยภาคเอกชนทั้งสิ้น ดังนั้น จะเห็นได้ว่ากฎหมายที่มีอยู่ในปัจจุบัน ได้แก่ กฎหมายเฉพาะต่างๆ และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่เพียงพอที่จะคุ้มครองข้อมูลส่วนบุคคลของเอกชนที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ โดยปัญหาดังกล่าวได้สะท้อนออกมาผ่านทางรายงานการประเมินความพร้อมในระบบการประมวลผลแบบคลาวด์ของบีเอสเอ ซึ่งบีเอสเอได้พิจารณาว่าประเทศไทยไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่สามารถใช้บังคับกับระบบการประมวลผลแบบคลาวด์ได้ ดังนั้น ในการประเมินความพร้อมดังกล่าวในหัวข้อของความเป็นส่วนตัวของข้อมูล ประเทศไทยจึงสอบตกในประเด็นนี้ ซึ่งตราบใดที่ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผลการประเมินของบีเอสเอในด้านความเป็นส่วนตัวของข้อมูลของประเทศไทยย่อมไม่ได้รับการพัฒนา ซึ่งเรื่องนี้ส่งผลกระทบโดยตรงต่อการให้บริการระบบการประมวลผลแบบคลาวด์ไม่ว่าโดยทางตรงหรือทางอ้อม สำหรับผลกระทบทางตรง คือ ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ยังไม่ได้รับความคุ้มครองมากเท่าที่รัฐควรจะให้ความคุ้มครอง และผลกระทบทางอ้อม คือ ภาพลักษณ์ของประเทศไทย การค้าระหว่างประเทศตลอดจนความมั่นใจของผู้ให้บริการและผู้ใช้บริการระบบการประมวลผลแบบคลาวด์ทั่วโลก ด้วยเหตุนี้ ประเทศไทยจึงควรต้องเร่งพิจารณาให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกบังคับใช้ ทั้งนี้ ไม่ใช่เพื่อเพิ่มคะแนนในการประเมินความพร้อมของบีเอสเอ เพราะผลการประเมินความพร้อมดังกล่าวเปรียบเสมือนกระจกเงาสำหรับสะท้อนให้ประเทศต่างๆ เห็นปัญหาภายในประเทศของตนเท่านั้น แต่เพื่อให้ประเทศไทยมีโครงสร้างพื้นฐานทางด้านกฎหมายสำหรับรองรับการพัฒนาและขับเคลื่อนเศรษฐกิจดิจิทัลและเพื่อคุ้มครองข้อมูลทั้งในมิติของประชาชนทั่วไปและในด้านการประกอบธุรกิจที่เกี่ยวข้องกับไอทีหรือเทคโนโลยี โดยเฉพาะอย่างยิ่ง ธุรกิจที่เกี่ยวข้องกับการประมวลผลและการบริหารจัดการข้อมูล ได้แก่ ธุรกิจการให้บริการระบบการประมวลผลแบบคลาวด์นั่นเอง

อย่างไรก็ตาม ผู้เขียนตั้งข้อสังเกตว่า หากประเทศไทยจะประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว กฎหมายดังกล่าวควรจะต้องผ่านการพิจารณาด้วยว่ามีความเหมาะสมและครอบคลุมกับธุรกิจการให้บริการระบบการประมวลผลแบบคลาวด์โดยภาคเอกชน เพราะไม่เช่นนั้นแล้ว แม้ประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่หากกฎหมายดังกล่าวไม่

สามารถให้ความคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ที่ให้บริการโดยภาคเอกชนได้แล้ว การประกาศใช้กฎหมายดังกล่าวอาจจะไม่ก่อให้เกิดประโยชน์เท่าที่ควรจะเป็น ซึ่งหากจะอาศัยช่องทางในการแก้ไขกฎหมายในอนาคต ผู้เขียนมีความเห็นว่าการดำเนินการเช่นว่านั้นย่อมไม่สามารถทำให้เกิดขึ้นได้โดยง่าย ดังนั้น ในระหว่างการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลทุกภาคส่วนไม่ว่าจะเป็นหน่วยงานผู้รับผิดชอบในการยกร่าง หน่วยงานเอกชนซึ่งเป็นผู้ให้บริการและผู้ใช้บริการ ตลอดจนประชาชนทั่วไปจึงควรเข้ามามีส่วนร่วมในการยกร่างและผลักดันกฎหมายฉบับนี้

5.3.2 ปัญหาความไม่เหมาะสมของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) เมื่อบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์โดยภาคเอกชน

ดังที่ได้กล่าวไว้ ณ ข้างต้นว่า หากประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับ กฎหมายดังกล่าวควรจะต้องบังคับใช้กับการให้บริการระบบการประมวลผลแบบคลาวด์โดยภาคเอกชนได้ ซึ่งในมุมมองของบีเอสเอที่สะท้อนผ่านทางรายงานผลการประเมินเห็นว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ได้เป็นอย่างดีนั้นกฎหมายดังกล่าวควรเป็นกฎหมายที่มีหลักการสอดคล้องกับข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ได้แก่ Directive 95/46EC และ GDPR ตลอดจนมีหลักการที่สอดคล้องกับกรอบการคุ้มครองความเป็นส่วนตัวของ APEC ได้แก่ APEC Privacy Framework โดยเฉพาะอย่างยิ่งหลักการเรื่องการแจ้งให้ทราบเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล หลักการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและการโอนหรือส่งข้อมูลระหว่างประเทศจะต้องได้รับยกเว้นจากการขึ้นทะเบียน และที่สำคัญบีเอสเอยังให้ข้อแนะนำด้วยว่าการจะคุ้มครองข้อมูลส่วนบุคคลได้อย่างดี ประเทศไทยควรต้องมีหน่วยงานที่มีประสิทธิภาพในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

มุมมองของบีเอสเอข้างต้นเป็นเพียงมุมมองหนึ่งที่จะช่วยสะท้อนว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยที่จะออกมาบังคับใช้ควรเป็นอย่างไร ซึ่งจากการศึกษาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ผู้เขียนพบว่าหากพิจารณาในภาพรวม ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ของประเทศไทย ก็มีหลักการไปในแนวทางเดียวกับข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและกรอบการคุ้มครองความเป็นส่วนตัวของ APEC แล้ว แต่อย่างไรก็ตามหากพิจารณาโดยละเอียด ผู้เขียนกลับพบว่าร่างพระราชบัญญัติฉบับดังกล่าวยังมีความไม่เหมาะสมในหลายประการในการที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ที่ให้บริการโดยภาคเอกชน เช่น การขาดหลักการเรื่องขอบเขตการบังคับใช้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กับข้อมูลส่วนบุคคลที่สูญเสียสิ่งเชื่อมโยงตัวบุคคล การขาดหลักการเรื่องผู้ควบคุมข้อมูลร่วมกัน การ

ขาดรายละเอียดที่ครบถ้วนเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูล การขาดหลักการเรื่องสิทธิในการโอนย้ายข้อมูลของเจ้าของข้อมูลและการขาดข้อยกเว้นบางประการเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ เป็นต้น ซึ่งจะได้ศึกษาโดยละเอียดดังต่อไปนี้

5.3.2.1 ขอบเขตของข้อมูลที่จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

นับตั้งแต่แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้รับความสนใจจนกระทั่งมีการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลในนานาประเทศนั้น ข้อมูลส่วนบุคคลถือเป็นสิ่งสำคัญที่กฎหมายให้ความคุ้มครองและข้อมูลส่วนบุคคลยังเป็นปัจจัยสำคัญในการพิจารณาว่าข้อมูลนั้นๆ จะตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หมายความว่า หากข้อมูลนั้นมีลักษณะเป็นข้อมูลส่วนบุคคล ข้อมูลดังกล่าวย่อมได้รับความคุ้มครองตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ในทางกลับกัน หากข้อมูลดังกล่าวไม่เข้าคำจำกัดความของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดแล้ว เช่น ข้อมูลทั่วๆ ไปที่ไม่มีสิ่งบ่งชี้ตัวบุคคลหรือข้อมูลความลับทางการค้าที่ไม่มีสิ่งบ่งชี้ตัวบุคคล เป็นต้น ข้อมูลดังกล่าวย่อมไม่อยู่ภายใต้การบังคับและไม่ได้รับความคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นๆ (แต่อาจได้รับความคุ้มครองตามกฎหมายอื่น) ดังนั้น เมื่อหลายปีที่ผ่านมาขณะที่สหภาพยุโรปกำลังศึกษาและประชุมเพื่อหาแนวทางในการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นบังคับใช้เป็นฉบับแรก ได้แก่ Directive 95/46/EC นั้น ประเด็นเรื่องการกำหนดว่าข้อมูลใดบ้างที่จะอยู่ภายใต้บังคับของกฎหมายดังกล่าว ประเด็นเรื่องบทนิยามของข้อมูลส่วนบุคคล โดยเฉพาะถ้อยคำที่ว่า ‘ส่วนบุคคล’ และประเด็นเรื่องข้อมูลที่สูญเสียสิ่งเชื่อมโยงตัวบุคคลไปแล้วโดยถาวรหรือโดยชั่วคราว ได้แก่ ข้อมูลที่จะต้องมีการเข้าถึงรหัสลับ (Encrypted data) ข้อมูลนิรนาม (anonymized data) และข้อมูลแฝง (Pseudonymised data) ยังคงมีลักษณะเป็นข้อมูลส่วนบุคคลอยู่หรือไม่ ถือประเด็นสำคัญที่ได้รับการหยิบยกขึ้นมาพิจารณาอย่างหลีกเลี่ยงไม่ได้ในยุคสมัยดังกล่าว จนกระทั่งเมื่อเข้ามาสู่ยุคของการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ ได้แก่ GDPR ประเด็นข้างต้นก็ยังคงเป็นที่ถกเถียงและวิพากษ์วิจารณ์กันอย่างกว้างขวางเช่นเดิม[26]

โดยทั่วไปการพิจารณาว่าข้อมูลใดๆ จะตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ จำเป็นต้องพิจารณาว่าข้อมูลนั้นมีลักษณะที่เป็นส่วนบุคคลหรือไม่

---

[26] Gerald Spindler and Philipp Schmechel, “Personal Data and Encryption in the European General Data Protection Regulation,” Journal of Intellectual Property, Information Technology and E-Commerce Law, Volume 7, 163-164 (September 2016).

เป็นหลัก[27] เนื่องจากข้อมูลที่จะตกอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้แก่ ข้อมูลส่วนบุคคลเท่านั้น กรณีจึงนำมาสู่ประเด็นที่จะต้องพิจารณาต่อไปว่าข้อมูลที่สูญเสียสิ่งที่จะเชื่อมโยงถึงตัวบุคคลไม่ว่าโดยถาวรหรือโดยชั่วคราวได้แก่ข้อมูลประเภทใดบ้าง และข้อมูลนั้นมีลักษณะเป็นข้อมูลส่วนบุคคลหรือไม่ ดังนี้

(1) เทคนิคที่ใช้ทำให้ข้อมูลสูญเสียสิ่งเชื่อมโยงตัวบุคคลไม่ว่าโดยถาวรหรือชั่วคราว

โดยหลักกระบวนการที่จะทำให้ข้อมูลส่วนบุคคลสูญเสียสิ่งที่จะสามารถเชื่อมโยงตัวบุคคลซึ่งเป็นเจ้าของข้อมูลได้จะประกอบไปด้วยกระบวนการต่างๆ ดังนี้

- **กระบวนการแปลงข้อมูลนิรนาม (Anonymization)**

กระบวนการแปลงข้อมูลนิรนาม (Anonymization) หมายถึง วิธีการใดๆ ที่จะทำให้ข้อมูลส่วนบุคคลในชุดข้อมูลของเจ้าของข้อมูลได้รับความคุ้มครองก่อนที่จะมีการส่งต่อไปยังบุคคลที่สาม ทำให้บุคคลที่สามซึ่งเป็นผู้รับข้อมูลมีโอกาสน้อยที่สุดที่จะนำข้อมูลดังกล่าวไปใช้ในการวิเคราะห์ที่ทำให้รู้ตัวเจ้าของข้อมูลส่วนบุคคลได้ ทั้งนี้ ในปัจจุบันกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ประกอบด้วย 3 เทคนิคหลัก[28] คือ

1. Data Hiding หรือ Suppression ซึ่งเป็นเทคนิคพื้นฐานของกระบวนการแปลงข้อมูลนิรนาม โดยเทคนิค Suppression จะดึงข้อมูลส่วนบุคคลที่ไม่สามารถเปิดเผยได้ เช่น ชื่อ-สกุล หมายเลขประจำตัวประชาชน หมายเลขประกันสังคม เป็นต้น ออกไปจากชุดข้อมูลทั้งหมดโดยมีวัตถุประสงค์ให้ข้อมูลดังกล่าวไม่ปรากฏในชุดข้อมูลอีกต่อไป ซึ่งวิธีการดึงข้อมูลดังกล่าวอาจโดยวิธีการแทนค่าข้อมูลนั้นด้วย ‘0’ ตัวอย่างการใช้เทคนิค Suppression แปลงข้อมูลได้แก่

ข้อมูลชุดเดิมเกี่ยวกับปัญหาสุขภาพผู้คนไข้

Patient name	Gender	Age	Zip code	Health Problem
Amit	Male	35	400071	Viral Infection

[27] ซึ่งวิธีการแยกแยกข้อมูลส่วนบุคคลโดยคำนึงว่าข้อมูลนั้นเป็นส่วนบุคคลหรือไม่เรียกกันโดยทั่วไปว่า “Black/White Approach”

[28] International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May2013 Page 1667-1670 เขียนโดย Asst.Prof.Ms. Apeksha Sakhare and Ms. Swati Ganar เรื่อง Anonymization: A Method To Protect Sensitive Data In Cloud

Patient name	Gender	Age	Zip code	Health Problem
Pankaj	Male	37	400182	Viral Infection
Vishal	Male	39	400095	Heart Problem
Sheetal	Female	54	440672	Flu
Pallavi	Female	58	440123	Heart Problem
Nilesh	Male	54	440893	Viral Problem
Sagar	Male	41	400022	Flu
Mahesh	Male	46	400135	Flu
Sujata	Female	44	400182	Flu

ข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนามโดยใช้เทคนิค Suppression จะคงเหลือเพียงเพศและปัญหาทางสุขภาพที่จะนำไปประมวลผลได้ โดยกระบวนการ Suppression จะแทนค่าชื่อ อายุและรหัสไปรษณีย์ด้วย ‘0’ ทั้งหมด ดังนี้

Patient name	Gender	Age	Zip code	Health Problem
0	Male	0	0	Viral Infection
0	Male	0	0	Viral Infection
0	Male	0	0	Heart Problem
0	Female	0	0	Flu
0	Female	0	0	Heart Problem
0	Male	0	0	Viral Problem
0	Male	0	0	Flu
0	Male	0	0	Flu
0	Female	0	0	Flu

2. Generalization เป็นเทคนิคในการทดแทนสิ่งเชื่อมโยงตัวบุคคลประเภท Quasi (Quasi Identifier) เช่น เพศ วันเกิด รหัสไปรษณีย์ การวินิจฉัยโรค เป็นต้น ด้วยข้อมูลอื่น โดยวันเดือนปีเกิดอาจทดแทนด้วยปีเกิดเท่านั้น หรือรหัสไปรษณีย์อาจเหลือเพียงชุดตัวเลขที่ไม่สามารถชี้เฉพาะเจาะจงได้ว่าเป็นพื้นที่ใด ตัวอย่างเช่น

ข้อมูลชุดเดิมเกี่ยวกับปัญหาสุขภาพผู้คนไข้

Patient name	Gender	Age	Zip code	Health Problem
Amit	Male	35	400071	Viral Infection
Pankaj	Male	37	400182	Viral Infection
Vishal	Male	39	400095	Heart Problem
Sheetal	Female	54	440672	Flu
Pallavi	Female	58	440123	Heart Problem
Nilesh	Male	54	440893	Viral Problem
Sagar	Male	41	400022	Flu
Mahesh	Male	46	400135	Flu
Sujata	Female	44	400182	Flu

รหัสไปรษณีย์ที่ผ่านกระบวนการแปลงข้อมูลนิรนามโดยใช้เทคนิค Generalization จะถูกแทนค่าด้วยด้วย * ทำให้ไม่สามารถระบุพื้นที่ได้ชัดเจน ดังนี้

Patient name	Gender	Age	Zip code	Health Problem
Amit	Male	35	400*	Viral Infection
Pankaj	Male	37	400*	Viral Infection
Vishal	Male	39	400*	Heart Problem
Sheetal	Female	54	440*	Flu
Pallavi	Female	58	440*	Heart Problem
Nilesh	Male	54	440*	Viral Problem
Sagar	Male	41	400*	Flu
Mahesh	Male	46	400*	Flu
Sujata	Female	44	400*	Flu

3. Aggregation วิธีการนี้จะไม่แสดงผลชุดข้อมูลทั้งหมดที่จัดเก็บไว้ แต่จะปรากฏผลรวมของชุดข้อมูลในเชิงสถิติแทน ยกตัวอย่างเช่น

ข้อมูลชุดเดิมเกี่ยวกับปัญหาสุขภาพผู้คนไข้

Patient name	Gender	Age	Zip code	Health Problem
Amit	Male	35	400071	Viral Infection
Pankaj	Male	37	400182	Viral Infection
Vishal	Male	39	400095	Heart Problem
Sheetal	Female	54	440672	Flu
Pallavi	Female	58	440123	Heart Problem
Nilesh	Male	54	440893	Viral Problem
Sagar	Male	41	400022	Flu
Mahesh	Male	46	400135	Flu
Sujata	Female	44	400182	Flu

วิธีการ Aggregation จะไม่แสดงข้อมูลตามตารางข้างต้น แต่จะแสดงผลรวมทางสถิติจากการที่ผู้ใช้งานค้นหาแทน เช่น หากผู้ใช้ข้อมูลค้นหาว่ามีบุคคลใดเป็นไข้หวัด (Flu) บ้าง ข้อมูลที่แสดงจะปรากฏเพียงว่ามีคนเป็นหวัดจำนวนทั้งสิ้น 4 คน ดังนี้

Health Problem	Number of patients
Flu	4

- **กระบวนการแปลงข้อมูลแฝง (Pseudonymization)**

กระบวนการแปลงข้อมูลแฝง (Pseudonymization) เป็นกระบวนการที่มีลักษณะคล้ายคลึงกับกระบวนการแปลงข้อมูลนิรนาม (Anonymization) โดยหมายถึง กระบวนการประมวลผลข้อมูลส่วนบุคคลในทางที่ข้อมูลส่วนบุคคลไม่สามารถพิจารณาได้ว่าเป็นข้อมูลของเจ้าของข้อมูลส่วนบุคคลคนใดโดยเฉพาะหากไม่มีการนำข้อมูลส่วนอื่นๆ ที่ถูกจัดเก็บไว้แยกต่างหากและมีมาตรฐานการจัดการองค์กรหรือมาตรฐานทางเทคนิคป้องกันไว้มาประกอบหรือมาเชื่อมโยงไม่ว่าโดยทางตรงหรือทางอ้อม[29] ตัวอย่างเช่น Phil Lee ซื้อสินค้าประเภท x เมื่อผ่านกระบวนการแปลงข้อมูลแฝงจะกลายเป็น Visitor 15364 ซื้อสินค้าประเภท x เป็นต้น

[29] (26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have

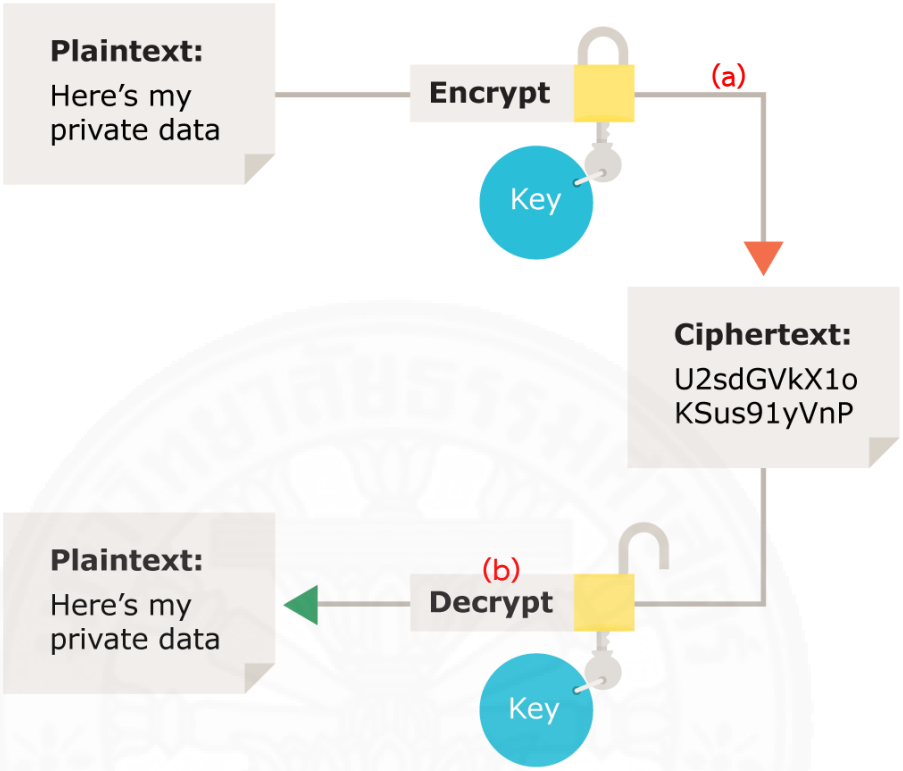
- **กระบวนการเข้ารหัสข้อมูล (Encryption)**

กระบวนการเข้ารหัสข้อมูล (Encryption) เป็นกระบวนการรักษาความปลอดภัยให้แก่ข้อมูลส่วนบุคคลวิธีการหนึ่งที่ได้รับความนิยมเป็นอย่างมาก โดยมีลักษณะเป็นการเข้ารหัสหรือการแปลงข้อมูลให้เป็นรหัสลับเพื่อไม่ให้ข้อมูลถูกอ่านได้โดยบุคคลที่ไม่ได้รับอนุญาตผ่านทางการนำข้อมูลเดิมที่บุคคลใดๆ ก็สามารถอ่านได้ในรูปแบบที่เรียกว่า “Plain Text” หรือ “Clear Text” มาทำการเข้ารหัสก่อนเพื่อเปลี่ยนแปลงข้อมูลเดิมให้เป็นข้อความที่เราเข้ารหัส (Ciphertext) และเมื่อข้อมูลถูกส่งไปยังบุคคลที่ได้รับอนุญาตให้เข้าถึงแล้วก็จะเข้าสู่กระบวนการที่เรียกว่า Decryption หรือกระบวนการถอดรหัสข้อมูล ในทางปฏิบัติ วิธีการที่นิยมใช้ในกระบวนการเข้ารหัสข้อมูล (Encryption) จำแนกได้เป็น 2 วิธี โดยพิจารณาจากความแตกต่างของกุญแจที่ใช้สำหรับเข้าถึงข้อมูล ดังนี้

1. Symmetric Encryption ซึ่งเป็นกระบวนการเข้ารหัสข้อมูลโดยที่กำหนดกุญแจสำหรับเข้าถึงข้อมูลเป็นชุดเดียวกันไม่ว่าในกระบวนการ Encryption หรือ Decrytion ซึ่งสามารถสรุปเป็นขั้นตอนได้ดังนี้

---

undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

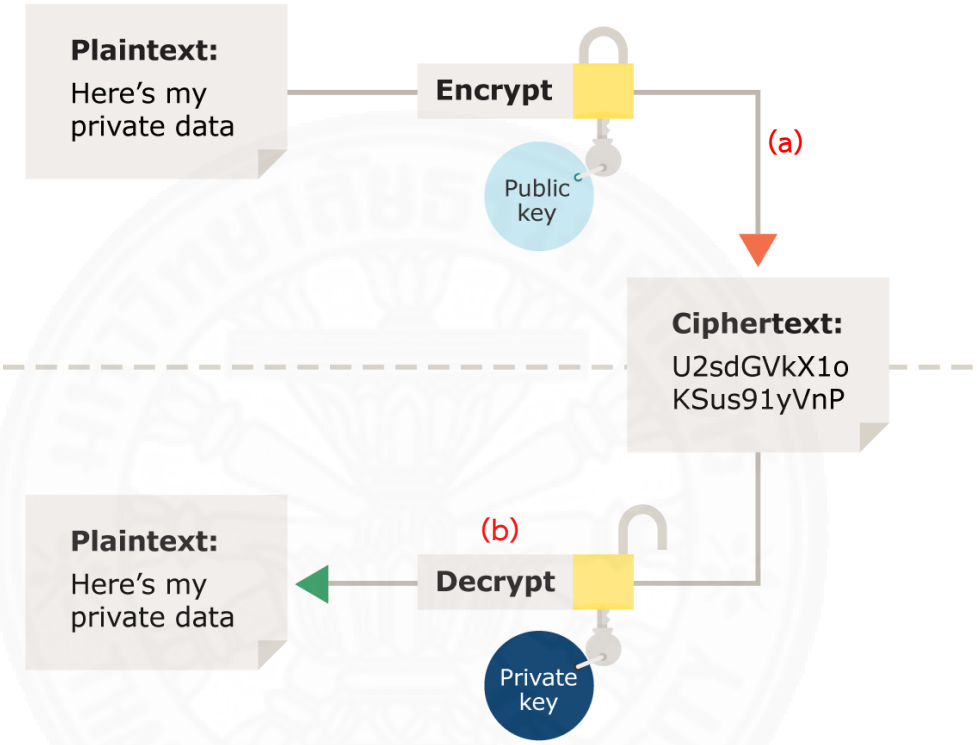


ภาพที่ 1 แสดงกระบวนการ Symmetric Encryption, Information Commissioner Office, "Types of encryption", https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/types-of-encryption/

(a) ผู้ส่งข้อมูลนำข้อมูล Plain Text ที่จะส่งมาทำการเข้ารหัสก่อนเพื่อเปลี่ยนแปลงข้อมูลเดิมให้เป็นข้อความที่เราเข้ารหัส (Ciphertext) และใส่กุญแจสำหรับเข้าถึงข้อมูล พร้อมทั้งให้กุญแจสำหรับเข้าถึงข้อมูลกับผู้รับข้อมูล หรือผู้รับข้อมูลอาจกำหนดกุญแจสำหรับเข้าถึงขึ้นเองและมอบกุญแจดังกล่าวให้แก่ผู้ส่งก็ได้

(b) ผู้รับข้อมูลทำการถอดรหัสข้อมูลที่ตนเองได้รับมา (Decryp ciphertext) โดยใช้กุญแจสำหรับเข้าถึงข้อมูล

2. Asymmetric Encryption ซึ่งเป็นกระบวนการเข้ารหัสข้อมูลโดยที่กำหนดกุญแจสำหรับเข้าถึงข้อมูลในกระบวนการ Encryption และ Decrytion ให้แตกต่างกัน โดยกุญแจหนึ่งจะเรียกว่า “Private Key” และกุญแจอีกอันหนึ่งจะเรียกว่า “Public Key” ซึ่งสามารถสรุปเป็นขั้นตอนได้ดังนี้



ภาพที่ 2 แสดงกระบวนการ Asymmetric Encryption, Information Commissioner Office, “Types of encryption”, https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/types-of-encryption/

(a) ผู้ส่งข้อมูลนำข้อมูล Plain Text ที่จะส่งมาทำการเข้ารหัสก่อนเพื่อเปลี่ยนแปลงข้อมูลเดิมให้เป็นข้อความที่เราเข้ารหัส (Ciphertext) ใส่กุญแจสำหรับกระบวนการ Encryption โดยเป็นกุญแจประเภท Public Key และตั้งค่ากุญแจสำหรับ Decryption โดยใช้กุญแจประเภท Private Key

(b) ผู้รับข้อมูลทำการถอดรหัสข้อมูลที่ตนเองได้รับมา (Decryp ciphertext) โดยใช้กุญแจประเภท Private Key

(2) ข้อพิจารณาทางกฎหมาย

กระบวนการดังกล่าวข้างต้นนับเป็นเทคโนโลยีที่เข้ามาช่วยในการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลในทางปฏิบัติและช่วยลดความเสี่ยงของเจ้าของข้อมูล ซึ่งจะเป็นประโยชน์ต่อเจ้าของข้อมูลโดยตรง ดังนั้น กระบวนการดังกล่าวจึงควรได้รับการส่งเสริมให้ผู้ให้บริการนำกระบวนการข้างต้นมาใช้ แต่อย่างไรก็ตาม กระบวนการดังกล่าวได้ก่อให้เกิดปัญหาที่ให้นักกฎหมายของแต่ละประเทศจะต้องมาพิจารณาว่า ข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) กระบวนการแปลงข้อมูลแฝง (Pseudonumization) และกระบวนการเข้ารหัสข้อมูล (Encyption) แล้วจะยังถือเป็นข้อมูลส่วนบุคคลที่ต้องตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ซึ่งในประเด็นนี้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศรวมถึงสหภาพยุโรปเอง จึงได้บัญญัติเกี่ยวกับการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับข้อมูลดังกล่าวไว้โดยเฉพาะเพื่อให้เกิดความชัดเจนในการบังคับใช้ โดยแบ่งพิจารณาแต่ละประเภทของกระบวนการข้างต้นได้ ดังนี้

<u>กระบวนการแปลงข้อมูลนิรนาม (Anonymization)</u> ในประเด็นเรื่องกระบวนการแปลงข้อมูลนิรนาม (Anonymization) นั้น สหภาพยุโรปได้ตระหนักถึงปัญหานี้มาตั้งแต่การยกร่าง Directive 95/46/EC จึงได้บัญญัติถึงข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ไว้ใน Recital 26 ขึ้นมาว่า Directive 95/46/EC ไม่ใช้บังคับกับข้อมูลส่วนบุคคลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ดังนั้น ข้อมูลใดที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลได้อย่างอิสระตราบเท่าที่ข้อมูลดังกล่าวไม่ได้เชื่อมโยงไปถึงตัวบุคคลซึ่งเป็นเจ้าของข้อมูล แม้ต่อมาเมื่อ GDPR เกิดขึ้นแล้ว คณะผู้ยกร่าง GDPR ยังคงเล็งเห็นถึงความสำคัญและปัญหาของกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ที่มีอยู่เดิม ดังนั้น GDPR จึงบัญญัติไว้ใน Recital 26 ในลักษณะเดียวกับ Directive 95/46/EC ว่า GDPR ไม่ใช้บังคับกับข้อมูลส่วนบุคคลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ซึ่งทำให้สูญเสียสิ่งเชื่อมโยงตัวบุคคลกับเจ้าของข้อมูล

นอกจากนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของประเทศญี่ปุ่น หรือ APPI ที่เพิ่งได้รับการแก้ไขและประกาศบังคับใช้เมื่อไม่นานมานี้ก็ได้รับหลักการและสภาพปัญหาของข้อมูลส่วนบุคคลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ไปไว้ในกฎหมายของตนเช่นเดียวกัน สังเกตได้จากการที่ APPI กำหนดบทนิยามของข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ซึ่งเรียกว่า “Anonymized Information” หรือ “ข้อมูลนิราม” ไว้ว่าหมายถึง ข้อมูลใดๆ เกี่ยวกับบุคคลที่ข้อมูลที่สามารถเชื่อมโยงตัวบุคคลหรือสิ่งบ่งชี้ตัวบุคคลถูกลบ

ออกทั้งหมดและสิ่งเชื่อมโยงหรือบ่งชี้ดังกล่าวไม่สามารถกู้คืนกลับมาได้ ทั้งนี้ มีผู้ให้ความเห็นไว้ว่า[30] หากผู้ให้บริการหรือผู้ควบคุมข้อมูลสามารถดำเนินการกับข้อมูลส่วนบุคคลให้ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ได้อย่างมีประสิทธิภาพซึ่งจะทำให้สิ่งสูญเสียสิ่งบ่งชี้ตัวบุคคลโดยถาวรแล้ว ผู้ให้บริการหรือผู้ควบคุมข้อมูลย่อมสามารถเปิดเผยข้อมูลดังกล่าวให้แก่บุคคลภายนอกได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล ดังนั้น หากตีความความเห็นดังกล่าวข้างต้นจะพบว่าข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ภายใต้ APPI เป็นข้อมูลที่สูญเสียสิ่งเชื่อมโยงบุคคลจึงไม่ถือเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของ APPI นั่นเอง

<u>กระบวนการแปลงข้อมูลแฝง (Pseudonymization)</u> กระบวนการแปลงข้อมูลแฝง (Pseudonymization) ก็ประสบปัญหาในทางปฏิบัติเช่นเดียวกับกระบวนการแปลงข้อมูลนิรนาม (Anonymization) กล่าวคือ ข้อมูลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) จะยังถือเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ โดยเฉพาะอย่างยิ่งในสหภาพยุโรป เนื่องจาก Directive 95/46/EC กล่าวถึงแต่เพียงข้อมูลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) เท่านั้น โดยมิได้กล่าวถึงข้อมูลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) แต่อย่างใด ดังนั้น เมื่อมีการยกร่าง GDPR เพื่อบังคับใช้จึงทำให้กระบวนการแปลงข้อมูลแฝง (Pseudonymization) เป็นกระบวนการที่ได้รับการกล่าวถึงในระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเป็นครั้งแรกใน GDPR โดย GDPR ตระหนักถึงปัญหาและความสำคัญของกระบวนการแปลงข้อมูลแฝง (Pseudonymization) ดังที่ได้กล่าวไว้ว่ากระบวนการแปลงข้อมูลแฝง (Pseudonymization) สามารถช่วยลดความเสี่ยงให้แก่เจ้าของข้อมูลได้[31]

อย่างไรก็ตาม เมื่อพิจารณาบทบัญญัติเกี่ยวข้องกับกระบวนการแปลงข้อมูลแฝง (Pseudonymization) ภายใต้ GDPR จะพบว่า กระบวนการแปลงข้อมูลแฝง

---

[30] DLA Piper, “Data Protection Laws of the World,” สืบค้นเมื่อวันที่ 3 พฤศจิกายน 2560, จาก https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all.

[31] Whereas: (28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.

(Pseudonymization) ยังมิใช่มาตรการเดียวที่จะเพียงพอให้ได้รับยกเว้นให้ไม่ต้องตกอยู่ภายใต้บังคับของการคุ้มครองข้อมูลส่วนบุคคลตามขอบเขตการบังคับใช้ของ GDPR ทั้งนี้ เนื่องจาก ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) ยังคงสามารถเชื่อมโยงถึงตัวบุคคลซึ่งเป็นเจ้าของข้อมูลได้หากมีข้อมูลอื่นมาเชื่อมโยงหรือประกอบเข้ากัน จึงถือว่าเป็นข้อมูลที่ยังสามารถเชื่อมโยงถึงตัวบุคคลได้หรือเป็นข้อมูลส่วนบุคคลนั่นเอง[32] ดังนั้น แม้ว่าข้อมูลดังกล่าวจะผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) แล้ว ข้อมูลดังกล่าวยังต้องอยู่ภายใต้บังคับของ GDPR อยู่เช่นเดิม

อนึ่ง การกำหนดให้ข้อมูลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) ยังคงเป็นข้อมูลส่วนบุคคลและอยู่ภายใต้บังคับของ GDPR มิได้หมายความว่าคณะผู้ยกร่าง GDPR ไม่ให้ความสำคัญกับกระบวนการแปลงข้อมูลแฝง (Pseudonymization) คณะผู้ยกร่าง GDPR ยังคงตระหนักถึงความสำคัญของกระบวนการแปลงข้อมูลแฝง (Pseudonymization) ที่จะช่วยคุ้มครองสิทธิของเจ้าของข้อมูล ดังนั้น คณะผู้ยกร่าง GDPR จึงให้สิทธิประโยชน์แก่ผู้ควบคุมข้อมูลเพื่อจูงใจให้มีการใช้กระบวนแปลงข้อมูลแฝง (Pseudonymization) เมื่อมีการประมวลผลข้อมูลส่วนบุคคล ซึ่งสิทธิประโยชน์ดังกล่าว ได้แก่

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ดั้งเดิม

โดยหลักตาม GDPR นั้น การประมวลผลข้อมูลส่วนบุคคลจะต้องกระทำภายใต้ขอบวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมเอาไว้หรือมีกฎหมายกำหนดอนุญาตให้สามารถกระทำได้เท่านั้น อย่างไรก็ตาม เพื่อเป็นการสนับสนุนกระบวนแปลงข้อมูลแฝง (Pseudonymization) มาตรา 5(4) ของ GDPR ได้กำหนดข้อยกเว้นของหลักการข้างต้นว่า หากผู้ควบคุมข้อมูลมีกระบวนการรักษาความปลอดภัยที่เหมาะสมซึ่งรวมถึงกระบวนเข้ารหัส (Encryption) หรือกระบวนการแปลงข้อมูลแฝง (Pseudonymization) แล้ว ผู้ควบคุมข้อมูลที่ได้ใช้กระบวนการ

---

[32] (28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

แปลงข้อมูลแฝง (Pseudonymization) กับข้อมูลส่วนบุคคลแล้วสามารถประมวลผลข้อมูลนอกเหนือจากวัตถุประสงค์ในการจัดเก็บข้อมูลได้

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในทางวิทยาศาสตร์ ประวัติศาสตร์และสถิตินอกเหนือจากวัตถุประสงค์ดั้งเดิม

ดังที่ได้กล่าวไว้ในเรื่องของหลักเกณฑ์ของ GDPR ว่าผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ดั้งเดิมที่เจ้าของข้อมูลได้ให้ความยินยอมไว้ได้ หากการประมวลผลดังกล่าวเป็นการประมวลผลที่มีวัตถุประสงค์ในทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ อย่างไรก็ตาม มาตรา 89(1) ของ GDPR กำหนดเป็นบทบังคับให้ผู้ควบคุมข้อมูลที่ประมวลผลเพื่อวัตถุประสงค์ดังกล่าวจะต้องมีมาตรการหรือเครื่องป้องกันคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม (appropriate safeguard) รวมทั้งมาตรการจัดการองค์กรและจัดการทางเทคนิคด้วย ตัวอย่างเช่น กระบวนการแปลงข้อมูลแฝง (Pseudonymization) เพื่อไม่ให้มีการเชื่อมโยงไปถึงสิ่งที่สามารถระบุตัวตนของเจ้าของข้อมูลได้

- ลดภาระหน้าที่ของผู้ควบคุมข้อมูลในการแจ้งความเสี่ยงแก่เจ้าของข้อมูลในกรณีที่ความเสี่ยงของข้อมูลส่วนบุคคลอยู่ในระดับสูง

ภายใต้มาตรา 32 ของ GDPR กำหนดว่าผู้ควบคุมข้อมูลจะต้องมีมาตรการป้องกันความเสียหายสำหรับคุ้มครองความปลอดภัยของข้อมูลซึ่งมาตรการดังกล่าว ได้แก่ กระบวนการแปลงข้อมูลแฝง (Pseudonymization) และกระบวนการเข้ารหัส (Encryption) ซึ่งการปรับใช้กระบวนการ Pseudonumization จะช่วยลดความเสี่ยงที่ข้อมูลส่วนบุคคลจะได้รับความเสียหายและช่วยให้ผู้ควบคุมข้อมูลลดภาระในการคอยตรวจสอบดูแลข้อมูลส่วนบุคคลที่มีความเสี่ยงในระดับสูง รวมทั้งลดภาระในการแจ้งความเสี่ยงดังกล่าวให้แก่เจ้าของข้อมูลด้วย

- ลดภาระหน้าที่ของผู้ควบคุมข้อมูลในการแจ้งสิทธิและปฏิบัติตามสิทธิของเจ้าของข้อมูลในการเข้าถึง (access) แก้ไข (rectification) และลบ (erasure) ข้อมูลส่วนบุคคล

หากผู้ควบคุมข้อมูลมีมาตรการคุ้มครองข้อมูลโดยใช้กระบวนการแปลงข้อมูลแฝง (Pseudonymization) กับข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลสามารถละเว้นการให้สิทธิเจ้าของข้อมูลในการเข้าถึง แก้ไขและลบข้อมูลส่วนบุคคลได้ตราบเท่าที่ข้อมูลนั้นไม่สามารถเชื่อมโยงถึงตัวบุคคลได้ ทั้งนี้ ตามมาตรา 11 แห่ง GDPR ซึ่งการละเว้นหน้าที่นี้จะใช้ได้ในเฉพาะกรณีที่ผู้ควบคุมข้อมูลสามารถแสดงให้เห็นได้ว่าไม่มีทางใดที่จะเชื่อมโยงข้อมูลดังกล่าวกับเจ้าของข้อมูล

จะเห็นได้ว่าเมื่อ GDPR มีผลใช้บังคับสหภาพยุโรปก็จะสามารถลดปัญหาในทางปฏิบัติได้อีกหนึ่งประเด็น ดังนั้น กรณีจึงยุติข้อถกเถียงว่าข้อมูลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonymization) จะถือเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของกฎหมายหรือไม่อีกต่อไป

<u>กระบวนการเข้ารหัส (Encryption)</u> เช่นเดียวกับกระบวนการอื่นๆ ปัญหาหลักในทางปฏิบัติเกี่ยวเนื่องกับกระบวนการเข้ารหัส (Encryption) คือ ข้อมูลที่ผ่านกระบวนการเข้ารหัส (Encryption) แล้วจะยังคงถือเป็นข้อมูลส่วนบุคคลที่จะตกอยู่ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ โดยเฉพาะอย่างยิ่งในระบบการประมวลผลแบบคลาวด์ที่กระบวนการเข้ารหัส (Encryption) จัดเป็นกระบวนการหนึ่งที่ได้รับความนิยมจากผู้ให้บริการระบบการประมวลผลแบบคลาวด์เป็นอย่างมาก ซึ่งมักจะเกิดคำถามเสมอว่าหากผู้ควบคุมข้อมูลใช้กระบวนการเข้ารหัส (Encryption) กับข้อมูลส่วนบุคคลก่อนอัพโหลดลงในระบบการประมวลผลแบบคลาวด์ ข้อมูลดังกล่าวจะยังถือเป็นข้อมูลส่วนบุคคลหรือไม่

กระบวนการเข้ารหัส (Encryption) ถูกบัญญัติอย่างเป็นทางการในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเป็นครั้งแรกใน มาตรา 32 และมาตรา 34 ของ GDPR โดยเป็นส่วนหนึ่งของมาตรการที่จะช่วยในการคุ้มครองข้อมูลส่วนบุคคล แต่ GDPR ไม่ได้กำหนดบทนิยามหรือคำจำกัดความของข้อมูลที่ผ่านกระบวนการเข้ารหัส (Encryption) ไว้โดยเฉพาะ ดังนั้น แม้ GDPR จะมีผลใช้บังคับกรณีก็ยังคงมีความไม่ชัดเจนว่าข้อมูลที่ผ่านกระบวนการเข้ารหัส (Encryption) จะมีผลเช่นไร เนื่องจากกระบวนการเข้ารหัส (Encryption) อาจทำให้ข้อมูลนั้นๆ สูญเสียสิ่งเชื่อมโยงส่วนบุคคลไปเลยหรือไม่ก็ยังสามารถเชื่อมโยงได้อยู่แต่ต้องอาศัยกุญแจ ซึ่งในกรณีเช่นนี้ว่ากระบวนการเข้ารหัส (Encryption) จะมีสถานะเป็นเพียงเครื่องมือหรือเทคโนโลยีที่ช่วยรักษาความปลอดภัยเท่านั้น ในปัจจุบัน GDPR ยังไม่สามารถแก้ไขปัญหาในส่วนนี้ได้อย่างชัดเจน ทำให้ในทางปฏิบัติก็ยังคงมีปัญหาอยู่ต่อไป

จากปัญหาข้างต้นที่เกิดขึ้นในต่างประเทศ เมื่อพิจารณาประเทศไทยจะพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ยังไม่ได้รับหลักการที่เกี่ยวเนื่องกับกระบวนการแปลงข้อมูลนิรนาม (Anonymization), กระบวนการแปลงข้อมูลแฝง (Pseudonumization) และกระบวนการเข้ารหัส (Encyption) มาบัญญัติไว้แต่อย่างใด เพราะฉะนั้น ปัญหาต่างๆ ในทางปฏิบัติที่เกิดขึ้นในต่างประเทศจึงยังคงเป็นปัญหาของประเทศไทยอยู่ เนื่องจากร่างพระราชบัญญัติให้คำจำกัดความของ “ข้อมูลส่วนบุคคล” ไว้ว่า ข้อมูลส่วนบุคคลหมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรม

โดยเฉพาะ ซึ่งเมื่อวิเคราะห์คำจำกัดความของข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติดังกล่าวย่อมสามารถตีความได้ว่า ข้อมูลที่ผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonumization) และกระบวนการเข้ารหัส (Encyption) ซึ่งยังมีโอกาสที่จะสามารถเชื่อมโยงไปยังบุคคลเจ้าของข้อมูลได้ไม่ว่าโดยทางตรงหรือทางอ้อม ทำให้ข้อมูลดังกล่าวแม้ว่าจะผ่านกระบวนการแปลงข้อมูลแฝง (Pseudonumization) และกระบวนการเข้ารหัส (Encyption) ก็ยังคงถือเป็นข้อมูลส่วนบุคคลและตกอยู่ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ได้

อย่างไรก็ตาม สำหรับข้อมูลส่วนบุคคลที่ผ่านกระบวนการแปลงข้อมูลนิรนาม (Anonymization) ซึ่งถือเป็นกระบวนการที่สามารถเชื่อมโยงกลับไปยังตัวเจ้าของข้อมูลได้น้อยที่สุดจนถึงกระทั่งไม่สามารถเชื่อมโยงได้เลย กรณีเช่นว่านี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพิจารณาว่าข้อมูลนั้นจะต้องตกอยู่ภายใต้บังคับหรือไม่ ซึ่งยังคงประเด็นที่ไม่ชัดเจน

<u>ข้อเสนอแนะ</u> ผู้เขียนมีความเห็นว่าหากจะให้ปัญหานี้ไม่เกิดขึ้นในทางปฏิบัติและเพื่อเป็นการส่งเสริมให้มีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างรัดกุม ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรกำหนดไปให้ชัดเจนเหมือนดังเช่นที่ Directive 95/45/EC และ GDPR ได้กำหนดไว้แล้ว โดยการแก้ไขมาตรา 4 โดยการเพิ่มอนุมาตรา (6) ดังนี้

> มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่
>
> (1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น
>
> (2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
>
> (3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภาพ รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
>
> (4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(5) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(6) ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลลบสิ่งเชื่อมโยงตัวบุคคลออกอย่างถาวรจนทำให้ไม่สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

5.3.2.2 หลักการเรื่องผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน (Joint Controller)

โดยหลักบุคคลที่จะตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศนั้น ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งกฎหมายแต่ละประเทศต่างให้คำจำกัดความของผู้ควบคุมข้อมูลส่วนบุคคลแตกต่างกันไป ดังนี้

- แนวปฏิบัติและข้อแนะนำขององค์การความร่วมมือทางเศรษฐกิจและการพัฒนาว่าด้วยการคุ้มครองความเป็นอยู่ส่วนตัวและการส่งโอนข้อมูลส่วนบุคคลข้ามประเทศ ค.ศ. 1980 (The Organization for Economic Cooperation and Development: OECD) ให้คำนิยามของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ไว้ว่า หมายถึง บุคคลผู้ซึ่งตามกฎหมายภายในมีอำนาจที่จะตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลหรือการใช้ข้อมูลส่วนบุคคล ไม่ว่าข้อมูลดังกล่าวจะถูกรวบรวม จัดเก็บ ประมวลผล หรือเผยแพร่โดยบุคคลดังกล่าวหรือตัวแทนซึ่งได้กระทำการในนามของบุคคลนั้น
- กฎเกณฑ์ของกลุ่มสหภาพยุโรป (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) ได้ให้คำนิยามของผู้ควบคุมข้อมูลไว้ว่า หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใดที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพังหรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป
- กฎเกณฑ์ของกลุ่มสหภาพยุโรปฉบับใหม่ (The General Data Protection Regulation: GDPR) ได้ให้คำนิยามของผู้ควบคุมข้อมูลส่วนบุคคลไว้เช่นเดียวกับกฎเกณฑ์ฉบับเดิมว่า หมายถึง บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใดที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพังหรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป

- แนวปฏิบัติและข้อแนะนำตามองค์กรความร่วมมือทางเศรษฐกิจในเอเชีย-แปซิฟิก (Asia-Pacific Economic Cooperation: APEC) ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ให้คำนิยามของผู้ควบคุมข้อมูล (Personal information controller) ไว้ว่า หมายถึง บุคคลหรือองค์กรผู้ซึ่งควบคุมการรวบรวม การครอบครอง การประมวลผลหรือการใช้ข้อมูลส่วนบุคคล รวมถึงบุคคลหรือองค์กรผู้ซึ่งออกคำสั่งแก่บุคคลอีกคนหนึ่งหรือองค์กรอีกองค์กรหนึ่งในการรวบรวม ครอบครอง ประมวลผล ใช้ โอนหรือเปิดเผยข้อมูลส่วนบุคคลในนามของตน ทั้งนี้ ไม่รวมถึงบุคคลหรือองค์กรผู้ซึ่งทำตามคำสั่งดังกล่าวโดยบุคคลหรือองค์กรอื่น และบุคคลธรรมดาที่เก็บรวบรวม ครอบครอง ประมวลผลหรือใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน ครอบครัวหรือเพื่อการใดๆ ภายในครอบครัวของตน
- มาตรา 3(7) แห่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเยอรมณี (BDSG)[33] ให้นิยามของผู้ควบคุมข้อมูลส่วนบุคคลไว้ว่า หมายถึง บุคคลธรรมดาหรือนิติบุคคลที่เก็บรวบรวม ประมวลผลหรือใช้ข้อมูลส่วนบุคคลในนามของตนเองหรือที่มอบหมายให้บุคคลอื่นดำเนินการแทน
- มาตรา 2(5) ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น[34] ให้นิยามของผู้ควบคุมข้อมูลส่วนบุคคล (business operator handling personal information) ไว้ว่า หมายถึง

---

[33] (7) “Controller” shall mean any person or body which collects, processes or uses personal data on his, her or its own behalf, or which commissions others to do the same.

[34] (5) The term "business operator handling personal information" as used in this Act means a business operator that has a personal information database etc. for business use; however, the following entities are excluded;

(i) national government organs;

(ii) local governments;

(iii) incorporated administrative agencies and other such entities (meaning independent administrative agencies and other such entities as provided in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); the same applies hereinafter);

(iv) local incorporated administrative agencies (meaning local incorporated administrative agencies as provided in Article 2, paragraph (1) of the Local

ผู้ประกอบการที่มีฐานข้อมูลส่วนบุคคลสำหรับใช้ในทางธุรกิจ แต่ไม่รวมถึง รัฐบาลกลาง รัฐบาลท้องถิ่น หน่วยงานอิสระของรัฐ เป็นต้น

- มาตรา 5 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ให้นิยามของผู้ควบคุมข้อมูลส่วนบุคคล ไว้ว่า หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ทั้งนี้ เมื่อพิจารณาบทนิยามของผู้ควบคุมข้อมูลตามกฎเกณฑ์ของสหภาพยุโรปทั้งฉบับเดิมและฉบับใหม่ จะพบว่ากฎเกณฑ์ดังกล่าวได้บัญญัติรองรับหลักการของผู้ควบคุมข้อมูลร่วมกัน (Joint Data Controller) ไว้ด้วย ซึ่งผู้ควบคุมข้อมูลร่วมกัน หมายถึง บุคคลธรรมดาหรือนิติบุคคลแยกต่างหากจากผู้ควบคุมข้อมูล โดยผู้ควบคุมข้อมูลร่วมกันดังกล่าวจะเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวร่วมกันกับผู้ควบคุมข้อมูล อย่างไรก็ตาม มิได้หมายความว่า ผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูลร่วมกันจะต้องคาดหวังสิ่งที่ได้รับจากการประมวลผลเหมือนกันจึงจะสามารถเป็นผู้ควบคุมข้อมูลร่วมกันได้ เนื่องจากสาระสำคัญของการเป็นผู้ควบคุมข้อมูลร่วมกัน ได้แก่ การกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลร่วมกันนั่นเอง

หลักการของผู้ควบคุมข้อมูลร่วมกันนี้เป็นหลักการที่ถูกกำหนดไว้ทั้งใน Directive 95/46/EC และ GDPR ของสหภาพยุโรปโดยมีจุดมุ่งหมายเพื่อเพิ่มความยืดหยุ่นและเพื่อรองรับกับเทคโนโลยีการประมวลผลที่เพิ่มความซับซ้อนมากกว่าในอดีต ตัวอย่างความสัมพันธ์ของผู้ควบคุมข้อมูลร่วมกันสำหรับกรณีทั่วไป ได้แก่ กรณีที่ธนาคารสหภาพยุโรปประสงค์จะใช้บริการระบบสื่อสารด้านการเงินระหว่างธนาคารผ่านระบบคอมพิวเตอร์ที่มีเครือข่ายเชื่อมโยงทั่วโลกที่ให้บริการโดย S.W.I.F.T (Society for Worldwide Interbank Financial Telecommunication) จึงว่าจ้าง S.W.I.F.T ซึ่งมีลักษณะเป็นผู้ประมวลผลในการจัดการโอนข้อมูลเกี่ยวกับธุรกรรมของธนาคาร แต่ S.W.I.F.T กลับเปิดเผยข้อมูลดังกล่าวที่จัดเก็บไว้ในระบบการประมวลผลในประเทศสหรัฐอเมริกาให้แก่หน่วยงานรัฐบาลของสหรัฐอเมริกาโดยปราศจากคำสั่งอย่างชัดแจ้งให้ดำเนินการเช่นว่านั้น กรณีจึงนำมาสู่การพิจารณาของคณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) ว่าการดำเนินการดังกล่าวชอบด้วยกฎหมายหรือไม่ ซึ่งจากการพิจารณาคณะกรรมการมีความเห็นว่าธนาคารสหภาพยุโรปและ S.W.I.F.T มีการดำเนินการเข้าลักษณะของผู้ควบคุมข้อมูลร่วมกันและต้องร่วมกันรับผิดต่อลูกค้าของธนาคารซึ่งเป็น

Incorporated Administrative Agencies Act (Act No. 118 of 2003); the same applies hereinafter);

เจ้าของข้อมูล ทั้งนี้ เนื่องจาก S.W.I.F.T เป็นผู้กำหนดหรือตัดสินใจการเปิดเผยข้อมูลดังกล่าวให้แก่หน่วยงานของสหรัฐอมเริกา อันเข้าลักษณะของการเป็นผู้ควบคุมข้อมูล ส่วนธนาคารสหภาพยุโรปก็ไม่สามารถตรวจตราผู้ประมวลผลได้ตามหน้าที่ภายใต้กฎหมาย ดังนั้นจึงต้องรับผิดในฐานะผู้ควบคุมข้อมูลด้วยเช่นกัน

ในมุมมองของคณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) ของสหภาพยุโรปที่มีความเห็นว่าผู้ใช้บริการระบบการประมวลผลแบบคลาวด์เป็นผู้ซึ่งทำหน้าที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลภายใต้ระบบการประมวลผลแบบคลาวด์ ดังนั้น ผู้ใช้บริการระบบการประมวลผลแบบคลาวด์จึงถือเป็นผู้ควบคุมข้อมูลที่จะปฏิบัติตามหน้าที่และความรับผิดภายใต้กฎเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ทั้งนี้ แม้ว่าผู้ใช้บริการจะกำหนดวัตถุประสงค์และวิธีการในการประมวลผลผ่านผู้ให้บริการระบบการประมวลผลแบบคลาวด์ก็ตาม ส่วนผู้ให้บริการระบบการประมวลผลแบบคลาวด์นั้นเป็นบุคคลที่ให้บริการระบบการประมวลผลแบบคลาวด์ในหลากหลายรูปแบบซึ่งเมื่อผู้ให้บริการระบบการประมวลผลแบบคลาวด์จัดเตรียมบริการของตนสำหรับการประมวลผลให้แก่ผู้ใช้บริการโดยหลักย่อมถือเป็นการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ใช้บริการและผู้ให้บริการย่อมถือเป็นผู้ประมวลผล มิใช่ผู้ควบคุมข้อมูล อย่างไรก็ตาม ผู้ให้บริการระบบการประมวลผลแบบคลาวด์อาจถือเป็นผู้ควบคุมข้อมูลร่วมกันกับผู้ใช้บริการได้เช่นเดียวกัน หากปรากฏข้อเท็จจริงว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประมวลผลข้อมูลดังกล่าวด้วยวิธีการและวัตถุประสงค์ที่ตกลงร่วมกันกับผู้ใช้บริการ แม้ว่าผู้ให้บริการจะมุ่งหวังสิ่งที่ได้จากการประมวลผลแตกต่างจากผู้ใช้บริการก็ตาม ตัวอย่างความสัมพันธ์ของผู้ควบคุมข้อมูลร่วมกันสำหรับกรณีการให้บริการระบบการประมวลผลแบบคลาวด์ ได้แก่ การให้บริการระบบการประมวลผลแบบคลาวด์ประเภท Public Software as a Service (SaaS) และ Public Platform as a Service ซึ่งแนวคิดที่พิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประเภท Public SaaS และ Public PaaS เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกันเกิดจากการพิจารณาของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส (Commission Nationale De l'informatique et des libertés: CNIL) ซึ่งได้ตีความไว้ว่า[35] ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ปรเภท Public SaaS และ Public

[35]Commission Nationale De l'informatique et des libertés, "Recommendations for companies planning to use Cloud Computing services," สืบค้นเมื่อวันที่ 17 เมษายน 2561, จาก https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

PaaS อยู่ในสถานะของ ‘ผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน หรือ Joint Controller’ เพราะผู้ให้บริการเป็นกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล จากการที่ผู้ให้บริการกำหนดข้อตกลงการใช้บริการหรือสัญญามาตรฐานในลักษณะที่ผู้ใช้บริการไม่มีอำนาจต่อรองและต้องยอมรับเสมอซึ่งจะส่งผลให้ผู้ใช้บริการไม่สามารถออกคำสั่งให้ผู้ให้บริการปฏิบัติตามความต้องการโดยเฉพาะของตนเองและไม่สามารถสอดส่องควบคุมความปลอดภัยของข้อมูลที่อยู่ในระบบการประมวลผลแบบคลาวด์ประเภทดังกล่าวได้ในทางปฏิบัติ ดังนั้น เมื่อผู้ให้บริการประเภท Public SaaS และ Public PaaS มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลแล้ว ผลที่ตามมาคือ ผู้ให้บริการรายดังกล่าวจะต้องตกลงขอบเขตหน้าที่ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศสกับผู้ใช้บริการซึ่งอยู่ในฐานะผู้ควบคุมข้อมูลไว้ในข้อตกลงการใช้บริการ ซึ่งหน่วยงาน CNIL ได้วางแนวปฏิบัติสำหรับขอบเขตหน้าที่และความรับผิดไว้ดังนี้

หน้าที่ตามกฎหมาย	บุคคลผู้รับผิดชอบ	หมายเหตุ
1. แจ้งการละเมิดข้อมูลส่วนบุคคลต่อ CNIL (Notification to CNIL)	ผู้ใช้บริการ	-
2. แจ้งข้อมูลให้เจ้าของข้อมูลทราบ (Information to data subject)	ผู้ใช้บริการ	แม้ว่าตามกฎหมายทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลจะมีหน้าที่นี้อยู่แล้ว แต่ CNIL แนะนำให้ผู้ให้บริการและผู้ใช้บริการตกลงให้ผู้ใช้บริการเป็นผู้รับผิดชอบ เพราะผู้ใช้บริการเป็นบุคคลที่ติดต่อกับเจ้าของข้อมูลโดยตรง แต่ผู้ให้บริการก็ต้องสนับสนุนข้อมูลที่ผู้ใช้บริการจะต้องแจ้งให้เจ้าของข้อมูลทราบด้วย
3. รักษาความปลอดภัยและความลับของข้อมูลส่วนบุคคล	ผู้ใช้บริการและผู้ให้บริการ	-
4. ปฏิบัติตามสิทธิของเจ้าของข้อมูล	ผู้ใช้บริการ	ผู้ให้บริการจะต้องให้ความช่วยเหลือผู้ใช้บริการเพื่อให้ผู้ใช้บริการสามารถปฏิบัติตามสิทธิของเจ้าของข้อมูลได้

สำหรับประเทศไทย เมื่อศึกษาเปรียบเทียบกับบทนิยามของผู้ควบคุมข้อมูลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) แล้วจะพบว่าร่างพระราชบัญญัติดังกล่าวยังไม่ปรากฏหลักการเรื่องผู้ควบคุมข้อมูลร่วมกันแต่อย่างใด ซึ่งผู้เขียนมองว่าหลักการของผู้ควบคุมข้อมูลร่วมกันนั้นถือเป็นหลักการสำคัญที่ควรบัญญัติไว้เพื่อรองรับกับการบังคับใช้กับการให้บริการระบบการประมวลแบบคลาวด์ มิเช่นนั้น กรณีย่อมอาจเกิดปัญหาในทางปฏิบัติว่าผู้ควบคุมข้อมูลร่วมกันดังกล่าวจะอยู่ในบังคับของร่างพระราชบัญญัติฉบับนี้หรือไม่ ทั้งนี้ เนื่องจากการให้บริการระบบการประมวลผลแบบคลาวด์มีลักษณะเป็นการให้บริการที่ทั้งผู้ให้บริการและผู้ใช้บริการสามารถมีลักษณะเป็นผู้ควบคุมข้อมูลร่วมกันได้ตามตัวอย่างข้างต้น

ข้อเสนอแนะ เพื่อให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีความชัดเจนและเหมาะสมกับสถานการณ์ของภาคธุรกิจในปัจจุบัน ผู้เขียนมีความเห็นว่าร่างพระราชบัญญัติดังกล่าวควรบัญญัติหลักการเรื่องผู้ควบคุมข้อมูลร่วมกันเพิ่มเติมก่อนการประกาศใช้บังคับ โดยการเพิ่มบทนิยามของผู้ควบคุมข้อมูลร่วมกันในมาตรา 6 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) และเพิ่มบทบัญญัติเกี่ยวกับหน้าที่ของผู้ควบคุมข้อมูลร่วมกันเป็นมาตรา 31/1 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ดังนี้

มาตรา 6 ในพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน หมายความว่า บุคคลหรือนิติบุคคลซึ่งกำหนดวิธีการและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลร่วมกับผู้อื่น

มาตรา 31/1

ในกรณีที่ผู้ควบคุมข้อมูลตั้งแต่ 2 รายขึ้นไปร่วมกันตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการของการประมวลผลข้อมูลส่วนบุคคล บุคคลดังกล่าวถือเป็นผู้ควบคุมข้อมูลร่วมกันและต้องกำหนดความรับผิดชอบในการปฏิบัติหน้าที่ตามที่พระราชบัญญัตินี้กำหนด

หากผู้ควบคุมข้อมูลส่วนบุคคลร่วมกันไม่ได้ดำเนินการตามวรรคแรก ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดแทน

5.3.2.3 หลักการเรื่องผู้ประมวลผลข้อมูล (Data Processor)

ภายใต้ระบบกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศนั้น บุคคลที่จะมีหน้าที่และความรับผิดตามกฎหมายนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจจะกำหนดไว้เพียงคนเดียว ได้แก่ ผู้ควบคุมข้อมูล หรือ จะกำหนดให้บุคคลใดๆ ที่เก็บรวบรวมหรือดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล จะต้องตกอยู่ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลก็ได้ ตัวอย่างเช่น Directive 95/46/EC ของสหภาพยุโรปที่แต่เดิมกำหนดให้เฉพาะผู้ควบคุมข้อมูลเท่านั้นที่จะมีหน้าที่และความรับผิดภายใต้กฎหมาย อย่างไรก็ตาม เมื่อ GDPR ยกร่างเสร็จ คณะทำงานหรือผู้ยกร่างก็ได้เพิ่มเติมหลักการว่าด้วยผู้ประมวลผลเข้าไปในร่างฉบับใหม่ โดยการกำหนดให้ผู้ประมวลผลสามารถเข้ามาทำหน้าที่ประมวลผลได้ภายใต้คำสั่งและการควบคุมดูแลของผู้ควบคุมข้อมูล ซึ่งเป็นไปในทิศทางเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี

แต่เดิมแม้ไม่ปรากฏหลักการว่าด้วยผู้ประมวลผลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่หากผู้ควบคุมข้อมูลมีความประสงค์จะให้บุคคลอื่นประมวลผลแทนตนเอง ผู้ควบคุมข้อมูลจะใช้วิธีเข้าทำสัญญาเป็นลายลักษณ์อักษรกับผู้ประมวลผลข้อมูลเพื่อที่ตกลงให้ผู้ประมวลผลข้อมูลจะต้องมีหน้าที่และความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับกับตนแทน ดังนั้น การที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลบัญญัติรับหลักการเรื่องผู้ประมวลผลไปบัญญัติไว้จึงเป็นเพียงการบัญญัติให้ชัดเจนขึ้นว่าผู้ประมวลผลจะต้องผูกพันตนโดยมีหน้าที่และความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น มิใช่เป็นการบัญญัติเพื่อรองรับหลักการใหม่แต่อย่างใด

เมื่อพิจารณาในบริบทของการให้บริการระบบการประมวลผลแบบคลาวด์ หลักการเรื่องผู้ประมวลผลข้อมูลก็มิใช่หลักการใหม่ในทางปฏิบัติเช่นเดียวกัน แต่อย่างไรก็ตาม หลักการว่าด้วยผู้ประมวลผลกลับถือเป็นหลักการสำคัญที่ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ให้ความสำคัญเป็นอย่างมาก ทั้งนี้ เนื่องจากแต่เดิมในทางปฏิบัติของประเทศในสหภาพยุโรปก่อนการยกร่างแก้ไขกฎหมายคุ้มครองส่วนบุคคลฉบับใหม่ได้เกิดปัญหาว่าด้วยเรื่องสถานะของผู้ประมวลผลแบบคลาวด์ขึ้น กล่าวคือ ผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีลักษณะเป็นผู้ควบคุมข้อมูล หรือเป็นผู้ประมวลผลข้อมูลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Directive 95/46/EC) เพราะหากผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีสถานะเป็นผู้ควบคุมข้อมูลแล้ว ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ย่อมมีหน้าที่และความรับผิดผูกพันตามกฎหมายว่าด้วย

การคุ้มครองข้อมูลส่วนบุคคลโดยตรง[36] ในทางกลับกันหากผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีสถานะเป็นเพียงผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ย่อมไม่มีหน้าที่และความรับผิดผูกพันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยตรง แต่อาจผูกพันตามสัญญาได้ หากข้อเท็จจริงปรากฏว่ามีการทำสัญญาดังกล่าวไว้ หรือหากปรากฏข้อเท็จจริงว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของตนเอง ซึ่งในทางปฏิบัตินั้นการพิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์เข้าลักษณะเป็นผู้ควบคุมข้อมูลหรือผู้ประมวลผลเป็นปัญหาที่ได้รับการวิพากษ์วิจารณ์อย่างกว้างขวางเพราะการพิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์จะอยู่ในสถานะของผู้ควบคุมข้อมูลหรือผู้ประมวลผลนั้นไม่ใช่เรื่องที่จะสามารถพิจารณาได้โดยง่าย ดังนั้น ผู้ให้บริการระบบการประมวลผลแบบคลาวด์จำนวนไม่น้อยจึงได้กำหนดข้อตกลงอย่างชัดแจ้งไว้ในสัญญาให้บริการระบบการประมวลผลแบบคลาวด์ว่าตนเองอยู่ในสถานะของผู้ประมวลผลข้อมูลส่วนบุคคลมิใช่ผู้ควบคุมข้อมูล โดยให้เหตุผลประกอบว่าการประมวลผลข้อมูลส่วนบุคคลของตนเป็นการดำเนินการตามคำสั่งหรือการตัดสินใจของลูกค้าซึ่งเป็นผู้ใช้บริการเท่านั้น และผู้ให้บริการบริการมิได้เก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น เป็นต้น[37] เพื่อให้ตนเองไม่มีภาระผูกพันตามหน้าที่และความรับผิดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นๆ ทั้งนี้ แม้ว่าการดำเนินการดังกล่าวจะทำให้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ไม่สามารถใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์หรือประโยชน์ของตนเองได้ก็ตาม[38]

---

[36] Article 3(1) of GDPR

The GDPR applies to the processing of personal data by a controller or a processor that falls within the scope of the GDPR (regardless of whether the relevant processing takes place in the EU or not).

[37] Akamai, Privacy Statement: "3. Akamai's processing of data is determined by ourbusiness customers. When processing data on behalf of business customers as an intermediaryservice provider, Akamai does not collect, use, or disclose personally identifiable consumer information, except as directed by Akamai's business customers..."

[38] Peter Carey, Data Protection A practical Guide to UK and EU Law, (Second Edition), (New York: Oxford University Press Inc., 2004), p.147.

เมื่อปัญหาเรื่องสถานะของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ส่งผลกระทบโดยตรงต่อการผูกพันตนภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้น คณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) ของสหภาพยุโรปจึงได้ออกความเห็นสำหรับการพิจารณาในประเด็นต่างๆ ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวเนื่องกับการให้บริการระบบการประมวลผลแบบคลาวด์ซึ่งรวมถึงประเด็นเรื่องสถานะของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ด้วย ภายใต้ความเห็นที่ 05/2012 เรื่องระบบการประมวลผลแบบคลาวด์นั้น คณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) มีความเห็นว่าผู้ใช้บริการระบบการประมวลผลแบบคลาวด์อยู่ในสถานะของผู้ควบคุมข้อมูล เนื่องจากเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลภายใต้ระบบการประมวลผลแบบคลาวด์ ในขณะที่ผู้ให้บริการระบบการประมวลผลแบบคลาวด์อยู่ในสถานะของผู้ประมวลผลข้อมูล เนื่องจากการประมวลผลของผู้ให้บริการนั้นเป็นการประมวลผลในนามของผู้ใช้บริการ ด้วยเหตุนี้ เพื่อให้ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ผูกพันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยตรงซึ่งจะช่วยเพิ่มประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลได้มากกว่าโดยเฉพาะอย่างยิ่งในกรณีที่ผู้ใช้บริการซึ่งอยู่ในสถานะของผู้ควบคุมข้อมูลนั้นเป็นบุคคลธรรมดา การเพิ่มบทบัญญัติว่าด้วยหน้าที่และความรับผิดของผู้ประมวลผลข้อมูลจึงเป็นสิ่งที่จำเป็นซึ่งนานาประเทศรวมถึงสหภาพยุโรปต่างให้ความสำคัญและรับหลักการเรื่องผู้ประมวลผลข้อมูลโดยผ่านทางการแก้ไขกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของตนเอง

สำหรับประเทศไทยเอง เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่าร่างพระราชบัญญัติดังกล่าวเพิ่งจะรองรับหลักการเรื่องผู้ประมวลผลข้อมูลส่วนบุคคล จากเดิมร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับก่อนๆ จะมีผลใช้บังคับแก่ผู้ควบคุมข้อมูลเท่านั้น ซึ่งสาเหตุที่ประเทศไทยกำหนดไว้ให้เฉพาะผู้ควบคุมข้อมูลเป็นผู้อยู่ภายใต้ร่างพระราชบัญญัติฉบับก่อนๆ นั้น รองศาสตราจารย์ ดร. กิตติศักดิ์ ปรกติ ได้ให้ความเห็นไว้ว่า[39] เนื่องจากประเทศไทยเกรงว่าหากกำหนดให้บุคคลที่เกี่ยวข้องในการเก็บรวบรวมหรือดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจะต้องอยู่ภายใต้ร่างพระราชบัญญัติดังกล่าวจะเป็นการสร้างภาระให้แก่ผู้ประกอบการมากจนเกินไป ดังนั้น ประเทศไทยจึงใช้วิธีการควบคุมผู้ควบคุมข้อมูลแทน อย่างไรก็ตาม การกำหนดเช่นว่านั้นย่อมทำให้สามารถตีความได้ว่าบุคคล

---

[39] เพลินตา ตันรังสรรค์, “โครงการเสวนาให้ความเห็นต่อร่างกฎหมาย เรื่อง “ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....,” จุลนิติ, ฉบับที่ 5, ปีที่ 7, น.77, (กันยายน – ตุลาคม 2553).

อื่นที่ไม่อยู่ในสถานะของผู้ควบคุมข้อมูลส่วนบุคคลจึงไม่อยู่ในบังคับของกฎหมายได้ กล่าวคือ บุคคลดังกล่าวสามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ตกอยู่ภายใต้ข้อจำกัดของกฎหมายที่กำหนดให้การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้เฉพาะกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูลและเป็นการเก็บรวบรวมภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายซึ่งเกี่ยวข้องโดยตรงกับกิจกรรมนั้นๆ และการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลดังกล่าวจะต้องเป็นการดำเนินการเท่าที่จำเป็นตามกรอบวัตถุประสงค์หรือเพื่อประโยชน์ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ในการเก็บรวบรวมเท่านั้น นอกจากนี้บุคคลซึ่งไม่ตกอยู่ภายใต้บังคับของกฎหมายยังสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศที่มีสาระสำคัญในหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยได้ ได้โดยไม่มีข้อจำกัดใดๆ

ด้วยเหตุนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จึงได้บัญญัติรองรับหลักการเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลไว้ ซึ่งการบัญญัติรองรับหลักการเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลนับว่าเป็นเรื่องที่สำคัญต่อการคุ้มครองข้อมูลส่วนบุคคลในบริบทของการให้บริการระบบการประมวลผลแบบคลาวด์โดยภาคเอกชนเป็นอย่างมาก โดยเฉพาะในช่วงเวลาที่ยังไม่ชัดเจนว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทยถือว่าอยู่ในสถานะใด เนื่องจากจากการศึกษาผู้เขียนพบว่า ในประเทศไทยยังไม่มีผู้ใดให้ความเห็นโดยชัดแจ้งว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์มีสถานะเป็นผู้ควบคุมข้อมูลหรือไม่ แต่อย่างไรก็ตาม เมื่อทำการศึกษาข้อตกลงการใช้บริการระบบการประมวลผลแบบคลาวด์ของผู้ให้บริการหลายราย อาทิ ไมโครซอฟต์ (Microsoft) เป็นต้น ผู้เขียนพบว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ได้กำหนดสถานะของตนเองไว้ในข้อตกลงการใช้บริการโดยระบุให้ผู้ใช้บริการเป็นผู้ควบคุมการเข้าถึงข้อมูล ดังนี้

“.... (iii) ผู้ใช้ ลูกค้าเป็นผู้ควบคุมการเข้าถึงโดยผู้ใช้และจะต้องรับผิดชอบในการใช้ผลิตภัณฑ์ของผู้ใช้ตามข้อตกลงนี้ ตัวอย่างเช่น ลูกค้าจะตรวจสอบให้แน่ใจว่าผู้ใช้ปฏิบัติตามนโยบายเรื่องการใช้อันเป็นที่ยอมรับ (Acceptable Use Policy)....”

ดังนั้น จากข้อตกลงดังกล่าวจึงอนุมานได้ว่า ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทยพิจารณาว่าตนเองอยู่ในสถานะของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งหากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) มีผลใช้บังคับ ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ก็จะมีหน้าที่และความรับผิดภายใต้ร่างพระราชบัญญัติดังกล่าว

อย่างไรก็ตาม เมื่อพิจารณารายละเอียดบทบัญญัติเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่าร่างพระราชบัญญัติดังกล่าวกำหนดรายละเอียดเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลไว้เพียง 3 มาตรา ได้แก่ มาตรา 6 ว่าด้วยบทนิยามของผู้ประมวลผลข้อมูลส่วนบุคคล มาตรา 30 ว่าด้วยหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล และมาตรา 72 ว่าด้วยความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งผู้เขียนมีความเห็นว่าบทบัญญัติเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติดังกล่าวยังไม่ครอบคลุมเมื่อเทียบกับหลักเกณฑ์ในระดับสากล โดยยังขาดสาระสำคัญในเรื่องดังต่อไปนี้

1. การกำหนดให้ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที
2. การกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถแต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งได้หากไม่มีกฎหมายกำหนดให้สามารถกระทำหรือหากไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล
3. การกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการที่รับผิดชอบโดยไม่ชักช้า เนื่องจากในทางปฏิบัติบุคคลที่จะทราบการละเมิดข้อมูลส่วนบุคคลก่อนผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ผู้ประมวลผลข้อมูล
4. การกำหนดให้ผู้ประมวลผลข้อมูลจะต้องปฏิบัติตามบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคลด้วย

ข้อเสนอแนะ ผู้เขียนมีความเห็นว่าหลักการเรื่องผู้ประมวลผลในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งสำคัญที่ผู้ร่างกฎหมายควรพิจารณาและให้ความสำคัญแม้ว่าการบัญญัติเช่นว่านั้นจะเป็นการสร้างภาระให้แก่ผู้ประกอบการก็ตาม เนื่องจากในปัจจุบันมีผู้ใช้บริการเป็นจำนวนมากไม่ว่าจะเป็นบุคคลธรรมดาหรือภาคธุรกิจที่ใช้บริการระบบการประมวลผลแบบคลาวด์ โดยเฉพาะอย่างยิ่งเมื่อผู้ใช้บริการระบบการประมวลผลแบบคลาวด์เป็นบุคคลธรรมดาซึ่งไม่มีอำนาจต่อรองกับผู้ให้บริการระบบบการประมวลผลแบบคลาวด์เพื่อจะกำหนดข้อสัญญาหรือข้อตกลงในการใช้บริการให้ผู้ให้บริการจะต้องผูกพันในการดำเนินการใดๆ กับข้อมูลส่วนบุคคลตามที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดไว้ได้ ดังนั้น หากในอนาคตร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) มีผลบังคับใช้เป็นกฎหมาย ผู้เขียนเห็นว่ากรณีอาจนำไปสู่ปัญหาที่เกี่ยวเนื่องกับการละเมิดข้อมูลส่วนบุคคลได้ในทางปฏิบัติและจำเป็นต้องแก้กฎหมายอีกครั้งในที่สุด ซึ่งจากประวัติศาสตร์ในการยกร่างกฎหมายของประเทศไทยที่ผ่านมา ความพยายามแก้ไขกฎหมายใน

ครั้งหนึ่งจำเป็นต้องใช้ระยะเวลาที่ค่อนข้างยาวนานกว่ากฎหมายนั้นๆ จะสามารถแก้ไขได้เป็นผลสำเร็จ ดังนั้น เพื่อให้การบังคับใช้กฎหมายสัมฤทธิ์ผลจึงควรมีการแก้ไขร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ให้มีหลักการเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลให้ครบถ้วนและสอดคล้องกับบริบทของการให้บริการระบบการประมวลผลแบบคลาวด์ก่อนที่จะมีการประกาศใช้บังคับเป็นกฎหมายอย่างเป็นทางการในราชกิจจานุเบกษา โดยการเพิ่มหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลข้างต้น เป็นอนุมตรา (4) ถึงอนุมาตรา (7) ในมาตรา 30 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ดังนี้

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

(4) แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที

(5) ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งโดยปราศจากกฎหมายกำหนดให้สามารถกระทำได้ หรือปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(7) ปฏิบัติตามบทบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

5.3.2.4 หลักการเรื่องสิทธิของเจ้าของข้อมูลในการโอนย้ายข้อมูลส่วนบุคคล (Data Portability)

สิทธิในการโอนย้ายข้อมูลเป็นสิทธิของเจ้าของข้อมูลที่เกิดขึ้นเป็นครั้งแรกเมื่อ GDPR มีผลใช้บังคับ โดยสิทธิในการโอนย้ายข้อมูลถูกกำหนดไว้ในมาตรา 20 ของ GDPR สิทธิในการโอนย้ายข้อมูลนี้เป็นสิทธิของเจ้าของข้อมูลที่ใกล้เคียงกับสิทธิในการเข้าถึงข้อมูล (Right to Access) เดิม แต่สิทธิเข้าถึงข้อมูลเดิมเจ้าของข้อมูลมักเกิดปัญหากับเจ้าของข้อมูลในทางปฏิบัติเนื่องจากรูปแบบของข้อมูลส่วนบุคคลที่เจ้าของข้อมูลจะเข้าถึงได้นั้นมักจะถูกกำหนดรูปแบบไว้โดยผู้ควบคุมข้อมูล ซึ่งก่อให้เกิดความไม่สะดวกในการเข้าถึงข้อมูลส่วนบุคคลดังกล่าว ดังนั้น สิทธิในการโอนย้ายข้อมูลจึงพัฒนาขึ้นโดยเปิดโอกาสให้เจ้าของข้อมูลสามารถรับสำเนาของข้อมูลส่วนบุคคลที่ตนได้ให้ไว้แก่ผู้ควบคุมข้อมูล หรือรับข้อมูลที่เกี่ยวข้องกับตนเอง แม้ว่าตนเองจะไม่ได้เป็นบุคคลที่ให้ข้อมูลดังกล่าวกับผู้ควบคุมข้อมูลก็ตาม โดยผู้ควบคุมข้อมูลต้องส่งมอบข้อมูลส่วนบุคคลในรูปแบบที่สามารถเปิดอ่านได้โดยง่าย นอกจากนี้ สิทธิประเภทนี้ยังเปิดโอกาสให้เจ้าของข้อมูลสามารถโอนย้ายข้อมูลส่วนบุคคลของตนที่ถูกจัดเก็บไว้ในระบบของผู้ควบคุมข้อมูลส่วนบุคคลรายหนึ่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่งได้ ทั้งนี้ สิทธิในการโอนย้ายข้อมูลตาม GDPR เกิดขึ้นโดยมีวัตถุประสงค์เพื่อให้อำนาจเจ้าของข้อมูลให้สามารถควบคุมข้อมูลส่วนบุคคลของตนที่ถูกจัดเก็บ รวบรวมหรือใช้โดยผู้ควบคุมข้อมูลให้มากขึ้น ซึ่งการให้สิทธินี้แก่เจ้าของข้อมูล คณะทำงานตามมาตรา 29 (Article 29 Data Protection Working Party) มองว่าสิทธิในการโอนย้ายข้อมูลนี้จะเป็นเครื่องมือสำคัญในการส่งเสริมให้เกิดตลาดดิจิทัลที่เป็นอันหนึ่งอันเดียวกันภายในสหภาพยุโรปและส่งเสริมให้เกิดการแข่งขันระหว่างผู้ให้บริการด้วยกันเอง ทั้งนี้ นอกจากเจ้าของข้อมูลมีสิทธิร้องขอสำเนาข้อมูลส่วนบุคคลและร้องขอให้มีการโอนย้ายข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลแล้ว เจ้าของข้อมูลยังมีสิทธิร้องขอตามสิทธิของตนข้างต้นต่องผู้ประมวลผลข้อมูลส่วนด้วย เนื่องจาก GDPR กำหนดให้ผู้ประมวลผลข้อมูลมีสิทธิและหน้าที่ในทำนองเดียวกับผู้ควบคุมข้อมูล

สิทธิในการโอนย้ายข้อมูลส่วนบุคคลถือเป็นสิทธิที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศควรให้ความสำคัญ โดยเฉพาะอย่างยิ่งในบริบทของการให้บริการระบบการประมวลผลแบบคลาวด์ เนื่องจากการให้สิทธิของ GDPR กำลังคำนึงถึงทางปฏิบัติของระบบการประมวลผลแบบคลาวด์ที่มีการแข่งขันสูงและผู้ใช้บริการควรจะมีสิทธิเลือกที่จะโอนย้ายข้อมูลของตนได้โดยไม่ต้องเริ่มให้ข้อมูลส่วนบุคคลของตนเองใหม่ เพราะในบางครั้งเมื่อผู้ใช้บริการใช้บริการระบบการประมวลผลแบบคลาวด์ไปชั่วระยะเวลาหนึ่ง ผู้ใช้บริการอาจเกิดความไม่ประทับใจในตัวผู้ให้บริการรายนั้นได้ ดังนั้น การให้ที่ GDPR ให้สิทธินี้แก่เจ้าของข้อมูลย่อมทำให้การใช้บริการระบบการประมวลผลแบบคลาวด์เกิดความต่อเนื่องในการใช้บริการด้วย

สำหรับประเทศไทย เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่าเจ้าของข้อมูลมีสิทธิเพียง 4 ประการภายใต้ร่างพระราชบัญญัติดังกล่าว ได้แก่ สิทธิเข้าถึงข้อมูล (Right to access) สิทธิในการลบ ทำลายหรือระงับการใช้ชั่วคราวหรือแปลงข้อมูล สิทธิในความถูกต้องหรือทันสมัยของข้อมูลส่วนบุคคล และสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ดังนั้น ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จึงยังไม่มีการบัญญัติรองรับสิทธิในการโอนย้ายข้อมูลแต่อย่างใด ทั้งที่สิทธิดังกล่าวถือเป็นสิ่งสำคัญที่เจ้าของข้อมูลควรได้รับเพื่อบริหารจัดการข้อมูลส่วนบุคคลของตนให้เกิดประโยชน์สูงสุด ดังนั้น ในปัจจุบันในการใช้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทย ผู้ใช้บริการจึงยังไม่สามารถโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ได้ สิ่งที่เจ้าของข้อมูลจะทำได้คือ การแจ้งให้ผู้ให้บริการรายเดิมลบข้อมูลส่วนบุคคลของตนเท่านั้น และไปเริ่มใช้บริการกับผู้ให้บริการรายใหม่แทน ซึ่งในการดำเนินการในลักษณะนี้ไม่เกิดประโยชน์ต่อทั้งผู้ใช้บริการและผู้ให้บริการระบบการประมวลผลแบบคลาวด์

แต่อย่างไรก็ตาม แม้ว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งจะเป็นกฎหมายหลักในการคุ้มครองข้อมูลส่วนบุคคลยังไม่ปรากฏหลักการเรื่องสิทธิในการโอนย้ายข้อมูลของเจ้าของข้อมูล แต่จากการศึกษาผู้เขียนพบว่าประเทศไทยมีความตื่นตัวกับสิทธิในการโอนย้ายข้อมูลของเจ้าของข้อมูลโดยมีความพยายามในการจะรองรับสิทธิส่วนนี้ให้แก่เจ้าของข้อมูลซึ่งนับว่าเป็นจุดเริ่มต้นที่ดีของประเทศไทย ทั้งนี้ ความพยายามในการจะรองรับสิทธิในการโอนย้ายข้อมูลให้แก่เจ้าของข้อมูล เกิดขึ้นจากแนวคิดของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“กลต.”) ที่จะแก้ไขหลักเกณฑ์ของตนเพื่อให้รองรับการโอนย้ายข้อมูลของลูกค้า ซึ่งแต่เดิมกลต. กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลลูกค้า (ได้แก่ ข้อมูลที่ลูกค้าได้ให้ไว้กับผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้าและข้อมูลที่เกิดจากการทำธุรกรรมของลูกค้ากับผู้ประกอบธุรกิจ) ไว้ให้ผู้ประกอบธุรกิจหลักทรัพย์จะต้องมีระบบการจัดการและจัดเก็บข้อมูล เอกสาร หรือหลักฐานเกี่ยวกับการประกอบธุรกิจให้ถูกต้อง ครบถ้วน ตรวจสอบได้ แต่กฎเกณฑ์ดังกล่าวยังขาดความชัดเจนในส่วนที่ผู้ประกอบธุรกิจต้องปฏิบัติตามการสั่งการของลูกค้าในการขอรับข้อมูลหรือให้โอนย้ายข้อมูลของตนไปยังบุคคลอื่น ดังนั้น กลต. จึงเห็นชอบในการแก้ไขกฎเกณฑ์ของตนเพื่อเป็นการคุ้มครองสิทธิของลูกค้า และกลต.ยังพิจารณาว่าสิทธิดังกล่าวช่วยลดภาระและต้นทุนให้กับทั้งลูกค้าและผู้ประกอบธุรกิจในการนำข้อมูลที่เคยให้ไว้แล้วในรูปแบบที่กำหนด เช่น ประวัติการซื้อขายหลักทรัพย์ เป็นต้น มาใช้ได้โดยไม่ต้องทำซ้ำอีก ทั้งนี้ สิทธิในการโอนย้ายข้อมูลของลูกค้าตามกฎเกณฑ์ที่จะแก้ไขของกลต. มีสาระสำคัญ ดังต่อไปนี้

(1) นิยามของข้อมูลของลูกค้า: ข้อมูลของลูกค้า หมายถึง ข้อมูลที่เกี่ยวข้องกับลูกค้าที่ได้ให้ไว้แก่ผู้ประกอบธุรกิจทั้งทางตรงและทางอ้อมที่สื่อความหมายถึงสิ่งเฉพาะตัวของลูกค้า เช่น ข้อมูลโปรไฟล์ลูกค้า (ชื่อ ที่อยู่ สถานที่ทำงาน เลขบัตรประจำตัวประชาชน ระดับการศึกษา) เอกสารประกอบการเปิดบัญชี ข้อมูลการทำความรู้จักลูกค้า เป็นต้น รวมถึงข้อมูลของลูกค้าที่เกี่ยวข้องกับการทำธุรกรรมกับผู้ประกอบธุรกิจ เช่น มูลค่าซื้อขายต่อปีย้อนหลัง ค่าคอมมิชชั่นที่จ่ายต่อปี ข้อมูลประวัติการกู้ยืมและชำระหนี้ เป็นต้น โดยไม่รวมถึงข้อมูลที่เกิดจากการที่ผู้ประกอบธุรกิจนำข้อมูลของลูกค้ามาทำการวิเคราะห์หรือวิจัย

(2) รูปแบบและวิธีการให้และโอนย้ายข้อมูล: ข้อมูลของลูกค้าที่ให้แก่ลูกค้าหรือโอนไปยังบุคคลอื่นตามความประสงค์ของลูกค้าจะต้องอยู่ในรูปแบบ commonly readable format โดยสามารถนำไปใช้ต่อได้ (Support re-use) เว้นแต่ลูกค้าจะได้แจ้งความประสงค์ไว้เป็นอย่างอื่น โดยผู้ประกอบธุรกิจจะต้องระบุเวลาของข้อมูลดังกล่าวเอาไว้ด้วย

(3) การยืนยันตัวตนของลูกค้า: ผู้ประกอบธุรกิจต้องจัดให้มีการยืนยันตัวตนของลูกค้าที่แสดงความประสงค์ในการขอรับข้อมูลของตนหรือขอโอนย้ายข้อมูลไปยังบุคคลอื่นตามความประสงค์ของลูกค้า เพื่อพิสูจน์ว่าผู้แสดงความประสงค์จะขอโอนย้ายข้อมูลนั้นเป็นเจ้าของข้อมูลที่แท้จริง

(4) หน้าที่ของผู้ประกอบธุรกิจเพื่อรองรับการให้และโอนย้ายข้อมูล: ผู้ประกอบธุรกิจจะต้องมีระบบงานที่เกี่ยวกับการให้ข้อมูลแก่ลูกค้าและการโอนย้ายข้อมูลไปยังบุคคลอื่นตามความประสงค์ของลูกค้า โดยระบบดังกล่าวจะต้องมีความปลอดภัยอย่างเพียงพอ และสามารถตรวจสอบการทำงานได้ นอกจากนี้ ผู้ประกอบธุรกิจต้องกำหนดหลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับการให้ข้อมูลแก่ลูกค้าและการโอนย้ายข้อมูลไปยังบุคคลอื่นตามความประสงค์ของลูกค้าไว้เป็นลายลักษณ์ด้วย ทั้งนี้ หลักเกณฑ์ดังกล่าวควรกำหนดรายละเอียดอย่างน้อยดังต่อไปนี้

- รายละเอียดเกี่ยวกับการแสดงความประสงค์ของลูกค้า
- การยืนยันตัวตนของลูกค้า เช่น ขั้นตอนการยืนยันตัวตน เอกสารที่เกี่ยวข้อง เป็นต้น
- ระยะเวลาในการให้ข้อมูลและโอนย้ายข้อมูลกรณีลูกค้าที่ยังเปิดบัญชีอยู่และกรณีลูกค้าที่ปิดบัญชีแล้ว
- การคิดค่าธรรมเนียม เป็นต้น

เมื่อผู้ประกอบธุรกิจกำหนดหลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับการให้ข้อมูลแก่ลูกค้าแล้ว ผู้ประกอบธุรกิจควรต้องแจ้งหลักเกณฑ์และวิธีปฏิบัติดังกล่าวให้ลูกค้าทราบด้วย เพื่อให้ลูกค้าสามารถใช้สิทธิของตนได้อย่างมีประสิทธิภาพ

อนึ่ง แม้ว่ากลต.จะมีความพยายามในการรองรับสิทธิของเจ้าของข้อมูลประเภทนี้ แต่อย่างไรก็ตาม กฎเกณฑ์ที่แก้ไขเพื่อให้รองรับสิทธิในการโอนย้ายข้อมูลนี้ยังไม่มีผลบังคับใช้ในปัจจุบัน เนื่องจากยังอยู่ในขั้นตอนของการรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้อง โดยกลต. ได้เผยแพร่เอกสารประกอบการรับฟังความคิดเห็นเลขที่ อนธ.15/2560 สู่สาธารณะเมื่อวันที่ 8 มิถุนายน 2560 และคาดว่าจะมีผลใช้บังคับในเร็ววันนี้

ข้อเสนอแนะ นับว่าความพยายามของกลต. เป็นจุดเริ่มต้นที่ดีที่จะทำให้ผู้เกี่ยวข้องตระหนักถึงความสำคัญของสิทธิของเจ้าของข้อมูลในการโอนย้ายข้อมูลส่วนบุคคลของตน ดังนั้น ผู้เขียนมีความเห็นว่า ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งจะมีผลเป็นกฎหมายหลักในการคุ้มครองข้อมูลส่วนบุคคล ก็ควรจะพิจารณาบัญญัติรับรองสิทธิประเภทนี้ด้วยเช่นกัน เนื่องจากการบัญญัติรับรองสิทธิประเภทนี้ย่อมก่อให้เกิดประโยชน์แก่ทั้งลูกค้าหรือผู้ใช้บริการและผู้ให้บริการในการประกอบธุรกิจทั้งภายในและภายนอกประเทศ ตลอดจนยังช่วยส่งเสริมการให้บริการระบบการประมวลผลแบบคลาวด์ในประเทศไทย โดยเพิ่มมาตรา 28/1 ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพื่อรองรับสิทธิของเจ้าของข้อมูล และแก้ไขเพิ่มเติมบทบัญญัติในมาตรา 29 (5) และมาตรา 30 (8) เพื่อเพิ่มหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลให้ต้องปฏิบัติตามสิทธิที่เจ้าของข้อมูลมีอยู่ ดังนี้

มาตรา 28/1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับข้อมูลส่วนบุคคลเกี่ยวกับตนที่ได้มอบความยินยอมให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในรูปแบบที่ใช้กันอยู่ทั่วไปและเข้าใจง่าย และมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลโอนย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลอีกรายหนึ่งได้โดยปราศจากอุปสรรคใดๆ

ในการใช้สิทธิตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจร้องขอให้เจ้าของข้อมูลส่วนบุคคลพิสูจน์ว่าตนเองเป็นเจ้าของข้อมูลที่แท้จริงได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอเช่นว่านั้นได้ หากการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลไม่สามารถกระทำได้โดยง่ายในทางเทคนิค หรือ การดำเนินการเช่นว่านั้นอาจทำให้กระทบต่อสิทธิและเสรีภาพของบุคคลอื่น

มาตรา 29 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ

(2) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(4) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 27 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(5) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

(4) แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที

(5) ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งโดยปราศจากกฎหมายกำหนดให้สามารถกระทำได้ หรือปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิด

ข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(7) ปฏิบัติตามบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

(8) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

หมายเหตุ: ในทางปฏิบัติข้อมูลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์มีทั้งข้อมูลที่เป็นข้อมูลส่วนบุคคลและที่ไม่ใช่ข้อมูลส่วนบุคคล สำหรับข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคลและถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ ผู้เขียนมีความเห็นว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ควรดำเนินการโอนย้ายเช่นเดียวกับข้อมูลส่วนบุคคลด้วย แม้ว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้จะไม่ได้กำหนดไว้ (เนื่องจากข้อมูลที่จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติฉบับนี้ ได้แก่ ข้อมูลส่วนบุคคล เท่านั้น) และในทางปฏิบัติการโอนย้ายข้อมูลทั้งหมดย่อมสะดวกต่อผู้ให้บริการระบบการประมวลผลแบบคลาวด์มากกว่าการแยกประเภทว่าข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลหรือไม่ ซึ่งหากในอนาคตประเทศไทยออกกฎหมายเกี่ยวกับการคุ้มครองข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล ดังที่สหภาพยุโรปกำลังยกร่าง A framework for the free flow of non-personal data in the EU อยู่นั้น กฎหมายดังกล่าวควรระบุหน้าที่ในการโอนย้ายนี้ไว้ในกฎหมายดังกล่าวด้วย

5.3.2.5 หลักการเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่งหรือโอนข้อมูลส่วนบุคคลถือเป็นเรื่องที่สำคัญที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลหลายประเทศให้ความเป็นสำคัญเป็นอย่างมาก เนื่องจากเทคโนโลยีปัจจุบันทำให้การส่งหรือโอนข้อมูลส่วนบุคคลไปยังแหล่งจัดเก็บข้อมูลหรือดาต้าเซ็นเตอร์ในต่างประเทศเกิดขึ้นมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งในระบบการประมวลผลแบบคลาวด์ที่ผู้ใช้บริการสามารถเรียกใช้ข้อมูลของตนโดยผ่านเครือข่ายไร้สายโดยข้อมูลดังกล่าวอาจจะถูกจัดเก็บไว้ในดาต้าเซ็นเตอร์หลายแห่งบนโลกนี้ เมื่อมีคำสั่งเรียกใช้งานข้อมูลดังกล่าว ข้อมูลก็สามารถวิ่งข้ามพรหมแดนของแต่ละประเทศได้อย่างรวดเร็ว ดังนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงจำเป็นต้องเข้ามาควบคุมการส่งหรือโอนข้อมูลระหว่างประเทศอย่างเคร่งครัด

เมื่อพิจารณาหลักเกณฑ์ว่าด้วยการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศของ GDPR จะพบว่าหลักเกณฑ์ดังกล่าวถูกกำหนดไว้ในมาตรา 44 และมาตรา 45 ของ GDPR โดยมีหลักการสำคัญ คือ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรป โดยหลักย่อมถือว่าเป็นการกระทำที่ต้องห้าม อย่างไรก็ตาม GDPR เปิดช่องให้การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรปสามารถเกิดขึ้นได้หากประเทศที่รับโอนข้อมูลนั้นมีกฎหมายให้

ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (Adequate level) ทั้งนี้ ในปัจจุบันประเทศที่ได้รับการพิจารณาว่ามีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ ได้แก่ ประเทศแคนาดา อาร์เจนตินา อิสลาเอล สวิตเซอร์แลนด์ นิวซีแลนด์ อุรุกวัย เป็นต้น อย่างไรก็ตาม หากประเทศที่รับโอนข้อมูลไม่เข้าข่ายเป็นประเทศที่ได้รับพิจารณาข้างต้น ผู้ส่งหรือโอนข้อมูลส่วนบุคคลยังสามารถโอนข้อมูลส่วนบุคคลไปยังประเทศดังกล่าวได้ภายใต้เงื่อนไขที่จำกัด คือ ผู้ส่งหรือโอนข้อมูลส่วนบุคคจะต้องมีมาตรรักษาความปลอดภัยที่เหมาะสม (Appropriate safeguard) เช่น การมีมาตรฐานหรือหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules: BCRs) ซึ่งได้รับการอนุมัติจากหน่วยงานคุ้มครองข้อมูลส่วนบุคคล Supervisory Authority) ด้วย โดยเป็นการอนุมัติเพียงครั้งเดียวสำหรับการส่งหรือโอนข้อมูลระหว่างบริษัทในเครือในอนาคตโดยไม่ต้องขออนุมัติอีก สำหรับกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือซึ่งตั้งอยู่ในประเทศนอกสหภาพยุโรป หรือกรณีมีเหตุการณ์พิเศษให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลสามารถส่งหรือโอนข้อมูลส่วนบุคคลได้ตามมาตรา 49 เช่น เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมแม้ได้รับแจ้งว่าประเทศปลายทางไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอและไม่มีมาตรรักษาความปลอดภัยที่เหมาะสม เป็นต้น

สำหรับประเทศไทย มาตรา 25 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดให้การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศสามารถกระทำได้โดยประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด ซึ่งคงต้องรอพิจารณาต่อไปว่าคณะกรรมการจะประกาศหลักเกณฑ์ใดออกมาให้ผู้ควบคุมข้อมูลต้องปฏิบัติตาม

อย่างไรก็ตาม มาตรา 25 ของร่างพระราชบัญญัติดังกล่าวยังกำหนดข้อยกเว้นให้การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศสามารถเกิดขึ้นได้โดยไม่มีเงื่อนไข หากเป็นกรณีดังต่อไปนี้

- เป็นการปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล
- เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้ หรือ
- กรณีอื่นๆ ตามที่กำหนดในกฎกระทรวง

อนึ่ง แม้ว่ามาตราดังกล่าวจะกำหนดข้อยกเว้นของการส่งหรือโอนข้อมูลส่วนบุคคล ซึ่งจะช่วยเพิ่มข้อยืดหยุ่นในการส่งหรือโอนข้อมูลส่วนบุคคลแล้วก็ตาม แต่ผู้เขียนพิจารณาแล้วเห็นว่าในทางปฏิบัติของระบบการประมวลผลแบบคลาวด์ ข้อยกเว้นดังกล่าวยังไม่รองรับกับสถานการณ์การให้บริการในปัจจุบันที่ผู้ให้บริการหลายรายมีบริษัทในเครือเป็นจำนวนมากซึ่งถือครองดาต้าเซ็นเตอร์ในแต่ละประเทศ ทำให้ต้องมีการส่งหรือโอนข้อมูลไปมาเป็นจำนวนมาก

<u>ข้อเสนอแนะ</u>: เพื่อให้เกิดความคล่องตัวในการจัดเก็บข้อมูลไว้ในดาต้าเซ็นเตอร์ในแต่ละประเทศ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรเพิ่มข้อยกเว้นสำหรับบริษัทในเครือในลักษณะเดียวกันกับ GDPR คือ ถ้าหากเป็นการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากคณะกรรมการแล้ว ให้การส่งหรือโอนข้อมูลส่วนบุคคลนั้นสามารถกระทำได้โดยอัตโนมัติ โดยการแก้ไขเพิ่มเติมมาตรา 25 (5) ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ดังนี้

> มาตรา 25 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 14 (5) เว้นแต่
>
> (1) เป็นการปฏิบัติตามกฎหมาย
>
> (2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
>
> (3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล
>
> (4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้
>
> <u>(5) เป็นการโอนข้อมูลระหว่างบริษัทในเครือซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรที่ได้รับอนุมัติจากคณะกรรมการ</u>
>
> (6) กรณีอื่นตามที่กำหนดในกฎกระทรวง

<u>หมายเหตุ:</u> ในทางปฏิบัติข้อมูลที่ถูกส่งหรือโอนไปย่อมมีทั้งข้อมูลที่เป็นข้อมูลส่วนบุคคลและไม่ใช่ข้อมูลส่วนบุคคล สำหรับข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคลและถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์นั้น ไม่อยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้การศึกษาในครั้งนี้ อย่างไรก็ตาม ผู้เขียนมีความเห็นว่าในปัจจุบันผู้ให้บริการระบบการประมวลผลแบบคลาวด์สามารถ

ส่งหรือโอนได้โดยอิสระ (โดยผู้ให้บริการอาจตกลงกับผู้ใช้บริการสำหรับการส่งหรือโอนตั้งแต่ต้น) เนื่องจากปัจจุบันยังไม่มีกฎหมายใช้บังคับใช้ส่วนนี้ แต่หากในอนาคตประเทศไทยจะออกกฎหมายเกี่ยวกับการคุ้มครองข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล ดังที่สหภาพยุโรปกำลังยกร่าง A framework for the free flow of non-personal data in the EU อยู่นั้น กฎหมายดังกล่าวก็ควรกำหนดถึงการส่งหรือโอนข้อมูลส่วนนี้ โดยจะต้องสนับสนุนการส่งหรือโอนข้อมูลในระบบการประมวลผลแบบคลาวด์ด้วย

5.3.2.6 การกำหนดโทษภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตาม GDPR บุคคลดังกล่าวต้องระวางโทษปรับทางปกครอง (Administrative penalty) 10 ล้านยูโรหรือ 2% ของรายได้ทั่วโลก (กรณีเป็นความผิดที่ไม่กระทบสิทธิของเจ้าของข้อมูลอย่างร้ายแรง) และระวางโทษปรับ 20 ล้านยูโรหรือ 4% ของรายได้ทั่วโลก (กรณีเป็นความผิดที่กระทบสิทธิของเจ้าของข้อมูลอย่างร้ายแรง) โดยไม่มีโทษทางอาญา ยกเว้นบางประเทศจะบทบัญญัติโทษทางอาญาเพิ่มเติมจากที่ GDPR กำหนดไว้ เช่น ประเทศเยอรมนี เป็นต้น

เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) นั้น จะพบว่าร่างพระราชบัญญัติดังกล่าว กำหนดทั้งความรับผิดทางแพ่ง โทษทางอาญาและโทษปรับทางปกครองไว้ ดังนี้

<u>ความรับผิดทางแพ่ง</u>

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดโทษทางแพ่งไว้สำหรับผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนหากปรากฏการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลนั้น ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลหรือไม่ก็ตาม อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ต้องรับผิดหากพิสูจน์ได้ว่าความเสียหายดังกล่าวเกิดจากเหตุสุดวิสัย การกระทำตามคำสั่งของเจ้าหน้าที่ เป็นต้น

<u>โทษทางอาญา</u>

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดโทษทางอาญาไว้ในกรณีดังต่อไปนี้

(1) ผู้ควบคุมข้อมูลส่วนบุคคลใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดที่กระทบความรู้ของประชาชน เพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น หรือโดยประการที่น่าจะทำให้ผู้อื่นนั้นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย จะต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

(2) ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

กรณีที่ผู้กระทำความผิดเป็นนิติบุคคล หากการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการแต่ละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลกระทำความผิด กรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลต้องระวางโทษในความผิดนั้นๆ ด้วย

<u>โทษปรับทางปกครอง</u>

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดโทษปรับทางปกครอง ดังนี้

(1) กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่แจ้งรายละเอียดที่ต้องแจ้งให้เจ้าของข้อมูลทราบ (มาตรา 20) ไม่ดำเนินการตามคำขอของเจ้าของข้อมูลเกี่ยวกับสิทธิเข้าถึงหรือให้เปิดเผยการได้มาซึ่งเจ้าของข้อมูลไม่ยินยอม (มาตรา 26 วรรค 4) ไม่จัดทำบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ (มาตรา 31) และไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการฯ กำหนด (มาตรา 17) ต้องระวางโทษปรับทางปกครองไม่เกิน 100,000 บาท

(2) กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่เก็บรวบรวมข้อมูลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (มาตรา 19) ทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล (มาตรา 21) เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง (มาตร 22) เปิดเผยหรือใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล (มาตรา 24) ไม่ปฏิบัติตามหลักเกณฑ์การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (มาตรา 25) ไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ในมาตรา 29 ขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือกรณีผู้ประมวลข้อมูลส่วน

บุคคลไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ในร่างพระราชบัญญัตินี้ ต้องระวางโทษปรับไม่เกิน 300,000 บาท

(3) กรณีผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนเก็บรวบรวม ใช้ หรือเปิดเผยโอนไปยังต่างประเทศซึ่งข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการกำหนดโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

เมื่อพิจารณาโทษตามร่างพระราชบัญญัติข้างต้น ผู้เขียนมีความเห็นดังต่อไปนี้

<u>ความรับผิดทางแพ่ง:</u> ผู้เขียนมีความเห็นว่าร่างพระราชบัญญัตินี้กำหนดโทษทางแพ่งไว้เฉพาะกรณีของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น แต่ในทางปฏิบัติย่อมมีโอกาสที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลได้ ดังนั้น เพื่อเป็นการคุ้มครองเจ้าของข้อมูลให้สามารถฟ้องร้องผู้ประมวลผลข้อมูลส่วนบุคคลได้โดยตรงและเพื่อให้ร่างพระราชบัญญัติฉบับนี้เกิดความสมบูรณ์ ผู้เขียนเสนอแนะให้แก้ไขมาตรา 64 โดยเพิ่มให้ผู้ประมวลผลต้องมีความรับผิดทางแพ่งด้วย ดังนี้

มาตรา 64 ผู้ควบคุมข้อมูลส่วนบุคคล <u>ผู้ประมวลผลข้อมูลส่วนบุคคล</u>ซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคล <u>ของผู้ประมวลผลข้อมูลส่วนบุคคล</u>หรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล <u>ผู้ประมวลผลข้อมูลส่วนบุคคล</u> นั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(3) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 14(6)

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

โทษทางอาญา: โทษทางอาญาที่กำหนดไว้ในมาตรา 65 และมาตรา 66 เป็นความผิดที่มีลักษณะใกล้เคียงกับกฎหมายอาญาในความผิดฐานหมิ่นประมาท (มาตรา 326) และความผิดฐานต่อสู้ขัดขวางเจ้าพนักงาน (มาตรา 138) ซึ่งผู้เขียนมีความเห็นว่าการกำหนดโทษนี้ไม่กระทบต่อหลักการคุ้มครองข้อมูลส่วนบุคคลในระดับสากล ในทางกลับกัน การกำหนดโทษเช่นว่านี้ยิ่งเป็นการคุ้มครองข้อมูลส่วนบุคคลประเภทพิเศษ คือ ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศานาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพหรือข้อมูลอื่นใดที่กระทบความรู้สึกประชาชนได้ดียิ่งขึ้น

อย่างไรก็ตาม สำหรับการกำหนดให้กรรมการต้องรับผิดกรณีที่ผู้กระทำความผิดเป็นนิติบุคคลในมาตรา 67 นั้น ผู้เขียนมีความเห็นว่า หากการกำหนดให้กรรมการต้องรับผิดเป็นไปเพื่อให้กรรมการให้ความสำคัญแก่การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว การเพิ่มโทษปรับทางปกครอง น่าจะเป็นสิ่งที่นิติบุคคลให้ความสำคัญมากยิ่งกว่า ยิ่งกำหนดโทษปรับทางปกครองไว้สูงมากเท่าไร นิติบุคคลก็จะยิ่งให้ความสำคัญกับการปฏิบัติตามกฎหมายมากยิ่งขึ้น อย่างเช่นในกรณีของ GDPR ที่กำหนดโทษปรับไว้สูง ผู้ประกอบการในประเทศต่างๆ ทั่วโลกจึงให้ความสำคัญในการปฏิบัติตาม GDPR ซึ่งหากบริษัทถูกบังคับโทษปรับทางปกครองไว้สูงแล้ว การบังคับโทษดังกล่าวย่อมส่งผลกระทบโดยตรงต่อการบริหารงานของกรรมการและความเชื่อมั่นของผู้ถือหุ้นต่อกรรมการ ซึ่งย่อมไม่ใช่สิ่งที่กรรมการปรารถนาให้เกิดขึ้น ดังนั้น ผู้เขียนเสนอแนะให้ตัดมาตรา 67 ออกจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) และเป็นเพิ่มโทษปรับทางปกครองให้สูงขึ้นแทน

โทษปรับทางปกครอง: ผู้เขียนมีความเห็นว่าการที่ร่างพระราชบัญญัติฉบับนี้กำหนดโทษปรับทางปกครองแทนโทษปรับทางอาญาเป็นสิ่งที่สมควรและสอดคล้องกับแนวทางสากล ได้แก่ GDPR ทั้งนี้ เนื่องจากโทษปรับทางปกครองทำให้กระบวนการเยียวยาเจ้าของข้อมูลส่วนบุคคลเกิดขึ้นได้อย่างรวดเร็ว เพราะโทษทางปกครองไม่จำเป็นต้องคำนึงถึงองค์ประกอบภายในของการกระทำความผิด ได้แก่ เจตนาหรือประมาท ดังเช่นกรณีโทษทางอาญา อย่างไรก็ตาม เมื่อพิจารณาจำนวนโทษปรับทางปกครอง ผู้เขียนกลับมีความเห็นว่าจำนวนโทษปรับทางปกครองที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้กำหนดไว้จำนวนนั้นยังไม่เพียงพอที่จะทำให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลเกรงกลัวและปฏิบัติตามบทบัญญัติแห่งกฎหมายนี้อย่างเคร่งครัด ซึ่งจะเป็นผลเสียต่อเจ้าของข้อมูลส่วนบุคคล กล่าวคือ เจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับความคุ้มครองเท่าที่ควรจะเป็น ดังนั้น ผู้เขียนเสนอแนะให้แก้ไขจำนวนโทษปรับทางปกครองของมาตรา 69 ถึงมาตรา 75 โดยเทียบเคียงกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับรับฟังความคิดเห็น) และ GDPR ดังนี้

มาตรา 69 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 20 มาตรา 26 วรรคสี่ มาตรา 31 หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 17 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 17 วรรคห้า ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 70 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ต้องระวางโทษปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 71 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 หรือฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 72 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 30 โดยไม่มีเหตุอันควร ต้องระวางโทษปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 73 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 62 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 63 วรรคสาม ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 74 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนหบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

5.3.2.7 การมีผลใช้บังคับย้อนหลังของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

มาตรา 2 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดให้ร่างพระราชบัญญัตินี้มีผลใช้บังคับเมื่อพ้นกำหนดระยะเวลา 1 ปี นับแต่วันประกาศในราชกิจจานุกเบกษาเป็นต้นไป ยกเว้นบทบัญญัติเกี่ยวกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่เก็บไว้ก่อนร่างพระราชบัญญัติมีผลใช้บังคับ ให้สามารถมีผลใช้บังคับทันทีนับจากวันถัดจากวันที่ประกาศในราชกิจจานุเบกษา

สำหรับบทบัญญัติเกี่ยวกับข้อมูลส่วนบุคคลที่เก็บไว้ก่อนร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) มีผลใช้บังคับนั้น ร่างพระราชบัญญัติดังกล่าวกำหนดไว้ในมาตรา 83 ดังนี้

(1) <u>การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล</u>: ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามกรอบวัตถุประสงค์ที่กำหนดไว้แต่เดิม แต่ผู้ควบคุมข้อมูลส่วนบุคคลต้องเปิดโอกาสให้เจ้าของข้อมูลสามารถยกเลิกความยินยอมที่ได้ให้ไว้ก่อนร่างพระราชบัญญัติมีผลใช้บังคับได้ โดยกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์จะให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลทราบ ทั้งนี้ การแจ้งยกเลิกความยินยอมจะต้องทำได้โดยง่ายด้วย

(2) <u>การเปิดเผยและการดำเนินการอื่นนอกเหนือจากการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล</u>: ผู้ควบคุมข้อมูลต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ กล่าวคือ ต้องดำเนินการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลใหม่ก่อน

เมื่อร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดไว้เช่นนี้ กรณีจึงมีประเด็นต้องพิจารณาว่าร่างพระราชบัญญัติฉบับนี้ควรกำหนดให้ทุกกรณีต้องขอความยินยอมใหม่หรือไม่ ซึ่งในประเด็นนี้ผู้เขียนมีความเห็นดังนี้

<u>ความเห็นต่อการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามมาตรา 83 วรรคหนึ่ง ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)</u>

แม้ว่าประเทศไทยจะไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้กับภาคเอกชนในลักษณะกฎหมายกลางมาก่อน แต่ก็มิได้หมายความว่าประเทศไทยไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกเหนือจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ประเทศไทยยังมีกฎหมายเฉพาะที่บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจำนวนหลายฉบับ ยกตัวอย่างเช่น

(ก) พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติฉบับนี้ให้ความคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับสินเชื่อของผู้ขอสินเชื่อจากสถานบันการเงินเท่านั้น ไม่รวมถึงข้อมูลส่วนบุคคลประเภทอื่นๆ ซึ่งภายใต้กฎหมายฉบับนี้ข้อมูลส่วนบุคคลของผู้ขอสินเชื่อ หมายถึง ข้อมูลที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ ซึ่งในกรณีของบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพ การสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประจำตัวเจ้าหน้าที่ของรัฐ หนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี) ตลอดจนประวัติการขอและการได้รับอนุมัติสินเชื่อและการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อ รวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

พระราชบัญญัติฉบับนี้ใช้บังคับกับบริษัทข้อมูลเครดิตที่ได้รับอนุญาต ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล โดยหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ได้แก่

- กำหนดหลักเกณฑ์ วิธีการและเงื่อนไขเกี่ยวกับระบบในการเก็บรวบรวม การบันทึก การเรียบเรียง การเก็บรักษา การแก้ไขข้อมูล การนำกลับมา การใช้ การเปิดเผย การพิมพ์ การทำให้เข้าถึง การลบ การทำลายข้อมูลเครดิต (“ประมวลผลข้อมูล”)
- บัญญัติห้ามจัดเก็บข้อมูลที่ไม่เกี่ยวกับการรับบริการหรือการขอสินเชื่อหรือข้อมูลบางอย่างโดยชัดแจ้ง และห้ามประมวลผลข้อมูลที่มีอายุเกินกว่าที่คณะกรรมการกำหนด
- ให้มีระบบรักษาความลับ ความปลอดภัย เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์ หรือป้องกันการแก้ไข ทำให้เสียหาย การเปิดเผยต่อบุคคลอื่นโดยไม่ได้รับอนุญาต
- ผู้ประกอบการต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลหากมีการใช้หรือการเปิดเผย ยกเว้นการเปิดเผยบางประการที่กฎหมายยกเว้นให้ไม่ต้องได้รับความยินยอม และการเปิดเผยดังกล่าว ผู้ประกอบการต้องแจ้งเป็นหนังสือให้เจ้าของข้อมูลทราบถึงการเปิดเผยดังกล่าวภายใน 30 วัน นับแต่วันที่เปิดเผยข้อมูล

(ข) พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

มาตรา 50 ของพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 กำหนดให้คณะกรรมการกิจการโทรคมนาคมแห่งชาติกำหนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม ซึ่งเมื่อวันที่ 16 สิงหาคม 2549 คณะกรรมการกิจการโทรคมนาคมแห่งชาติได้ออกประกาศตามมาตรา 50 โดยให้นิยามของข้อมูลส่วนบุคคล คือ ข้อมูลผู้ใช้เลขหมายโทรคมนาคม ข้อเท็จจริง รายละเอียดเกี่ยวกับผู้ใช้บริการที่สามารถระบุตัวผู้ใช้บริการหรืออาจระบุตัวผู้ใช้บริการนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ข้อมูลการใช้บริการ เลขหมายโทรคมนาคม รวมทั้งพฤติกรรมการใช้บริการโทรคมนาคมของผู้ใช้บริการ แต่ไม่รวมถึงข้อมูลทางเทคนิคที่ใช้เท่าที่จำเป็น เพื่อประโยชน์ในการบริหารโครงข่ายโทรคมนาคม เพื่อประโยชน์ในการติดต่อสื่อสาร และเพื่อประโยชน์ในการดำเนินธุรกิจในภาพรวมของผู้รับใบอนุญาต

ภายใต้พระราชบัญญัตินี้ หลักการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วย

- <u>การประมวลผลข้อมูลส่วนบุคคล</u>: ผู้รับใบอนุญาตจะกระทำได้ต่อเมื่อได้รับความยินยอมจากผู้ใช้บริการ โดยกระทำเพื่อประโยชน์ในการดำเนินกิจการโทรคมนาคมเท่านั้น และต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด ยกเว้น กรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลต่อหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่งคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือกรณีที่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพอนามัยของผู้ใช้บริการ หรือเป็นการส่งข้อมูลส่วนบุคคลให้คณะกรรมการหรือสำนักงาน จะไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลผู้ใช้บริการ
- <u>การเก็บรวบรวมข้อมูลส่วนบุคคล</u>: ผู้รับใบอนุญาตต้องเก็บรวบรวมข้อมูลส่วนบุคคลจากผู้ใช้บริการโดยตรง เท่าที่จำเป็นแก่การดำเนินกิจการโทรคมนาคมและเป็นไปตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย และผู้รับใบอนุญาตจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการที่เป็นลักษณะพิการทางร่างกาย (เว้นแต่การเก็บรวบรวมข้อมูลเพื่อประโยชน์ในการให้บริการที่เหมาะสมตามลักษณะพิการทางร่างกาย) ที่เป็นลักษณะทางพันธุกรรม และเป็นข้อมูลที่กระทบต่อความรู้สึกหรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้ใช้บริการอย่างชัดแจ้ง
- <u>การเก็บรักษาข้อมูลส่วนบุคคล</u>: ผู้รับใบอนุญาตต้องเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการในช่วงเวลา 3 เดือนสุดท้ายของการใช้บริการนับถัดจากวันที่ใช้บริการในปัจจุบัน ทั้งนี้ กรณีการให้บริการโทรคมนาคมสิ้นสุดลง ให้เก็บรักษาข้อมูลส่วนบุคคลไว้เป็นเวลา 3 เดือน นับถัดจากวัน

สิ้นสุดการให้บริการ เว้นแต่ กรณีมีความจำเป็นจะเก็บไว้เมื่อพ้นกำหนด 3 เดือนได้แต่ต้องไม่เกิน 2 ปี นับจากวันที่การให้บริการโทรคมนาคมสิ้นสุดลง หรือมีกฎหมายอื่นกำหนดให้เก็บรักษาไว้นานกว่า 3 เดือน

- สิทธิของผู้ใช้บริการ: ผู้ใช้บริการมีสิทธิขอตรวจดู ขอสำเนาหรือขอสำเนารับรองถูกต้องเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ ขอแก้ไขหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลของผู้ใช้บริการให้ถูกต้องสมบูรณ์ ขอระงับการใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ และเพิกถอนความยินยอมให้ประมวลผลไม่ว่าเวลาใดก็ตาม

(ค) พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534

กฎหมายฉบับนี้ให้ความคุ้มครองข้อมูลส่วนบุคคลของราษฎรไทยชนิดที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคลซึ่งจัดเก็บและครอบครองดูแลโดยนายทะเบียนราษฎรของรัฐ ได้แก่ นายทะเบียนประจำสำนักทะเบียนกลาง นายทะเบียนประจำสำนักทะเบียนกรุงเทพมหานคร นายทะเบียนประจำสำนักทะเบียนจังหวัด นายทะเบียนประจำสำนักทะเบียนอำเภอ นายทะเบียนประจำสำนักทะเบียนท้องถิ่น นายทะเบียนประจำสำนักทะเบียนสาขา นายทะเบียนประจำสำนักทะเบียนเฉพาะกิจ

กฎหมายฉบับนี้กำหนดหลักเกณฑ์เกี่ยวการจัดเก็บ (การแจ้งและการรับแจ้งของผู้มีหน้าที่ การบันทึกลงรายการ จัดทำหลักฐานทะเบียน) การแก้ไขข้อความรายการทะเบียน การจำหน่ายรายการทะเบียน การเพิกถอนหลักฐานทะเบียน ตลอดจนกำหนดสิทธิของเจ้าของข้อมูลให้สามารถขอคัดและรับรองเอกสารข้อมูลทะเบียนประวัติราษฎร ขอแก้ไขเพิ่มเติม ลบ หรือทำให้ทันสมัยซึ่งข้อมูลใดๆ ในข้อมูลทะเบียนประวัติราษฎรเพื่อให้เกิดความถูกต้องตามความเป็นจริง และอุทธรณ์ต่อรัฐมนตรีว่าการกระทรวงมหาดไทยภายใน 15 วันนับแต่วันรับทราบคำสั่งจากนายทะเบียนกลาง ให้กรณีที่นายทะเบียนที่ไม่รับคำขอ หรือไม่ดำเนินการตามคำขอทั้งหมดหรือบางส่วนให้

(ง) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ปรากฏอยู่ในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553 โดยประกาศดังกล่าวกำหนดให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ต้องปฏิบัติตามที่ประกาศฉบับนี้กำหนด เช่น

- จัดเก็บรวบรวมข้อมูลส่วนบุคคลโดยมีขอบเขตจำกัดและใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม ตลอดจนให้เจ้าของข้อมูลทราบและได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

- ข้อมูลที่เก็บรวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย
- ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บรวมถึงการนำข้อมูลไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน
- ห้ามไม่ให้มีการเปิดเผยหรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือเป็นกรณีที่กฎหมายกำหนดให้กระทำได้
- ให้มีมาตรการในการรักษาความมั่งคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ
- ให้ผู้ควบคุมข้อมูลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควร

(จ) พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550

พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ได้บัญญัติรับรองสิทธิในข้อมูลด้านสุขภาพของบุคคลและการรักษาความลับส่วนบุคคลไว้ในมาตรา 7 ของพระราชบัญญัติดังกล่าว โดยไม่ได้บัญญัติบทนิยามของข้อมูลด้านสุขภาพบุคคลไว้ ทั้งนี้ หลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 7 คือ ข้อมูลด้านสุขภาพของบุคคลเป็นความลับของบุคคล และการเปิดเผยข้อมูลด้านสุขภาพของบุคคลแก่ผู้ที่ไม่เกี่ยวข้องกับการรักษาพยาบาลไม่อาจทำได้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือมีกฎหมายกำหนดให้เปิดเผยข้อมูลได้

จากตัวอย่างบทบัญญัติแห่งกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลของไทย จะเห็นได้ว่าแม้ในอดีตที่ผ่านมาประเทศไทยจะไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะกฎหมายกลาง แต่ข้อมูลส่วนบุคคลที่ถูกนำไปใช้ในบริบทต่างๆ ล้วนได้รับความคุ้มครองในระดับที่สอดคล้องกับหลักสากลแล้ว อย่างไรก็ตาม สำหรับข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ ผู้เขียนมีความเห็นว่า ยังไม่มีกฎหมายใดไม่ว่าจะเป็นพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และกฎหมายเฉพาะเรื่องตามที่ยกตัวอย่างไว้ข้างต้น จะสามารถใช้บังคับได้ ดังนั้น การที่มาตรา 83 วรรคหนึ่ง กำหนดให้ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามกรอบวัตถุประสงค์ที่กำหนดไว้แต่เดิม แต่ผู้ควบคุมข้อมูลส่วน

บุคคลต้องเปิดโอกาสให้เจ้าของข้อมูลสามารถยกเลิกความยินยอมที่ได้ให้ไว้ก่อนร่างพระราชบัญญัติมีผลใช้บังคับได้ จะทำให้ข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ไม่ได้รับความคุ้มครองเท่าที่ควรจะเป็น เพราะในช่วงก่อนที่ร่างพระราชบัญญัตินี้ใช้บังคับข้อมูลดังกล่าวไม่มีกฎหมายคุ้มครองเหมือนเช่นข้อมูลส่วนบุคคลที่ถูกจัดเก็บโดยผู้ให้บริการโทรคมนาคม หรือผู้ให้บริการที่เกี่ยวข้องกับข้อมูลสุขภาพ เป็นต้น ด้วยเหตุนี้ หากจะให้เจ้าของข้อมูลทุกท่านได้รับความคุ้มครองข้อมูลส่วนบุคคลอย่างเสมอภาค ผู้เขียนเสนอแนะให้แก้มาตรา 83 วรรคหนึ่ง โดยเพิ่มเติมบทบัญญัติให้เฉพาะผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลโดยปฏิบัติตามกฎหมายที่กำหนดบทบัญญัติคุ้มครองข้อมูลส่วนบุคคลไว้แล้วสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามกรอบวัตถุประสงค์ที่กำหนดไว้แต่เดิมได้ ส่วนผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลมาก่อนร่างพระราชบัญญัติฉบับนี้ใช้บังคับโดยไม่ได้มีกฎหมายอื่นกำหนดให้ต้องปฏิบัติตามบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะ จะต้องปฏิบัติตามร่างพระราชบัญญัติฉบับนี้โดยไม่มีข้อยกเว้นดังนี้

มาตรา 83 ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้วก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมที่ ทั้งนี้ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

การดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยไม่ได้ปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

<u>ความเห็นต่อการเปิดเผยและการดำเนินการอื่นนอกเหนือจากการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามมาตรา 83 วรรคสอง ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)</u>

กรณีที่มาตรา 83 วรรคสองของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) กำหนดให้การใช้และการเปิดเผยทุกกรณีต้องดำเนินการตามร่างพระราชบัญญัตินี้นั้น ผู้เขียนเห็นด้วยว่าแม้ว่าประเทศไทยจะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และกฎหมายเฉพาะเรื่องที่บัญญัติหลักการว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการสากลไว้แล้วก็ตาม แต่การเปิดเผยและการดำเนินการอื่นนอกจากการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล เป็นการกระทำการที่มีความเสี่ยงจะก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลมากกว่าการเก็บรวบรวมไว้และการใช้โดยทั่วไป ดังนั้น ผู้เขียนจึงมีความเห็นเป็นไปในแนวทางเดียวกับผู้ยกร่าง คือ ควรกำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามพระราชบัญญัติฉบับนี้ คือ ขอความยินยอมจากเจ้าของข้อมูลใหม่ทุกกรณีโดยไม่มีข้อยกเว้น ทั้งนี้ เพื่อเป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลตามสิทธิขั้นพื้นฐานตามรัฐธรรมนูญของเจ้าของข้อมูลสส่วนบุคคล

5.4 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับแก้ไขเพิ่มเติมให้ครอบคลุมการให้บริการระบบการประมวลผลแบบคลาวด์)

จากปัญหาข้างต้น โดยเฉพาะอย่างยิ่งปัญหาความไม่เหมาะสมของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ในประเด็นต่างๆ ข้างต้น ผู้เขียนจึงได้แก้ไขเพิ่มเติมประเด็นที่สำคัญข้างต้น ตลอดจนความไม่สมบูรณ์ชัดเจนของถ้อยคำหลายประการเพื่อให้ร่างพระราชบัญญัติฉบับนี้สามารถใช้บังคับกับระบบการประมวลผลแบบคลาวด์ได้ และเป็นเพื่อแนวทางสำหรับการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยมีสาระสำคัญดังต่อไปนี้

บันทึกหลักการและเหตุผล

ประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ....

หลักการ

ให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เหตุผล

(1) เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือนร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

(2) เนื่องจากปัจจุบันนานาประเทศต่างออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศ ซึ่งจะกำหนดให้การโอนข้อมูลระหว่างกันสามารถกระทำได้เฉพาะกรณีที่ประเทศนั้นๆ มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ ซึ่งจะกระทบต่อหน่วยงานภาคเอกชนของไทยที่จำเป็นต้องรับและส่งข้อมูลส่วนบุคคลระหว่างประเทศ

ดังนั้น จึงสมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

ข้อสังเกต: เหตุผลในการยกร่างของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับนี้ยังขาดเหตุผลในการส่งเสริมการประกอบธุรกิจของภาคเอกชนในไทย เนื่องจากภารกิจของกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น ไม่จำกัดอยู่เพียงการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลเท่านั้น แต่ยังควรต้องช่วยส่งเสริมให้การค้าภายในและระหว่างประเทศ สามารถดำเนินต่อไปได้

ร่าง

พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ....

.....

.....

.....

.....

.....

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา 26 ประกอบกับมาตรา 32 มาตรา 33 และมาตรา 37 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิเสรีภาพของบุคคลตามพระราชบัญญัตินี้เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

.....

.....

มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่บทบัญญัติในหมวด 1 บทบัญญัติในหมวด 4 และมาตรา 77 มาตรา 78 มาตรา 79 มาตรา 80 มาตรา 81 มาตรา 82 และมาตรา 83 ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลและบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(2) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลแต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคล ผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(5) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(6) ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลลบสิ่งเชื่อมโยงตัวบุคคลออกอย่างถาวรจนทำให้ไม่สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

ข้อสังเกต: การกำหนดเพิ่มเติมข้างต้นเป็นการกำหนดเพื่อรองรับหลักการเรื่องข้อมูลนิรนาม (Anomymous Data) ซึ่งจะช่วยส่งเสริมให้ผู้ควบคุมข้อมูลหลายรายหันมาใช้เทคโนโลยีในการทำให้ข้อมูลส่วนบุคคลกลายเป็นข้อมูลนิรนาม เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคลและเพื่อให้สามารถนำข้อมูลดังกล่าวไปใช้ในเชิงธุรกิจได้

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

มาตรา 5 พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าผู้นั้นจะอยู่ในหรือนอกราชอาณาจักรก็ตาม

การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่กระทำนอกราชอาณาจักรแม้แต่ส่วนหนึ่งส่วนใดของการกระทำได้กระทำในราชอาณาจักร หรือกระทำนอกราชอาณาจักรที่ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักรหรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นนั้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักร ให้ถือว่าเป็นการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้กระทำในราชอาณาจักร

มาตรา 6 ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ชื่อสกุล ชื่อกลาง ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อสังเกต: การเพิ่มบทนิยามข้างต้นเป็นไปเพื่อให้เกิดความชัดเจนว่าขอบเขตของข้อมูลส่วนบุคคลใดบ้างที่จะได้รับความคุ้มครอง ทั้งนี้ การกำหนดให้ข้อมูลส่วนบุคคลไม่รวมถึงการระบุเฉพาะชื่อ ชื่อสกุล ชื่อกลาง ตำแหน่ง สถานที่ทำงานหรือที่อยู่ทางธุรกิจ ถือเป็นการกำหนดหลักการที่ถูกต้อง เนื่องจากชื่อ สถานที่ทำงานหรือที่อยู่ทางธุรกิจเป็นสิ่งเจ้าของชื่อดังกล่าวสามารถเปิดเผยให้บุคคล

ทั่วไปรับรู้ได้ โดยไม่ถือเป็นความลับ โดยเฉพาะอย่างยิ่งหากนำชื่อไปรวมกับสถานที่ทำงานซึ่งมักจะปรากฏบนนามบัตรทางธุรกิจ ยิ่งแสดงให้เห็นว่าข้อมูลดังกล่าวไม่ควรถูกระบุให้เป็นข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติฉบับนี้

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน หมายความว่า บุคคลหรือนิติบุคคลซึ่งกำหนดวิธีการและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลร่วมกับผู้อื่น

ข้อสังเกต: การเพิ่มบทนิยามข้างต้นเป็นไปเพื่อรองรับหลักการเรื่องผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน (Joint Controller)

"ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

"เจ้าของข้อมูลส่วนบุคคล" หมายความว่า บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล และให้หมายความรวมถึง

(1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ

(3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

ข้อสังเกต: การแก้ไขบทนิยามข้างต้นเป็นไปเพื่อให้เกิดความชัดเจน

"บุคคล" หมายความว่า บุคคลธรรมดา

"คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"สำนักงาน" หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"เลขาธิการ" หมายความว่า เลขาธิการสำนักงานคณะกรรมการการคุ้มครองข้อมูลส่วนบุคคล

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา 7 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้ใช้บังคับได้

หมวด 1
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 8 ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(1) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ

(3) กรรมการโดยตำแหน่ง จำนวนแปดคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา อัยการสูงสุด เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้แทนสภาหอการค้าแห่งประเทศไทย ผู้แทนสภาอุตสาหกรรมแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

(4) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล <u>ซึ่งมาจากทั้งภาครัฐและภาคเอกชน</u>

<u>ข้อสังเกต</u>: การเพิ่มที่มาของกรรมการผู้ทรงคุณวุฒิข้างต้น เป็นไปเพื่อให้ภาคเอกชนเข้ามามีส่วนร่วมกับการกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของประเทศ เพื่อให้สอดรับกับทั้งการคุ้มครองข้อมูลส่วนบุคคลและการรองรับภาคธุรกิจ

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา 11 ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

มาตรา 9 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(1) มีสัญชาติไทย

(2) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(3) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(4) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา 10 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา 11 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 10 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 9

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระให้รองประธานกรรมการทำหน้าที่เป็นประธานกรรมการเป็นการชั่วคราว

มาตรา 12 การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้รองประธานกรรมการทำหน้าที่เป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการและรองประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด

มาตรา 13 กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณาให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา 14 คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้

(1) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติตามนโยบายและแผนระดับชาติดังกล่าว

(2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนยุทธศาสตร์ตาม (1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าวเพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

(3) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(4) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

(6) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ

(7) พิจารณากำหนดค่าปรับทางปกครองตามมาตรา 69 มาตรา 70 มาตรา 71 มาตรา 72 มาตรา 73 มาตรา 74 และมาตรา 75 รวมทั้งฟ้องคดีต่อศาลปกครอง ทั้งนี้ ในกรณีที่มีการบังคับทางปกครองเพื่อชำระค่าปรับทางปกครอง ให้คณะกรรมการเป็นผู้มีอำนาจออกคำสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินในการบังคับทางปกครองและให้ประธานกรรมการเป็นผู้ลงนามแทนในคำสั่งดังกล่าว

(8) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(9) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้

(10) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(11) ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัตินี้

(12) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(13) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(14) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ

มาตรา 15 ให้กรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

อนุกรรมการและกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา 16 คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการให้นำความในมาตรา 12 มาใช้บังคับโดยอนุโลม

หมวด 2
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 1
บททั่วไป

มาตรา 17 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

มาตรา 18 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ส่วนที่ 2
การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา 19 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 20 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ ในรูปแบบที่เข้าใจง่าย

(1) วัตถุประสงค์ของการเก็บรวบรวม

(2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ

(5) สิทธิของเจ้าของข้อมูลตามมาตรา 26 มาตรา 27 และมาตรา 28

กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

ข้อสังเกต: เป็นการเพิ่มเพื่อให้การดำเนินการตามกฎหมายสามารถเกิดขึ้นได้จริง เนื่องจากหากรายละเอียดดังกล่าวไม่อยู่ในรูปแบบที่เข้าถึงได้โดยง่าย เจ้าของข้อมูลอาจให้ความยินยอมโดยสำคัญผิดได้

มาตรา 21 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล

(6) เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

(7) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา 22 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตามมาตรา 23

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

มาตรา 23 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) ได้รับยกเว้นตามมาตรา 21 (2) หรือ (6)

(2) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ส่วนที่ 3
การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 21 หรือมาตรา 23 หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา 22(3) แล้วแต่กรณี

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่งจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา 31

ส่วนที่ 4
การโอนข้อมูลส่วนบุคคลระหว่างประเทศ

มาตรา 25 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 14 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(5) เป็นการโอนข้อมูลระหว่างบริษัทในเครือซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรที่ได้รับอนุมัติจากคณะกรรมการ

(6) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ข้อสังเกต: เนื่องจากในการดำเนินธุรกิจระหว่างประเทศอาจจำเป็นต้องมีการโอนข้อมูลส่วนบุคคลของลูกค้าระหว่างกลุ่มบริษัทเดียวกัน ดังนั้น การกำหนดข้อยกเว้นข้างต้นจึงจะช่วยให้ภาคธุรกิจสามารถโอนข้อมูลส่วนบุคคลได้คล่องตัวขึ้นโดยอยู่บนพื้นฐานของเงื่อนไขที่ว่ากลุ่มบริษัทดังกล่าวมีนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ชัดจนและไม่ขัดต่อกฎหมายฉบับนี้ (เทียบเคียงจาก GDPR)

หมวด 3
สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา 26 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้

(1) เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล

(2) มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย

(3) การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น

(4) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 31

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ทั้งนี้ คณะกรรมการจะประกาศกำหนดระยะเวลาในการดำเนินการตามคำขอให้เร็วขึ้นหรือขยายระยะเวลาดังกล่าวหรือกำหนดหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

มาตรา 27 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา 28 ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามวรรคหนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามวรรคหนึ่งไว้ในรายการตามมาตรา 31

มาตรา 28/1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับข้อมูลส่วนบุคคลเกี่ยวกับตนที่ได้มอบความยินยอมให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในรูปแบบที่ใช้กันอยู่ทั่วไปและเข้าใจง่าย และมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลโอนย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลอีกรายหนึ่งได้โดยปราศจากอุปสรรคใดๆ

ในการใช้สิทธิตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจร้องขอให้เจ้าของข้อมูลส่วนบุคคลพิสูจน์ว่าตนเองเป็นเจ้าของข้อมูลที่แท้จริงได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอเช่นว่านั้นได้ หากการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลไม่สามารถกระทำได้โดยง่ายในทางเทคนิค หรือ การดำเนินการเช่นว่านั้นอาจทำให้กระทบต่อสิทธิและเสรีภาพของบุคคลอื่น

ข้อสังเกต: การเพิ่มบทบัญญัติข้างต้นเป็นไปเพื่อรองรับสิทธิในการโอนย้ายข้อมูลของเจ้าของข้อมูลส่วนบุคคล (Data Portability) (เทียบเคียงจาก GDPR)

มาตรา 29 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ

(2) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(4) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 27 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(5) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ข้อสังเกต: การเพิ่มบทบัญญัติข้างต้นเป็นการเพิ่มเพื่อให้เจ้าของข้อมูลสามารถบังคับใช้สิทธิของตนกับผู้ควบคุมข้อมูลได้จริง

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

(4) แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที

(5) ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งโดยปราศจากกฎหมายกำหนดให้สามารถกระทำได้ หรือปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้า

(7) ปฏิบัติตามบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

(8) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

ข้อสังเกต: เป็นการเพิ่มหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้รองรับหลักการว่าด้วยผู้ประมวลผลข้อมูลส่วนบุคคลอย่างครบถ้วนและเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถบังคับใช้สิทธิของตนกับผู้ประมวลผลข้อมูลได้จริง

มาตรา 31 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้และการเปิดเผยตามมาตรา 24 วรรคสาม

(7) การปฏิเสธคำขอตามมาตรา 26 วรรคสาม และมาตรา 28 วรรคสอง

มาตรา 31/1 ในกรณีที่ผู้ควบคุมข้อมูลตั้งแต่ 2 รายขึ้นไปร่วมกันตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการของการประมวลผลข้อมูลส่วนบุคคล บุคคลดังกล่าวถือเป็นผู้ควบคุมข้อมูลร่วมกันและต้องกำหนดความรับผิดชอบในการปฏิบัติหน้าที่ตามที่พระราชบัญญัตินี้กำหนด

หากผู้ควบคุมข้อมูลส่วนบุคคลร่วมกันไม่ได้ดำเนินการตามวรรคแรก ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดแทน

ข้อสังเกต: เป็นการกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนร่วมกัน (Joint Controller) เพื่อรองรับหลักการของผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน (Joint Controller) (เทียบเคียงจาก GDPR)

หมวด 4
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 32 ให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

สำนักงานเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยแรงงานรัฐวิสาหกิจสัมพันธ์ กฎหมายว่าด้วยการประกันสังคม

และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

ให้สำนักงานเป็นหน่วยงานของรัฐตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่

มาตรา 33 นอกจากดำเนินการให้เป็นไปตามวัตถุประสงค์ตามมาตรา 32 วรรคหนึ่ง ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

(1) จัดทำร่างแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการ

(2) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(3) วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(4) สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล และแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการ

(5) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(6) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(7) เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานภาครัฐ หน่วยงานเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

(8) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(9) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามอำนาจหน้าที่ของสานักงาน

(10) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(11) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

มาตรา 34 ในการดำเนินงานของสำนักงาน นอกจากอำนาจหน้าที่ตามที่บัญญัติในมาตรา 33 แล้ว ให้สำนักงานมีอำนาจหน้าที่ทั่วไป ดังต่อไปนี้ด้วย

(1) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิต่าง ๆ

(2) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน

(3) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน

(4) ถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นในกิจการที่เกี่ยวกับวัตถุประสงค์ของสำนักงาน

(5) กู้ยืมเงินเพื่อประโยชน์ในการดำเนินการตามวัตถุประสงค์ของสำนักงาน

(6) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(7) ดำเนินการอื่นใดที่จำเป็นหรือต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของสำนักงาน

(8) ปฏิบัติการใด ๆ ให้เป็นไปตามพระราชบัญญัตินี้ หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือคณะกรรมการมอบหมาย

การถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นตาม (4) และการกู้ยืมเงินตาม (5) ให้เป็นไปตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา 35 ทุนและทรัพย์สินในการดำเนินงานของสำนักงานประกอบด้วย

(1) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา 80

(2) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(3) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้จากการดำเนินงาน

(4) เงินอุดหนุนจากภาคเอกชนหรือองค์กรอื่น รวมทั้งจากต่างประเทศหรือองค์การระหว่างประเทศ และเงินหรือทรัพย์สินที่มีผู้อุทิศให้

(5) ดอกผลและผลประโยชน์หรือรายได้อื่นใดที่เกิดจากการดำเนินงานของสำนักงาน

ทรัพย์สินของสำนักงานไม่อยู่ในความรับผิดแห่งการบังคับคดีและมาตรการบังคับทางปกครอง

เงินและทรัพย์สินของสำนักงานไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน ยกเว้นดอกผล และผลประโยชน์หรือรายได้อื่นตามวรรคหนึ่ง (5) เมื่อใช้จ่ายตามอำนาจหน้าที่ของสำนักงานแล้ว ที่เหลือให้นำส่งคลังเป็นรายได้แผ่นดิน

มาตรา 36 ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ประธานกรรมการซึ่งรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติและกรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งจำนวนหกคน

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานเป็นผู้ช่วยเลขานุการได้ตามความจำเป็นแต่ไม่เกินสองคน

กรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งตามวรรคหนึ่ง ต้องมีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยสามคน และด้านอื่นที่เกี่ยวข้องอันเป็นประโยชน์ต่อการดำเนินงานของสำนักงาน

ให้นำบทบัญญัติมาตรา 9 และมาตรา 11 มาใช้บังคับกับประธานกรรมการและกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา 37 ให้ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวาระการดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง ให้ดำเนินการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ภายในหกสิบวัน ในระหว่างที่ยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา 38 ในกรณีที่ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ พ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนและในกรณี

ที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้ดำเนินการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิแทนตำแหน่งที่ว่างภายในหกสิบวันนับแต่วันที่ตำแหน่งว่างลง และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน เว้นแต่วาระของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิเหลือไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

มาตรา 39 การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

ในการวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้ามีคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

กรรมการที่มีส่วนได้เสียในเรื่องที่มีการพิจารณาจะเข้าร่วมประชุมมิได้

การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจกระทำโดยวิธีการทางอิเล็กทรอนิกส์ตามที่คณะกรรมการกำหนดก็ได้

มาตรา 40 คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีอำนาจและหน้าที่ ดังต่อไปนี้

(1) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(2) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

(3) อนุมัติแผนการดำเนินงาน แผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(4) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(5) แต่งตั้งคณะกรรมการสรรหาเลขาธิการ

(6) วินิจฉัยอุทธรณ์คำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(7) ประเมินผลการดำเนินการของสำนักงาน และการปฏิบัติงานของเลขาธิการ

(8) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการกำกับสำนักงานคุ้มครองข้อมูลส่วนหรือตามที่คณะรัฐมนตรีมอบหมาย

ข้อบังคับตาม (2) ถ้ามีการจำกัดอำนาจเลขาธิการในการทำนิติกรรมกับบุคคลภายนอกให้ประกาศในราชกิจจานุเบกษา

มาตรา 41 คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจแต่งตั้งคณะอนุกรรมการ เพื่อปฏิบัติหน้าที่หรือกระทำการอย่างหนึ่งอย่างใดตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมอบหมายได้

คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจแต่งตั้งบุคคลซึ่งมีความเชี่ยวชาญหรือประสบการณ์ที่จะเป็นประโยชน์ในการปฏิบัติหน้าที่ของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้

การปฏิบัติหน้าที่และจำนวนของคณะอนุกรรมการตามวรรคหนึ่งหรือบุคคลตามวรรคสอง ให้เป็นไปตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ให้นำมาตรา 39 มาใช้บังคับแก่คณะอนุกรรมการโดยอนุโลม

มาตรา 42 ให้ประธานกรรมการและกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประธานอนุกรรมการและอนุกรรมการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง ได้รับเบี้ยประชุมหรือค่าตอบแทนตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา 43 ให้สำนักงานมีเลขาธิการคนหนึ่งซึ่งคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง มีหน้าที่บริหารกิจการของสำนักงาน

การแต่งตั้งเลขาธิการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์และวิธีการสรรหาตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 44 ผู้ที่จะได้รับการแต่งตั้งเป็นเลขาธิการต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(1) มีสัญชาติไทย

(2) อายุไม่เกินห้าสิบห้าปีบริบูรณ์

(3) สามารถทำงานให้แก่สำนักงานได้เต็มเวลา

(4) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงานและการบริหารจัดการ

(5) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(6) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(7) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(8) ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจ หรือจากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(9) ไม่เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(10) ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่พรรคการเมือง

(11) ไม่เป็นผู้มีส่วนได้เสียในกิจการที่เกี่ยวข้องกับสำนักงานไม่ว่าโดยทางตรงหรือทางอ้อม

มาตรา 45 เลขาธิการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระติดต่อกันไม่ได้

ก่อนครบกำหนดตามวาระการดำรงตำแหน่งของเลขาธิการเป็นเวลาไม่น้อยกว่าสามสิบวันแต่ไม่เกินหกสิบวัน หรือภายในสามสิบวันนับแต่วันที่เลขาธิการพ้นจากตำแหน่งก่อนครบวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งคณะกรรมการเพื่อสรรหาเลขาธิการคนใหม่ ทั้งนี้ ให้คณะกรรมการสรรหาเสนอรายชื่อบุคคลที่เหมาะสมไม่เกินสามคนต่อคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 46 ในแต่ละปีให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 47 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 45 เลขาธิการพ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) อายุครบหกสิบปีบริบูรณ์

(4) คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน มีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(6) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 44

มาตรา 48 ให้เลขาธิการมีอำนาจหน้าที่ ดังต่อไปนี้

(1) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนระดับชาติ แผนยุทธศาสตร์ นโยบายของคณะรัฐมนตรี คณะกรรมการ และคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และระเบียบข้อบังคับหรือมติของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2) วางระเบียบเกี่ยวกับการดำเนินงานของสำนักงานโดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(3) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามระเบียบหรือข้อบังคับของสำนักงาน

(4) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(5) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงาน และลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามระเบียบหรือข้อบังคับที่คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(6) ปฏิบัติการอื่นใดตามระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการรับผิดชอบในการบริหารงานของสำนักงานขึ้นตรงต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 49 ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการ เป็นผู้แทนของสำนักงาน เพื่อการนี้ เลขาธิการจะมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทนก็ได้ แต่ต้องเป็นไปตามข้อบังคับที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 50 ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้กำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา 51 เพื่อประโยชน์ในการบริหารงานของสำนักงาน เลขาธิการอาจขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐ มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราวได้ ทั้งนี้ เมื่อได้รับอนุมัติจากผู้บังคับบัญชาหรือนายจ้างของผู้นั้น และมีข้อตกลงที่ทำไว้ในการอนุมัติ และในกรณีที่เจ้าหน้าที่ของรัฐได้รับอนุมัติให้มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราว ให้ถือว่าเป็นการได้รับอนุญาตให้ออกจากราชการหรือออกจากงานไปปฏิบัติงานใด ๆ

เมื่อสิ้นสุดระยะเวลาที่ได้รับอนุมัติให้มาปฏิบัติงานในสำนักงาน ให้เจ้าหน้าที่ของรัฐตามวรรคหนึ่ง มีสิทธิได้รับการบรรจุและแต่งตั้งให้ดำรงตำแหน่งและรับเงินเดือนในส่วนราชการหรือหน่วยงานเดิมไม่ต่ำกว่าตำแหน่งและเงินเดือนเดิมตามข้อตกลงที่ทำไว้ในการอนุมัติ

ในกรณีที่เจ้าหน้าที่ของรัฐผู้นั้นกลับมาบรรจุและได้รับแต่งตั้งในส่วนราชการหรือหน่วยงานเดิมตามวรรคสองแล้ว ให้นับระยะเวลาของเจ้าหน้าที่ของรัฐผู้นั้นระหว่างที่มาปฏิบัติงานในสำนักงานสำหรับการคำนวณบำเหน็จบำนาญหรือประโยชน์ตอบแทนอื่นทำนองเดียวกันเสมือนอยู่ปฏิบัติราชการหรือปฏิบัติงานเต็มเวลาดังกล่าว แล้วแต่กรณี

มาตรา 52 ข้าราชการหรือเจ้าหน้าที่ของรัฐซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากส่วนราชการหรือหน่วยงานของรัฐ ที่ได้ย้ายมาปฏิบัติหน้าที่ที่สำนักงานโดยได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัด ให้ถือเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในสำนักงานเป็นระยะเวลาในการชดใช้ทุน

ในกรณีที่หน่วยงานของรัฐแห่งใดประสงค์จะขอให้พนักงานของสำนักงานซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากสำนักงานไปเป็นข้าราชการหรือเจ้าหน้าที่ของรัฐในหน่วยงานของรัฐแห่งนั้น ต้องได้รับความเห็นชอบจากเลขาธิการก่อน และให้ถือว่าการไปปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นระยะเวลาในการชดใช้ทุน

มาตรา 53 การบัญชีของสำนักงานให้จัดทำตามหลักสากล ตามแบบและหลักเกณฑ์ที่คณะกรรมการกากับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 54 ให้สำนักงานจัดทางบดุล งบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในหนึ่งร้อยยี่สิบวันนับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อคณะกรรมการเพื่อรับรอง

มาตรา 55 ให้สำนักงานจัดทำรายงานการดำเนินงานประจำปีเสนอคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นชอบ

มาตรา 56 ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามอำนาจหน้าที่และตามกฎหมาย นโยบายของรัฐบาล แผนยุทธศาสตร์ และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่ออำนาจหน้าที่ของสำนักงาน นโยบายของรัฐบาล แผนยุทธศาสตร์ หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้

ในกรณีที่เลขาธิการฝ่าฝืนหรือไม่กระทำการตามคำสั่งของรัฐมนตรีตามวรรคหนึ่ง ให้รัฐมนตรีส่งเรื่องให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาดำเนินการตามอำนาจหน้าที่ต่อไป

หมวด 5
การร้องเรียน

มาตรา 57 ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร

คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่งและการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา 58 คณะกรรมการผู้เชี่ยวชาญมีอำนาจและหน้าที่ ดังต่อไปนี้

(1) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้

(2) ตรวจสอบการกระทำใดๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(3) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(4) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ

มาตรา 59 เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียน ให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

มาตรา 60 ในกรณีที่ผู้ร้องเรียนตามมาตรา 59 ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา 59 วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นไม่ได้กำหนดให้ไม่ให้รับไว้พิจารณาให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา

เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา 59 (1) หรือตรวจสอบการกระทำใดๆ ตามมาตรา 59(2) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง

ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่าเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้ หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้

(1) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด

(2) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (1) หรือ (2) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น

การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสองหรือวรรคสาม (1) หรือ (2) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน

มาตรา 61 คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา 60 วรรคหนึ่งหรือยุติเรื่องตามมาตรา 60 วรรคสอง หรือคำสั่งตามมาตรา 60 วรรคสาม (1) หรือ (2) ให้เป็นที่สุด

มาตรา 62 ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะเรียกให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้

มาตรา 63 ในการปฏิบัติตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ดังต่อไปนี้

(1) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้

(2) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำความผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

ในการดำเนินการตาม (2) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร

หมวด 6
ความรับผิดทางแพ่ง

มาตรา 64 ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคล ของผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล นั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(3) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 14(6)

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ข้อสังเกต: เป็นการเพิ่มบุคคลที่ต้องรับผิดทางแพ่งเพื่อให้สอดคล้องกับทางปฏิบัติที่มีโอกาสที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลได้

หมวด 7
บทกำหนดโทษ

ส่วนที่ 1
โทษอาญา

มาตรา 65 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 เพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น หรือโดยประการที่น่าจะทำให้ผู้อื่นนั้นเกิดความเสียหาย เสียชื่อเสียง

ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 66 ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

~~มาตรา 67 ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆ ด้วย~~

ข้อสังเกต: ผู้เขียนมีความเห็นว่าการกำหนดโทษให้กรรมการต้องรับผิดทางอาญาไม่ช่วยก่อให้เกิดความตระหนักถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการ ดังนั้น จึงเห็นควรตัดมาตรานี้ออกจากร่างพระราชบัญญัติฉบับนี้

มาตรา 68 บรรดาความผิดตามพระราชบัญญัตินี้ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้

เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ส่วนที่ 2
โทษทางปกครอง

มาตรา 69 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 20 มาตรา 26 วรรคสี่ มาตรา 31 หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 17 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 17 วรรคห้า ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 70 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ต้องระวางโทษ

ปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 71 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 หรือฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 72 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 30 โดยไม่มีเหตุอันควร ต้องระวางโทษปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 73 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 62 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 63 วรรคสาม ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 74 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

ข้อสังเกต: ผู้เขียนมีความเห็นว่าจำนวนโทษปรับทางปกครองที่ร่างพระราชบัญญัติฉบับนี้กำหนดไว้ยังไม่เพียงพอที่จะทำให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกรงกลัวและปฏิบัติตามกฎหมายนี้อย่างเคร่งครัดจึงเสนอให้แก้ไขจำนวนโทษปรับทางปกครอบโดยเทียบเคียงกับร่างพระราชบัญญัติฉบับรับฟังความคิดเห็นและ GDPR

มาตรา 75 ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด

ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

บทเฉพาะกาล

มาตรา 76 ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา 8 (2) (3) และกรรมการตามวรรคสอง เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ และให้รอบประธานกรรมการทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา 8(1) และกรรมการผู้ทรงคุณวุฒิตามมาตรา 8(4) ภายในเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 77 ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 78 ในวาระเริ่มแรกที่ยังไม่มีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ให้รัฐมนตรีแต่งตั้งผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือบุคคลใดตามที่รัฐมนตรีเห็นสมควร ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 79 ในวาระเริ่มแรก เมื่อได้จัดตั้งสำนักงานแล้วแต่ยังไม่มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ และผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลที่รัฐมนตรีแต่งตั้ง จำนวนสี่คน เป็นกรรมการ และให้ผู้ปฏิบัติหน้าที่เลขาธิการตามมาตรา 78 เป็นเลขานุการของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยให้ปฏิบัติหน้าที่เป็นการชั่วคราวไปจนกว่าจะมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 80 ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

มาตรา 81 ในวาระเริ่มแรก ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานเป็นพนักงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนดได้

มาตรา 82 ในระหว่างที่ยังมิได้มีการออกประกาศ ระเบียบ หรือข้อบังคับในส่วนที่เกี่ยวข้องกับสำนักงานตามพระราชบัญญัตินี้ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถกำหนดให้นำประกาศ ระเบียบ หรือข้อบังคับของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือของหน่วยงานของรัฐอื่นซึ่งอยู่ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ใช้บังคับอยู่ในวันก่อนวันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ มาใช้บังคับโดยอนุโลมกับสำนักงานได้ ทั้งนี้ เท่าที่ไม่ขัดหรือแย้งกับพระราชบัญญัตินี้

มาตรา 83 ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้วก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วน

บุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

การดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยไม่ได้ปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

ข้อสังเกต: เป็นการแก้ไขเพิ่มเติมเพื่อให้ครอบคลุมข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ที่ไม่เคยได้รับความคุ้มครองตามกฎหมายใดๆ มาก่อน

มาตรา 84 การดำเนินการออกกฎกระทรวง ประกาศ ระเบียบและข้อบังคับตามพระราชบัญญัตินี้ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

ระบบการประมวลผลแบบคลาวด์เป็นเทคโนโลยีที่มีความสำคัญอย่างมากต่อทั้งผู้ประกอบการและบุคคลทั่วไป ที่จะช่วยให้สามารถประกอบธุรกิจหรือดำรงชีวิตได้อย่างสะดวกสบายและประหยัดค่าใช้จ่ายมากยิ่งขึ้น โดยในปัจจุบันประเทศไทยมีผู้ให้บริการระบบการประมวลผลแบบคลาวด์เป็นจำนวนมากและมีแนวโน้มจะเพิ่มมากขึ้นเรื่อยๆ ในอนาคต ระบบการประมวลผลแบบคลาวด์เป็นระบบที่เกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคล เนื่องจากผู้ประกอบการหรือผู้ใช้งานทั่วไปนิยมที่จะนำข้อมูลที่มีลักษณะเป็นข้อมูลส่วนบุคคลของตนไปประมวลผลหรือจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ของภาคเอกชนที่ให้บริการโดยไม่คิดค่าใช้จ่าย ซึ่งผู้เขียนเห็นว่า การเก็บข้อมูลส่วนบุคคลของตนไว้ในความครอบครองของบุคคลอื่น ย่อมก่อให้เกิดความเสี่ยงที่ข้อมูลดังกล่าวจะรั่วไหลและก่อให้เกิดความเสียหายเป็นอย่างมาก ดังนั้น นานาประเทศที่มีการให้บริการระบบการประมวลผลแบบคลาวด์จึงควรต้องตระหนักถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบการประมวลผลแบบคลาวด์ ไม่ว่าจะโดยส่งเสริมให้เกิดการสร้างเครื่องป้องกันการรั่วไหลของข้อมูลหรือการบัญญัติกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลนั้นๆ ซึ่งเมื่อพิจารณากฎหมายคุ้มครองข้อมูลส่วนบุคคลส่วนใหญ่จะพบว่าหลายประเทศและองค์การสากลต่างแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมและเหมาะสมกับการให้บริการระบบการประมวลผลแบบคลาวด์มากยิ่งขึ้น ไม่ว่าจะเป็น กฎหมายของสหภาพยุโรปทั้งฉบับเดิม (Directive 95/46/EC) และฉบับใหม่ (GDPR) กฎหมายของประเทศเยอรมนี กฎหมายของประเทศญี่ปุ่น เป็นต้น นอกจากนั้น บางประเทศยังบัญญัติกฎหมายที่ใช้บังคับกับการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์โดยเฉพาะอีกด้วย อาทิ ประเทศแม็กซิโก ประเทศเกาหลีใต้ เป็นต้น

เมื่อพิจารณากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย จะพบว่าในขณะนี้ประเทศไทยมีกฎหมายกลางที่จะสามารถใช้คุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ได้เพียงฉบับเดียว คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งพระราชบัญญัติดังกล่าวยังคงมีข้อจำกัดอยู่ว่าจะใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐเท่านั้น ดังนั้น เมื่อพิจารณาพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ในบริบทของการให้บริการระบบการประมวลผลแบบคลาวด์จะพบว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะใช้บังคับได้เฉพาะกรณีที่หน่วยงานของรัฐเป็นผู้ให้บริการระบบ

การประมวลผลแบบคลาวด์เองเท่านั้น ซึ่งจะทำให้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่สามารถใช้บังคับได้ในทางปฏิบัติ เนื่องจากในปัจจุบันผู้ให้บริการระบบการประมวลผลแบบคลาวด์เป็นการให้บริการโดยภาคเอกชน ด้วยเหตุนี้ความหวังของการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บอยู่ในระบบการประมวลผลแบบคลาวด์ของประเทศไทยจึงอยู่ที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ซึ่งยังอยู่ในระหว่างการพิจารณาอีกครั้งของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

อย่างไรก็ตาม เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ผู้เขียนพบว่า ร่างพระราชบัญญัติดังกล่าวยังไม่สอดคล้องกับรูปแบบธุรกิจหรือรูปแบบการให้บริการของระบบการประมวลผลแบบคลาวด์ ดังนี้

6.1.1 ขอบเขตของข้อมูลที่จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

แต่เดิมกฎหมายคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศและร่างพระราชบัญญัติของประเทศไทยเอง ต่างกำหนดให้กฎหมายของตนมีผลใช้บังคับเฉพาะกับข้อมูลที่เข้าลักษณะเป็นข้อมูลส่วนบุคคลเท่านั้น นั่นหมายความว่า หากข้อมูลใดไม่เข้าลักษณะหรือคำจำกัดความของข้อมูลส่วนบุคคล ได้แก่ ข้อมูลที่สามารถเชื่อมโยงถึงตัวบุคคลซึ่งเป็นเจ้าของข้อมูลได้ ข้อมูลนั้นจะไม่ตกอยู่ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งการกำหนดขอบเขตการบังคับใช้เช่นนี้อาจก่อให้เกิดปัญหาในการบังคับใช้กฎหมายในปัจจุบัน เนื่องจากเทคโนโลยีการป้องกันการเข้าถึงข้อมูลส่วนบุคคล เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลหรือข้อมูลทางธุรกิจที่สำคัญรั่วไหล ทำให้เกิดกระบวนการทำให้ข้อมูลส่วนบุคคลสูญเสียสิ่งเชื่อมโยงตัวบุคคลไป ดังนั้น ผู้ที่ได้รับข้อมูลดังกล่าวจะไม่สามารถเชื่อมโยงถึงตัวบุคคลที่เป็นเจ้าของข้อมูลได้ไม่ว่าชั่วคราวหรือถาวร ซึ่งกระบวนการดังกล่าว ได้แก่ กระบวนการ Anonymization กระบวนการ Pseudonymization และกระบวนการ Encryption เป็นต้น กรณีจึงเกิดปัญหาในทางปฏิบัติว่าข้อมูลที่ผ่านกระบวนการเหล่านี้จะยังมีลักษณะเป็นข้อมูลส่วนบุคคลที่ยังตกอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่

ด้วยเหตุนี้ หลายประเทศจึงปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนเอง เพื่อให้เกิดความชัดเจนว่า ข้อมูลเหล่านี้จะอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนหรือไม่ อาทิ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปฉบับเดิม (Directive 95/46/EC) ซึ่งบัญญัติให้กฎหมายดังกล่าวไม่มีผลใช้บังคับกับข้อมูลส่วนบุคคลที่ได้ผ่านกระบวนการ Anonymization แล้ว ดังนั้น ผู้ควบคุมข้อมูลจึงสามารถประมวลผลข้อมูลดังกล่าวได้อย่างอิสระ

ตราบเท่าที่ข้อมูลนั้นไม่สามารถเชื่อมโยงถึงตัวบุคคลที่เป็นเจ้าของข้อมูลได้ จะเห็นได้ว่า Directive 95/46/EC ไม่ได้กล่าวถึงข้อมูลที่ผ่านกระบวนการ Pseudonymization และกระบวนการ Encryption แต่อย่างใด

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปฉบับใหม่ (GDPR) บัญญัติสอดคล้องกับ Directive 95/46/EC คือ กฎหมายดังกล่าวจะไม่มีผลใช้บังคับกับข้อมูลส่วนบุคคลที่ได้ผ่านกระบวนการ Anonymization และยังบัญญัติครอบคลุมไปถึงข้อมูลที่ผ่านกระบวนการ Pseudonymization ด้วย แต่สำหรับข้อมูลที่ผ่านกระบวนการ Pseudonymization นั้น GDPR บังคับให้ข้อมูลดังกล่าวยังอยู่ภายใต้บังคับของ GDPR เนื่องจากข้อมูลที่ผ่านกระบวนการ Pseudonymization เป็นข้อมูลที่ไม่ได้สูญเสียสิ่งเชื่อมโยงตัวบุคคลเป็นการถาวรเหมือนดังเช่นข้อมูลที่ผ่านกระบวนการ Anonymization อย่างไรก็ตาม GDPR ยังไม่บัญญัติครอบคลุมถึงข้อมูลที่ผ่านกระบวนการ Encryption เช่นเดิม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (APPI) บัญญัติให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการ Anonymization ได้อย่างมีประสิทธิภาพซึ่งจะทำให้สูญเสียสิ่งบ่งชี้ตัวบุคคลโดยถาวรแล้ว ผู้ให้บริการหรือผู้ควบคุมข้อมูลย่อมสามารถเปิดเผยข้อมูลดังกล่าวให้แก่บุคคลภายนอกได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล ดังนั้น หากตีความความเห็นดังกล่าวข้างต้นจะพบว่าข้อมูลที่ผ่านกระบวนการ Anonymization ภายใต้ APPI เป็นข้อมูลที่สูญเสียสิ่งเชื่อมโยงบุคคลจึงไม่ถือเป็นข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของ APPI อย่างไรก็ตาม APPI ไม่ได้บัญญัติครอบคลุมถึงกรณีของข้อมูลส่วนบุคคลที่ผ่านกระบวนการ Pseudonymization และกระบวนการ Encryption แต่อย่างใด

สำหรับประเทศไทย เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่าร่างพระราชบัญญัติดังกล่าวไม่ได้บัญญัติถึงข้อมูลที่ผ่านกระบวนการ Anonymization กระบวนการ Pseudonymization และกระบวนการ Encryption แต่อย่างใด ดังนั้น กรณีจึงเกิดความไม่แน่นอนว่าข้อมูลเหล่านี้จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... หรือไม่ ในปัจจุบัน

6.1.2 หลักการเรื่องผู้ควบคุมข้อมูลร่วมกัน (Joint Data Controller) ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ผู้ควบคุมข้อมูลร่วมกัน หมายถึง บุคคลธรรมดาหรือนิติบุคคลแยกต่างหากจากผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูลร่วมกันดังกล่าวจะเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวร่วมกันกับผู้ควบคุมข้อมูล ซึ่งเมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) เทียบกับกฎหมายคุ้มครอง

ข้อมูลส่วนบุคคลของสหภาพยุโรปทั้งฉบับเดิมและฉบับใหม่จะพบว่า ร่างพระราชบัญญัติของไทยไม่รองรับหลักการว่าด้วยผู้ควบคุมข้อมูลร่วมกัน ทั้งที่หลักการของผู้ควบคุมข้อมูลร่วมกันเป็นหลักการที่สำคัญที่จะช่วยรองรับการคุ้มครองข้อมูลส่วนบุคคลในระบบการประมวลผลแบบคลาวด์ เพราะในการให้บริการระบบการประมวลผลแบบคลาวด์นั้น ผู้ให้บริการและผู้ใช้บริการอาจอยู่ในสถานะของผู้ควบคุมข้อมูลร่วมกันได้ หากปรากฏข้อเท็จจริงว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประมวลผลข้อมูลดังกล่าวด้วยวิธีการและวัตถุประสงค์ที่ตกลงร่วมกันกับผู้ใช้บริการ ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศสมีความเห็นว่าผู้ใช้บริการและผู้ให้บริการระบบการประมวลผลแบบคลาวด์ประเภท Public SaaS และ Public PaaS มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน

6.1.3 หลักการเรื่องผู้ประมวลผลข้อมูลภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ผู้ประมวลผลข้อมูลส่วนบุคคลถือเป็นบุคคลสำคัญในการให้บริการระบบการประมวลผลแบบคลาวด์ เนื่องจากคณะทำงานของการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 29 (Article 29 Data Protection Working Party) พิจารณาว่าผู้ให้บริการระบบการประมวลผลแบบคลาวด์อยู่ในสถานะของผู้ประมวลผลข้อมูลส่วนบุคคล และเมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่าร่างพระราชบัญญัติฉบับนี้ได้รองรับหลักการเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลเอาไว้แล้ว แต่อย่างไรก็ตาม เมื่อพิจารณารายละเอียดบทบัญญัติเรื่องผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) จะพบว่า บทบัญญัติเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติดังกล่าวยังไม่ครอบคลุมเมื่อเทียบกับหลักเกณฑ์ในระดับสากล

6.1.4 หลักการเรื่องสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของเจ้าของข้อมูล (Data Portability)

สิทธิในการโอนย้ายข้อมูลส่วนบุคคลเป็นสิทธิที่กำหนดถึงการทำสำเนาของผู้ควบคุมข้อมูลหรือผู้ประมวลผลและส่งมอบให้แก่เจ้าของข้อมูล รวมถึงสิทธิในการโอนย้ายข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลรายหนึ่งไปยังผู้ควบคุมข้อมูลอีกรายหนึ่ง หรือผู้ประมวลผลรายหนึ่งไปยังผู้ประมวลผลอีกรายหนึ่ง ซึ่งจะสอดคล้องกับการใช้บริการระบบการประมวลผลแบบคลาวด์ที่อาจเปลี่ยนไปใช้บริการของผู้ให้บริการรายอื่นได้ ดังนั้น การขาดสิทธิดังกล่าวย่อมก่อให้เกิดความไม่

ต่อเนื่องจากในการใช้บริการระบบการประมวลผลแบบคลาวด์และก่อให้เกิดความยุ่งยากและความไม่คล่องตัวแก่เจ้าของข้อมูล ซึ่งจะเป็นผลกระทบต่อการแข่งขันภายในตลาดเทคโนโลยี

6.1.5 หลักการเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ข้อยกเว้นเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่กำหนดไว้ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ยังไม่เพียงพอกับการให้บริการระบบการประมวลผลแบบคลาวด์ ทั้งนี้ เนื่องจากในทางปฏิบัติของระบบการประมวลผลแบบคลาวด์ซึ่งผู้ให้บริการหลายรายมีบริษัทในเครือจำนวนมากเพื่อถือครองดาต้าเซ็นเตอร์หลายแห่งทั่วโลก ทำให้ต้องมีการส่งหรือโอนข้อมูลระหว่างบริษัทในเครือด้วยกันเองจำนวนมาก

6.1.6 การกำหนดโทษภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ความรับผิดทางแพ่ง: ร่างพระราชบัญญัตินี้กำหนดให้เฉพาะผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้นที่ต้องรับผิดทางแพ่ง แต่ในทางปฏิบัติย่อมมีโอกาสที่ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลได้

โทษอาญา: การกำหนดให้กรรมการต้องรับผิดกรณีที่ผู้กระทำความผิดเป็นนิติบุคคลไม่ช่วยให้ผู้ประกอบการเกิดความตระหนักในการให้ความคุ้มครองข้อมูลและในการปฏิบัติตามกฎหมาย

โทษปรับทางปกครอง: จำนวนโทษปรับทางปกครองยังไม่เพียงพอที่จะทำให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกิดความเกรงกลัวและปฏิบัติตามบทบัญญัติแห่งกฎหมายนี้อย่างเคร่งครัด

6.1.7 การมีผลใช้บังคับย้อนหลังของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

การที่ร่างพระราชบัญญัตินี้กำหนดให้ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลต่อไปได้ตามวัตถุประสงค์เดิม โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่ายนั้น ก่อให้เกิดช่องว่างในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ เพราะข้อมูลส่วนบุคคลโดยส่วนใหญ่มีกฎหมายเฉพาะที่กำหนดบทบัญญัติให้ผู้ที่เกี่ยวข้องต้องปฏิบัติตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับหลักการสากลอยู่แล้ว ในขณะที่

ข้อมูลส่วนบุคคลที่อยู่ในระบบการประมวลผลแบบคลาวด์ไม่มีกฎหมายใดให้ความคุ้มครองไว้โดยเฉพาะ การกำหนดให้ข้อมูลส่วนบุคคลทุกประเภทที่ผู้ควบคุมข้อมูลเก็บไว้ก่อนร่างพระราชบัญญัตินี้มีผลใช้บังคับสามารถเก็บรวบรวมและใช้ต่อไปได้ จึงไม่เป็นธรรม นอกจากนี้ในทางปฏิบัติบุคคลที่เก็บรวบรวมข้อมูลไม่ได้จำกัดเฉพาะผู้ควบคุมข้อมูลส่วนบุคคล แต่ยังรวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลด้วย

ฉะนั้น จากการศึกษาข้างต้นจึงอาจกล่าวโดยสรุปได้ว่า ประเทศไทยกำลังประสบปัญหาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์โดยปัญหาของประเทศไทยนั้น แบ่งออกเป็น 2 ระยะ กล่าวคือ ระยะแรก ประเทศไทยกำลังประสบปัญหาการขาดแคลนกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่จะบังคับใช้กับระบบการประมวลผลแบบคลาวด์ประการหนึ่ง และระยะสอง หากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่กำลังอยู่ในการพิจารณามีผลใช้บังคับแล้ว ประเทศไทยจะประสบปัญหาอีกประการหนึ่ง คือ ร่างพระราชบัญญัติดังกล่าวไม่สอดคล้องกับรูปแบบธุรกิจหรือรูปแบบการให้บริการระบบการประมวลผลแบบคลาวด์ ซึ่งจะทำให้ร่างพระราชบัญญัติที่มีผลใช้บังคับจะต้องเข้าสู่กระบวนการแก้ไขปรับปรุงใหม่อีกรอบซึ่งอาจใช้ระยะเวลายาวนานในการแก้ไขปรับปรุง ดังนั้น ประเทศไทยจึงควรพิจารณาแก้ไขร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ให้สอดคล้องกับรูปแบบการประกอบธุรกิจของระบบการประมวลผลแบบคลาวด์ และเร่งผลักดันให้กฎหมายที่ได้รับการแก้ไขมีผลใช้บังคับโดยเร็ว

6.2 ข้อเสนอแนะ

เพื่อประโยชน์ต่อการจัดทำกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมและเหมาะสมกับธุรกิจของการให้บริการระบบการประมวลผลแบบคลาวด์ที่กำลังได้รับความนิยมอย่างต่อเนื่อง ผู้เขียนมีความเห็นว่าประเทศไทยควรเร่งพิจารณาให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) มีผลบังคับใช้โดยเร็วและครอบคลุมถึงการให้บริการระบบการประมวลผลแบบคลาวด์ โดยอาจพิจารณาเทียบเคียงจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ผู้เขียนได้เพิ่มเติมหลักการและรายละเอียดการให้ความคุ้มครองข้อมูลส่วนบุคคลในประเด็นดังต่อไปนี้เข้าไป ทั้งนี้ เพื่อให้ร่างพระราชบัญญัติที่จะมีผลใช้บังคับเป็นกฎหมายนั้นสามารถคุ้มครองข้อมูลส่วนบุคคลได้ในความเป็นจริง โดยเฉพาะอย่างยิ่งในระบบการประมวลผลแบบคลาวด์

6.2.1 ขอบเขตของข้อมูลที่จะตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรกำหนดให้ชัดเจนว่าข้อมูลที่ผ่านกระบวนการ Anonymization กระบวนการ Pseudonymization และกระบวนการ Encryption ยังคงมีลักษณะเป็นข้อมูลส่วนบุคคลและตกอยู่ภายใต้บังคับของร่างพระราชบัญญัติหรือไม่ โดยผู้เขียนมีความเห็นว่า ข้อมูลที่ยังควรต้องอยู่ภายใต้บังคับของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ได้แก่ ข้อมูลที่ผ่านกระบวนการ Pseudonymization และกระบวนการ Encryption ทั้งนี้ เนื่องจากข้อมูลทั้งสองประเภท มีลักษณะเป็นข้อมูลที่สูญเสียสิ่งเชื่อมโยงบุคคลเป็นการชั่วคราวเท่านั้น ข้อมูลดังกล่าวจึงยังควรได้รับความคุ้มครองภายใต้ร่างพระราชบัญญัติฉบับนี้ ดังนั้น ร่างพระราชบัญญัติดังกล่าวจึงควรแก้ไขมาตรา 4 โดยการเพิ่มอนุมาตรา (6) ดังนี้

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภาพ รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(5) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

<u>(6) ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลลบสิ่งเชื่อมโยงตัวบุคคลออกอย่างถาวรจนทำให้ไม่สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม</u>

6.2.2 หลักการเรื่องผู้ควบคุมข้อมูลร่วมกัน (Joint Data Controller)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรบัญญัติรองรับหลักการของผู้ควบคุมข้อมูลร่วมกัน โดยกำหนดบทนิยามของผู้ควบคุมข้อมูลร่วมกันในมาตรา 6 ดังนี้

มาตรา 6 ในพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน หมายความว่า บุคคลหรือนิติบุคคลซึ่งกำหนดวิธีการและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลร่วมกับผู้อื่น

และกำหนดบทบัญญัติเกี่ยวกับหน้าที่ของผู้ควบคุมข้อมูลร่วมกันต่อการปฏิบัตตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายนี้ โดยกำหนดเพิ่มเป็นมาตรา 31/1 ดังนี้

มาตรา 31/1

ในกรณีที่ผู้ควบคุมข้อมูลตั้งแต่ 2 รายขึ้นไปร่วมกันตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการของการประมวลผลข้อมูลส่วนบุคคล บุคคลดังกล่าวถือเป็นผู้ควบคุมข้อมูลร่วมกันและต้องกำหนดความรับผิดชอบในการปฏิบัติหน้าที่ตามที่พระราชบัญญัตินี้กำหนด

หากผู้ควบคุมข้อมูลส่วนบุคคลร่วมกันไม่ได้ดำเนินการตามวรรคแรก ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดแทน

6.2.3 หลักการเรื่องผู้ประมวลผลข้อมูล (Data Processor)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรบัญญัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้ครอบคลุม ทั้งนี้ เพื่อให้สอดรับกับหลักการสากลและสามารถคุ้มครองเจ้าของข้อมูลส่วนบุคคลได้จริงในทางปฏิบัติโดยเพิ่มรายละเอียดเกี่ยวกับกับการกำหนดให้ผู้ประมวลผลข้อมูลมีหน้าที่แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที การกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถแต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งหากไม่มีกฎหมายกำหนดให้สามารถกระทำได้หรือหากไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล การกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการที่รับผิดชอบโดยไม่ชักช้า เนื่องจากในทางปฏิบัติบุคคลที่จะทราบการละเมิดข้อมูลส่วนบุคคลก่อนผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ผู้ประมวลผลข้อมูล และการกำหนดให้ผู้ประมวลผลข้อมูลจะต้องปฏิบัติตามบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล ไว้ในอนุมาตรา (4) – (7) ของมาตรา 30 ดังนี้

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

(4) แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที

(5) ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งโดยปราศจากกฎหมายกำหนดให้สามารถกระทำได้ หรือปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้าถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(7) ปฏิบัติตามบทบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

6.2.4 สิทธิการโอนย้ายข้อมูล (Data Portability)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรบัญญัติรองรับหลักเกี่ยวกับสิทธิในการโอนย้ายข้อมูลของเจ้าของข้อมูล เพื่อให้สอดคล้องกับพฤติกรรมการใช้บริการระบบการประมวลผลแบบคลาวด์ของผู้ใช้บริการและเพื่อให้สอดคล้องกับหลักการสากล โดย

(1) เพิ่มสิทธิของเจ้าของข้อมูลส่วนบุคคลในมาตรา 28/1 ดังนี้

มาตรา 28/1

เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับข้อมูลส่วนบุคคลเกี่ยวกับตนที่ได้มอบความยินยอมให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในรูปแบบที่ใช้กันอยู่ทั่วไปและเข้าใจง่าย และมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลโอนย้ายข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลอีกรายหนึ่งได้โดยปราศจากอุปสรรคใดๆ

ในการใช้สิทธิตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจร้องขอให้เจ้าของข้อมูลส่วนบุคคลพิสูจน์ว่าตนเองเป็นเจ้าของข้อมูลที่แท้จริงได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอเช่นว่านั้นได้ หากการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลไม่สามารถกระทำได้โดยง่ายในทางเทคนิค หรือ การดำเนินการเช่นว่านั้นอาจทำให้กระทบต่อสิทธิและเสรีภาพของบุคคลอื่น

(2) แก้ไขเพิ่มเติมมาตรา 29 (5) และมาตรา 30 (8) เพื่อเพิ่มหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลให้ต้องปฏิบัติตามสิทธิที่เจ้าของข้อมูลมีอยู่ ดังนี้

มาตรา 29 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ

(2) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(4) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 27 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(5) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

(4) แจ้งคำสั่งที่ขัดหรือแย้งกับกฎหมาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยทันที

(5) ไม่แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลอีกทอดหนึ่งโดยปราศจากกฎหมายกำหนดให้สามารถกระทำได้ หรือปราศจากความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล

(6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังคณะกรรมการโดยไม่ชักช้า

(7) ปฏิบัติตามบทบัญญัติว่าด้วยการโอนหรือส่งข้อมูลส่วนบุคคล

(8) ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 26 ถึงมาตรา 28/1

6.2.5 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรบัญญัติรองรับข้อยกเว้นเกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างบริษัทในเครือในลักษณะเดียวกันกับ GDPR โดยการแก้ไขเพิ่มเติมมาตรา 25 (5) ดังนี้

มาตรา 25 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 14 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(5) เป็นการโอนข้อมูลระหว่างบริษัทในเครือซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรที่ได้รับอนุมัติจากคณะกรรมการ

(6) กรณีอื่นตามที่กำหนดในกฎกระทรวง

6.2.6 การกำหนดโทษภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรแก้ไขบทกำหนดโทษดังต่อไปนี้

ความรับผิดทางแพ่ง: แก้ไขมาตรา 64 โดยเพิ่มให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดทางแพ่งด้วย ดังนี้

มาตรา 64 ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคล ของผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล นั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(3) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 14(6)

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

โทษทางอาญา: ตัดมาตรา 67 ออกจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

~~มาตรา 67 ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆ ด้วย~~

โทษปรับทางปกครอง: เพิ่มจำนวนโทษปรับทางปกครองโดยแก้ไขมาตรา 69 ถึงมาตรา 75 ดังนี้

มาตรา 69 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 20 มาตรา 26 วรรคสี่ มาตรา 31 หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 17 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 17 วรรคห้า ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้ของบริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 70 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ต้องระวางโทษปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 71 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 หรือฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 72 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 30 โดยไม่มีเหตุอันควร ต้องระวางโทษปรับทางปกครอง~~ไม่เกินสามแสนบาท~~ 5 ล้านบาทหรือ 2% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 73 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 62 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 63 วรรคสาม ต้องระวางโทษปรับทางปกครอง~~ไม่เกินหนึ่งแสนบาท~~ 2 ล้านบาท หรือ 1% ของรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

มาตรา 74 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับทางปกครอง~~ไม่เกินห้าแสนหบาท~~ 10 ล้านบาท หรือ 4% ชองรายได้บริษัทในปีที่ไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมาย

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

6.2.7 การมีผลใช้บังคับย้อนหลังของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ) ควรแก้ไขมาตรา 83 เพื่อให้เกิดความเป็นธรรมต่อการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในระบบการประมวลผลแบบคลาวด์ ดังนี้

มาตรา 83 ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้ว ก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

การดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้โดยไม่ได้ปฏิบัติตามบทบัญญัติแห่งกฎหมายเฉพาะว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

บรรณานุกรม

หนังสือและบทความในหนังสือ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. คู่มือการเลือกใช้บริการ Cloud Computing, กรุงเทพมหานคร:กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2556.

โจวาน เคอร์บาลิจา. An Introduction to Internet Governance เปิดประตูสู่การอภิบาลอินเทอร์เน็ต. แปลโดย พิภพ อุดมอิทธิพงศ์. กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง. 2558.

นคร เสรีรักษ์. การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอสำหรับประเทศไทย. กรุงเทพมหานคร: บริษัท พี.เพรส จำกัด, 2559.

_____. ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. กรุงเทพมหานคร: พี.เพรส, 2557.

บุญญรัตน์ โชคบันดาลชัย. กฎหมายสื่อสารมวลชน: การคุ้มครองสิทธิส่วนบุคคลและชื่อเสียงเกียรติคุณ. พิษณุโลก: สำนักพิมพ์มหาวิทยาลัยนเรศวร, 2558.

มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง. โลกใหม่ใครกำกับ? กรณีศึกษาเกี่ยวกับอินเทอร์เน็ต. กรุงเทพมหานคร:มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2558.

ศรีราชา เจริญพานิช. คำอธิบายกฎหมายว่าด้วยทรัพย์สิน. พิมพ์ครั้งที่ 5. กรุงเทพฯ : วิญญูชน, 2557.

สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. กรุงเทพมหนาคร: สำนักพิมพ์นิติธรรม, 2555.

อาณัติ รัตนถิรกุล. ก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ในองค์กร (ภาคปฏิบัติ). กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น, 2558.

บทความวารสาร

กิตติศักดิ์ ปรกติ. “กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 514.

ชั่งทอง โอภาสศิริวิทย์. “การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในประเทศไทย: ปัจจุบันและอนาคต.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 613.

จันทจิรา เอี่ยมมยุรา. “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 627.

_____. “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 653.

จุฬารัตน์ ยะปะนัน. “ร่างกฎหมายที่น่าสนใจ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” จุลนิติ ฉบับที่ 3. ปีที่ 7. (พฤษภาคม – มิถุนายน 2553): 75.

จอมพล พิทักษ์สันตโยธิต. “APEC privacy framework กับความพร้อมด้านกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.” บทบัณฑิตย์ เล่มที่ 70. (ธันวาคม 2557): 136.

อรอมล อาระพล, “หลักการคุ้มครองข้อมูลส่วนบุคคล: กรอบแนวคิดในทางระหว่างประเทศ.” Thailand Economic & Business Review ฉบับที่ 4. ปีที่12. (เมษายน 2559): 44.

ประสิทธิ์ ปิวาวัฒนพาณิช. “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 535.

ปฏิวัติ อุ่นเรือน. “การโอนข้อมูลส่วนบุคคลระหว่างประเทศ.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 34. ฉบับที่ 4. (ธันวาคม 2547): 557.

เพชรรัตน์ จงปัญญาประพันธ์. “ความสำคัญของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีที่ 33. ฉบับที่ 4. (ธันวาคม 2546): 823.

เพลินตา ตันรังสรรค์. “โครงการเสวนาให้ความเห็นต่อร่างกฎหมาย เรื่อง “ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” จุลนิติ 73. ฉบับที่ 5. ปีที่ 7. (กันยายน – ตุลาคม 2553): 77.

ลันตา อุตมะโภคิน. “ร่างกฎหมายที่น่าสนใจ: ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” จุลนิต ฉบับที่ 3. ปีที่ 11. (พฤษภาคม – มิถุนายน 2557): 75.

วิวัฒน์ มีสุวรรณ์. “ระบบประมวลผลแบบกลุ่มเมฆในงานทางการศึกษา (Cloud Computing for Education).” วารสารศึกษาศาสตร์ มหาวิทยาลัยนเรศวร ปีที่ 16. ฉบับที่ 1. (มกราคม - มีนาคม 2557): 149.

ศรีสมรัก อินทุจันทร์ยง. “การประมวลผลในกลุ่มเมฆ (Cloud Computing).” วารสารบริหารธุรกิจ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์ ปีที่ 33. ฉบับที่ 128. (ตุลาคม-ธันวาคม 2553): 14.

สุภัทท์ บุญญานนท์. “คำอธิบายกฎหมายไอทีในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....” สรรพากรสาส์น ฉบับที่ 12. ปีที่ 49. (ธันวาคม 2545): 65.

อริยพร โพธิใส. “หลักการให้ความคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย.” จุลนิติ ฉบับที่ 5. ปีที่ 11. (กันยายน – ตุลาคม 2557): 137.

วิทยานิพนธ์

กิตติพงศ์ กมลธรรมวงศ. “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย: ปัญหาและแนวทางแก้ไข.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549.

ชาญชัย อรรคผาติ. “ปัจจัยที่ส่งผลต่อทัศนคติในการยอมรับในเทคโนโลยีคลาวด์คอมพิวติ้ง เพื่อประยุกต์ใช้ในการให้บริการระบบบัญชีออนไลน์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในมุมมองของผู้ทำบัญชี.” วิทยานิพนธ์มหาบัณฑิต คณะการบัญชี มหาวิทยาลัยธรุกิจบัณฑิตย์, 2557.

ชินดนัย สังคะคุณ. “การจัดเก็บภาษีเงินได้นิติบุคคลจากการให้บริการของบริษัทต่างประเทศ: กรณีการให้บริการประมวลผลแบบคลาวด์.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558.

น้ำทิพย์ บุญเกิด. “ความรับผิดทางอาญากรณีละเมิดข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์.” สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

นคร เสรีรักษ์. “การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย.” วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต สาขาวิชาสหวิทยาการ คณะบัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2548.

นัทรี เกตุแก้ว. “ความรับผิดทางแพ่งของผู้ให้บริการ Cloud Computing.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557.

พนิดา พูลสวัสดิ์. “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2556.

สุภิชัย สิริชัยรังสรรค์. “การจัดเก็บภาษีเงินได้นิติบุคคลจากบริษัทต่างประเทศจากการพาณิชย์อิเล็กทรอนิกส์.” สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

สื่ออิเล็กทรอนิกส์

ธนาคารแห่งประเทศไทย. “ประกาศธนาคารแห่งประเทศไทยที่ สนส. 19/2559 เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน.” https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2560/ThaiPDF/25600035.pdf, 15 เมษายน 2561.

บีเอสเอ แอนด์ กาแล็กซี่. “ผลการประเมินความพร้อมของประเทศต่างๆ ทั่วโลก สำหรับเทคโลโยลีคลาวด์คอมพิวติ้ง โดยบีเอสเอ (BSA) ประจำปี พ.ศ. 2559 : การเผชิญหน้ากับความท้าทายใหม่.” http://cloudscorecard.bsa.org/2016/Pdf/BSA_2016_Global_Cloud_Score card_th.pdf, 10 ตุลาคม 2559.

_____. “เทคโนโลยีการประมวลผลแบบกระจาย (Distributed Computing).” http://app.eduzones.com/portal/siamese/1924, 18 กันยายน 2559.

_____. "Cloud Computing คืออะไร? Cloud Computing ดีอย่างไร." http://www.it24hrs.com/2015/cloud-computing-and-cloud-definition, 26 สิงหาคม 2559.

_____. "การให้บริการของ Cloud Provider มั่นใจได้จริงหรือ?" http://www.acinfotec.com/2015/12/03/cloud-provider/, 26 สิงหาคม 2559.

_____. "โครงสร้างพื้นฐานของระบบ Cloud Computing." https://blog.sogoodweb.com/Article/Detail/9115, 10 มกราคม 2560.

ราชบัณฑิตยสถาน. "พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๕๔." http://www.royin.go.th/dictionary, 30 ธันวาคม 2559.

ศูนย์ข้อมูลข่าวสาร สป.ทส. "คู่มือการปฏิบัติงานตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ." http://slc.mnre.go.th, 5 มีนาคม 2560.

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. "คำศัพท์ Cloud computing." http://www.thaiglossary.org/node/51370, 18 กันยายน 2559.

สำนักงานรัฐบาลอิเล็กทรอนิกส์. "ประวัติความเป็นมา." https://www.ega.or.th/th/profile_History/, 15 เมษายน 2561.

สำนักงานรัฐบาลอิเล็กทรอนิกส์. "G-Cloud อีจีเอ ตอบโจทย์หน่วยงานภาครัฐ เผย ก.สาธารณสุข แชมป์ใช้งานคลาวด์พร้อมดันบริการใหม่ๆเข้าระบบ."https://www.ega.or.th/th/content/913/11935, 15 เมษายน 2561.

BOOKS

Buyya, Rajkumar, Broberg, James Goscinski and Andrzej. Cloud computing: principles and paradigms. Hoboken, NJ: Wiley, 2011.

Chris Reed. Computer Law. Seventh Edition. New York. Oxford University Press Inc., 2011.

Christopher Kuner. European Data Privacy Law and Online Business. New York: Oxford University Press Inc., 2003.

Diane Rewland and Elizabeth Macdonald. Information Technology Law. Second Edition. Great Britain, 2000.

Graham J H Smith Bird & Bird. Internet Law and Regulation. Fourth Edition. London: Sweet & Maxwell, 2007.

Global Legal Group. The International Comparative Legal Guide to: Data Protection 2016. United Kingdom: Global Legal Group, 2016.

Lan J Lloyd, Information Technology Law. Fourth edition. United States: Oxford University Press Inc., 2005.

Leenes, Ronald Brakel, Rosamunde van Gutwirth, Serge Hert, Paul De. Data Protection and Privacy: (In) visibilities and Infrastructures. Springer, 2017.

Timothy J. O'Leary, Linda I. O'Leary, Daniel A. O'Leary. คอมพิวเตอร์และเทคโนโลยีสารสนเทศสมัยใหม่. แปลโดย ศศลักษณ์ ทองขาวและคณะ. กรุงเทพมหานคร: แมคกรอ-ฮิล อินเตอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2558.

Peter Carey. Data Protection A Practical Guide to UK and EU Law. New York: Oxford University Press Inc., 2004.

Velte, Toby J. and Elsenpeter, Robert. Cloud computing : a practical approach. New York, N.Y. : McGraw Hill, 2010.

Winnie Chang. A Practical Guide To Singapore Data Protection Law. Singapore. C.O.S. Printers Pte Ltd, 2013.

ARTICLES

Ahmed E. Youssef. "Exploring Cloud Computing Services and Applications." Journal of Emerging Trends in Computing and Information Sciences. Vol.3. No.6. (July 2012).

Anna Kaushil and Ashok Kumar. "Application of Cloud Computing in Libraries." International Journal of Information Dissemination and Technology, Vol.3. Issue 4. (October-December 2013).

Anthony Bisong and Syed (Shawon) M. Rahman. "An overview of the security concerns in enterprise cloud computing." International Journal of Network Security & Its Applications (IJNSA). Vol.3. No.1. (January 2011).

Aysem Diker Vanberg and Mehmet Bilal Ünver. "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?." EJLT European Journal of Law and Technology. Vol 8. No.1. (2017).

Aysem Diker Vanberg. "The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?." Journal of Internet law. Vol.21. Number 7. (January 2018).

Bunkar, R. K.; Rai, P. K. "STUDY ON SECURITY MODEL IN CLOUD COMPUTING." International Journal of Advanced Research in Computer Science. Vol. 8. Issue 7. (July – August 2017).

Carla Bulford. "Between East and West: The APEC Privacy Framework and the Balance of International Data Flows." I/S Journal of law and policy for the information society. (2012).

Citizens Information Board. "General Data Protection Regulation (GDPR)." The journal of developments in social services, policy and legistration in Ireland. Volume 44. Issue 8. (August 2017).

Fuster, Gloria Gonzalez. “Security and the future of personal data protection in the European Union.” Security & Human Rights. Vol. 23. Issue 4. (2013).

Gerald Spindler and Philipp Schmechel. “Personal Data and Encryption in the European General Data Protection Regulation.” Journal of Intellectual Property, Information Technology and E-Commerce Law. Volume 7. (September, 2016): 164.

Gilbert, Francoise. “Security and the future of personal data protection in the European Union.” Journal of Internet Law. Vol. 19. Issue 11. (May 2016).

Gellert, Raphaël. “Understanding Data Protection as a risk regulation.” Journal of Internet Law. Vol. 18. Issue 11. (May 2015).

Mark Webber. “The GDPR’s impact on the cloud service provider as a processor.” Privacy & Data Protection Journal. Volume 16. Issue 4. (2016).

McCallister, Jennifer; Zanfir-Fortuna, Gabriela; Mitchell, Jennifer. “Getting ready for the EU’s stringent data privacy rule.” Journal of Accountancy. Vol. 225. Issue 1. (January 2018).

Michelle Goddard. “The EU General Data Protection Regulation (GDPR): European regulation that has a global impact.” International Journal of Market Research. Vol. 59. Issue 6. (November 2017).

Mohsin Nazir. “Cloud Computing: Overview & Current Research Challenges.” IOSR Journal of Computer Engineering. Volume 8. Issue 1. (November – Decemeber 2012).

Noriko Higashizawa and Yuri Aihara. “Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan).” Defense Counsel Journal. Vol. 84. Issue 4. (2017).

R. Arokia Paul Rajan and S. Shanmugapriyaa. “Evolution of Cloud Storage as Cloud Computing Infrastructure Service.” IOSR Journal of Computer Engineering. Vol.1. Issue 1. (May – June 2012).

Romansky, Radi. “Cloud Services: Challenges for personal data protection.” International Journal on Information Technologies & Security. Vol. 4. Issue 3. (2012).

Safari, Beata A. “INTANGIBLE PRIVACY RIGHTS: HOW EUROPE'S GDPR WILL SET A NEW GLOBAL STANDARD FOR PERSONAL DATA PROTECTION.” Seton Hall Law Review. Vol. 47. Issue 3. (2017).

Santosh Kumar and R.H. Goudar. “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A survey.” International Hournal of Future Computer and Communication. Vol.1. No.4. (December 2012).

TIAN, GEORGE YIJUN. “Current Issues of cross-boarder personae data protection in the context of cloud computing and trans-pacific partnership agreement: join or withdraw.” Wisconsin International Law Journal. Vol. 34. Issue 2. (Winter 2016).

Tzolov, Tzanko. “Data Model in the context of the general data protection regulation.” International Journal on Information Technologies & Security. Vol. 9. Issue 4. (2017).

Vidović, Marina krinjar. “EU DATA PROTECTION REFORM: CHALLENGES FOR CLOUD COMPUTING.” Croatian Yearbook of European Law & Policy. Vol. 12. (2016).

ELECTRONIC MEDIAS

Alesia Bulanok and Alex Khizniak. “The Government of South Korea Creates an Open PaaS with Cloud Foundry.” https://www.altoros.com/blog/south-korea-adopts-cloud-foundry-as-its-paas/, April 16, 2018.

Alston & Bird. “An English-Language Primer on Germany’s GDPR Implementation Statute: Part 1 of 5” https://www.jdsupra.com/legalnews/an-english-language-primer-on-germany-s-59204/, September 30, 2017.

BSA. “2018 BSA Global Cloud Computing Scorecard Powering a Bright Future.” http://cloudscorecard.bsa.org/2018/, February 2, 2018.

Cattelecom. “IRIS Platform Innovative Cloud Ecosystem by CAT.” http://iris.cattelecom.com/en, October 10, 2016.

Chris Copland. “Betterworking appointed to UK Government G-Cloud procurement framework.” http://www.betterworking.com/blog/betterworking-appointed-to-uk-government-g-cloud-procurement-framework/, April 15, 2018.

Commission Nationale De l’informatique et des libertés. “Recommendations for companies planning to use Cloud Computing services.” https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf, April 17, 2018.

DPL Piper. “New amendments to Japanese privacy law.” https://www.dlapiper.com/en/japan/insights/publications/2015/09/new-amendments-to-japanese-privacy-law/, February 28, 2017.

Eleni Frantziou. “Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos.” https://academic.oup.co/hrlr/article/14/4/761/644686/Further-Developments-in-the-Right-to-be-Forgotten, September 18, 2016.

Eric Kosinski and Shino Asayama. “Transfer of Personal Data Under Japan's Amended Personal Information Protection Act.” https://www.whitecase.com/publications/article/transfer-personal-data-under-japans-amended-personal-information-protection-act, March 6, 2017.

European Data Protection Supervisor. “The History of the General Data Protection Regulation.”https://edps.europa.eu/data-protection/data-protection/legislation /history-general-data-protection-regulation_en, February 24, 2560.

INET. “About INET.” https://inet.co.th/ about/index.php?MainID=4, October 10, 2016.

Jim Manica. “Dell Trying to Trademark Cloud Computing.” https://www.informationweek.com/mobile/dell-trying-to-trademark-cloud-computing/d/d-id/1070638?, January 10, 2017.

Jongjin. "ระบบประมวลผลกลุ่มเมฆ(Cloud Computing)." http://www.vcharkarn.com/blog/ 38378/4390, August 28, 2016.

Lennart Schüßler and Natallia Karniyevich. “Germany is the first EU Member State to enact new Data Protection Act to align with the GDPR.” https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr, July 20, 2017.

Microsoft. “ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud.” https://www.microsoft.com/en-us/TrustCenter/Compliance/iso-iec-27018, June 23, 2017.

Miguel Recio. “Mexico's new public-sector data protection law.” https://iapp.org/news/a/mexicos-new-public-sector-data-protection-law/, September 30, 2017.

Nadezhda Purtova. “Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence.” https://papers.ssrn.com/sol3/papers.cfm?abstract_Id=1641027, February 2, 2018.

_____. “Illusion of Personal Data as No One's Property.” https://papers.ssrn.com/sol3/papers.cfm?abstract_Id=2346693, February 2, 2018.

Nophakhun Limsamarnphun. “Thai law needs to catch up with the cloud.” http://www.nationmultimedia.com/news/national/3 0 3 0 1 6 3 1 , February 20, 2017.

OECD. “THIRTY YEARS AFTER THE OECD PRIVARY GUIDELINES.” http://www.oecd.org/sti/ieconomy/49710223.pdf, October 20, 2016.

Pamela Samuelson. “Privacy As Intellectual Property?” http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf, February 2, 2018

Privacy laws and business. “Mexico: DP regulations enter into force.” https://www.privacylaws.com/Publictions/enews/International-E-news/Dates/2012/1/Mexicao-DP-regulations-enter-into-force, September 29, 2016.

SIVADON. “จาก Grid Computing ไปถึง Cloud Computing ตอนที่ 1.” https://javaboom.wordpress .com /2008/11/27/grid2cloud_pt1/, September 18, 2016.

_____. “จาก Grid Computing ไปถึง Cloud Computing ตอนที่ 2.”https://javaboom.wordpress .com /2010/07/02/grid2cloud_pt2/, September 18, 2016.

SuperGrit, “รับมือภัยพิบัติด้วย “คลาวด์ คอมพิวติ้ง.” https://www.blognone.com/node/30896, November 11, 2017.

Thai Netizen Network. “รายงานการละเมิดความเป็นส่วนตัวออนไลน์ไทย พ.ศ. 2556.” https://thainetizen.org/privacy-report-2013/, February 19, 2017.

Thanakrit Lersmethasakul. “e-Government Cloud Computing.” https://www/slideshare.net/lersmethasakul/e-government-cloud-service, April 15, 2018.

The U.S. Department of Commerce’s International Trade Administration, “Overview of Cloud Computing in Japan.” https://www.export.gov/article?id=Overview-of-Cloud-Computing-in-Japan, April 15, 2018.

True IDC. “About us – True IDC.” https://www.trueidc.com/about/th, October 10, 2016.

TOT, “TOT Cloud,” http://www.tot.co.th/SME/Content.aspx?id=E4491781 7805434BBEB8DB5D1D1F0F3D, October 10, 2017.

ภาคผนวก

ภาคผนวก ก

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปฉบับเดิม (DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between

all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the

protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in

respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from

him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas

the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a

Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant

to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the

processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure

that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information

proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII
CONFIDENTIALITY AND SECURITY OF PROCESSING
Article 16
Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17
Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take

place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or

admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority

or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.
6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.
2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.
The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.
The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:
- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.
When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

ภาคผนวก ข
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปฉบับใหม่ (The General Data Protection Regulation)

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1)The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2)The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3)Directive 95/46/EC of the European Parliament and of the Council [4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4)The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data,

freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5)The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6)Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7)Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8)Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9)The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels

of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10)In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11)Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12)Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13)In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the

internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC [5].

(14)The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15)In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16)This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17)Regulation (EC) No 45/2001 of the European Parliament and of the Council [6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18)This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the

holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19)The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council ([7]). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20)While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data

when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21)This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council [(8)], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22)Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23)In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24)The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour

takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25)Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26)The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27)This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28)The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.

(29)In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept

separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30)Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31)Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32)Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33)It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34)Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35)Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [(9)] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36)The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory

authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37)A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38)Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39)Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be

processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40)In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41)Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42)Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [(10)] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43)In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to

be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44)Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45)Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46)The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47)The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their

relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48)Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49)The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

(50)The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51)Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by

the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52)Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53)Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or

historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54)The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [(11)], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55)Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56)Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57)If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the

digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58)The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59)Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60)The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61)The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the

circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62)However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63)A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64)The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller

should not retain personal data for the sole purpose of being able to react to potential requests.

(65)A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66)To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67)Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68)To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69)Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70)Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time

and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71)The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72)Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73)Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74)The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75)The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data

are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76)The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77)Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78)The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to

fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79)The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80)Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81)To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the

processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82)In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83)In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84)In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85)A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their

personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86)The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87)It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88)In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-

enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89)Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90)In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91)This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects

from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92)There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93)In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94)Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95)The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96)A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal

data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97)Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98)Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99)When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100)In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101)Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of

protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102)This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103)The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104)In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member

States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105)Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106)The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council [(12)] as established under this Regulation, to the European Parliament and to the Council.

(107)The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108)In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109)The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110)A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111)Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and

necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112)Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113)Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country

of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114)In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115)Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116)When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information

and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117)The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118)The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119)Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120)Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121)The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122)Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this

Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123)The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124)Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125)The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory

authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126)The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127)Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned (‘one-stop-shop mechanism’), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128)The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129)In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and

authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130)Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131)Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible

infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132)Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133)The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134)Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135)In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136)In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding

decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137)There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138)The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139)In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140)The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141)Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject

considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142)Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143)Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative,

corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144)Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145)For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146)The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147)Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council [(13)] should not prejudice the application of such specific rules.

(148)In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner

in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an

equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152)Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153)Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154)This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data

pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council [(14)] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155)Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156)The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to

object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157)By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158)Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159)Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public

health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160)Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161)For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (15) should apply.

(162)Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163)The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council (16) provides further specifications on statistical confidentiality for European statistics.

(164)As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing

Member State obligations to adopt rules on professional secrecy where required by Union law.

(165)This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166)In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167)In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168)The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169)The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170)Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171)Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172)The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 ([17]).

(173)This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à-vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ([18]), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b)by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d)by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a)the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b)the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1)‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2)‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3)‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(4)‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5)‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6)‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7)‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8)‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9)‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10)‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11)‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12)‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13)‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14)‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15)‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16)‘main establishment’ means:

(a)as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b)as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17)'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18)'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19)'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20)'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21)'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22)'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a)the controller or processor is established on the territory of the Member State of that supervisory authority;

(b)data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23)'cross-border processing' means either:

(a)processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b)processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24)'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the

risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25)'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [19];

(26)'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c)processing is necessary for compliance with a legal obligation to which the controller is subject;

(d)processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for

which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a)any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b)the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c)the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e)the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a)the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b)processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c)processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d)processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e)processing relates to personal data which are manifestly made public by the data subject;

(f)processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g)processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h)processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i)processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j)processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data

subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a)charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a)the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c)the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d)where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f)where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a)the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b)the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c)where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e)whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a)the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c)the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f)where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a)the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b)where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c)the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d)where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f)from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a)within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b)if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c)if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b)the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c)obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d)where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c)the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d)where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e)the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g)where the personal data are not collected from the data subject, any available information as to their source;

(h)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a)the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b)the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c)the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e)the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f)the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b)for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c)for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d)for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a)the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b)the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c)the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d)the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable

format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a)the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular

situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a)is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d)the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e)other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g)the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h)a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f)the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h)the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to

demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a)processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a)processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b)ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d)respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e)taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f)assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g)at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h)makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.

Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a)the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c)a description of the categories of data subjects and of the categories of personal data;

(d)the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f)where possible, the envisaged time limits for erasure of the different categories of data;

(g)where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a)the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d)where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a)describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b)communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d)describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a)the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b)the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c)it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in

a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a)a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b)processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a)a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b)an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c)an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d)the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks

of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a)where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c)the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a)the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b)the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c)the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a)to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b)to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c)to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e)to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g)the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h)the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i)the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k)out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a)demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b)established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c)established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d)demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63.

Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b)the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council [(20)] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a)demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b)undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c)established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d)established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the

controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e)demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a)the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b)the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c)the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a)are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b)expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a)the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b)the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d)the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e)the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f)the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g)how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h)the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j)the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k)the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l)the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m)the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n)the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a)the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b)the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c)the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f)the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g)the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a)develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b)provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c)engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d)promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b)the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c)the rules and procedures for the appointment of the member or members of each supervisory authority;

(d)the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e)whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f)the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of

office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b)promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c)advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d)promote the awareness of controllers and processors of their obligations under this Regulation;

(e)upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f)handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g)cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h)conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i)monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j)adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k)establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m)encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n)encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o)where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p)draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q)conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u)keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a)to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d)to notify the controller or the processor of an alleged infringement of this Regulation;

(e)to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f)to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a)to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b)to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c)to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d)to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g)to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h)to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i)to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j)to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a)to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b)to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c)to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant

shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a)it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b)compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the

request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the

law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a)aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b)concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c)aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d)aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a)the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b)the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a)where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b)where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c)where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a)monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b)advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c)advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d)issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e)examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k)draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l)review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m)issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n)encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o)carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p)specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q)provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s)provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t)issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u)promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v)promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w)promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x)issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y)maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b)to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c)to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g)the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council [(21)].

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a)the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c)any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d)the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f)the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h)the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i)where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j)adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k)any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a)the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a)the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c)the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e)non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and

benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a)Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

---

(1) OJ C 229, 31.7.2012, p. 90.

(2) OJ C 391, 18.12.2012, p. 127.

(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(5) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

(6) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(7) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

(8) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(9) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(10) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

(11) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(12) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

([13]) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

([14]) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

([15]) Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

([16]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

([17]) OJ C 192, 30.6.2012, p. 7.

([18]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([19]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

([20]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

([21]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

ภาคผนวก ค
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on the Protection of Personal Information (Act No.57 of 2003) and Amended Act on the Protection of Personal Information)

Act on the Protection of Personal Information

(Act No. 57 of May 30, 2003)

Chapter I General Provisions

(Purpose)

Article 1 The purpose of this Act is to protect the rights and interests of individuals while taking consideration of the usefulness of personal information, in view of a remarkable increase in the utilization of personal information due to development of the advanced information and communications society, by clarifying the responsibilities of the State and local governments, etc. with laying down basic principle, establishment of a basic policy by the Government and the matters to serve as a basis for other measures on the protection of personal information, and by prescribing the duties to be observed by entities handling personal information, etc., regarding the proper handling of personal information.

(Definitions)

Article 2 (1) The term "personal information" as used in this Act shall mean information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

(2) The term "a personal information database, etc." as used in this Act shall mean an assembly of information including personal information as set forth below:

(i) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

(ii) in addition to what is listed in the preceding item, an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved.

(3) The term "a business operator handling personal information" as used in this Act shall mean a business operator using a personal information database, etc. for its business; however, the following entities shall be excluded;

(i) The State organs

(ii) Local governments

(iii) Incorporated administrative agencies, etc. (which means independent administrative agencies

as provided in paragraph (1) of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003); the same shall apply hereinafter)

(iv) Local independent administrative institutions (which means local incorporated administrative agencies as provided in paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003); the same shall apply hereinafter)

(v) Entities specified by a Cabinet Order as having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of utilization of personal information they handle.

(4) The term "personal data" as used in this Act shall mean personal information constituting a personal information database, etc.

(5) The term "retained personal data" as used in this Act shall mean such personal data over which a business operator handling personal information has the authority to disclose, to correct, add or delete the content, to discontinue its utilization, to erase, and to discontinue its provision to a third party, excluding the data which is specified by a Cabinet Order as harming public or other interests if its presence or absence is known and the data which will be erased within a period of no longer than one year that is specified by a Cabinet Order.

(6) The term "person" as to personal information as used in this Act shall mean a specific individual identified by personal information.

(Basic Principle)

Article 3 In view of the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information shall be promoted.

Chapter II Responsibilities of the State and Local governments, etc.

(Responsibilities of the State)

Article 4 The State shall be responsible for comprehensively formulating and implementing measures necessary for ensuring the proper handling of personal information in conformity with the purport of this Act.

(Responsibilities of Local governments)

Article 5 Local governments shall be responsible for formulating and implementing the measures necessary for ensuring the proper handling of personal information according to the

characteristics of their area in conformity with the purport of this Act.

(Legislative Measures, etc.)

Article 6 The Government shall take necessary legislative and other measures to ensure that special measures will be taken for the protection of the personal information which especially needs to be ensured the strict implementation of its proprer handling for the further protection of the rights and interests of individuals in view of the nature and the method of utilization of the personal information.

Chapter III Measures for the Protection of Personal Information, etc.

Section 1 Basic Policy on the Protection of Personal Information

Article 7 (1) The Government shall establish a basic policy on the protection of personal information (hereinafter referred to as "Basic Policy") in order to ensure the comprehensive and integrated promotion of measures for the protection of personal information.

(2) The Basic Policy shall cover the following matters:

(i) The basic direction concerning the promotion of measures for the protection of personal information

(ii) Matters concerning the measures for the protection of personal information to be taken by the State

(iii) Basic matters concerning the measures for the protection of personal information to be taken by local governments

(iv) Basic matters concerning the measures for the protection of personal information to be taken by incorporated administrative agencies, etc.

(v) Basic matters concerning the measures for the protection of personal information to be taken by local incorporated administrative agencies.

(vi) Basic matters concerning the measures for the protection of personal information to be taken by entities handling personal information and authorized personal information protection organizations provided in paragraph (1) of Article 40

(vii) Matters concerning the smooth processing of complaints about the handling of personal information

(viii) Other important matters concerning the promotion of measures for the protection of personal information

(3) The Prime Minister shall prepare a draft of the Basic Policy, consulting the Quality of Life Council, and seek a cabinet decision.

(4) When a cabinet decision is made under the preceding paragraph, the Prime Minister shall publicly announce the Basic Policy without delay.

(5) The provisions of the preceding two paragraphs shall apply mutatis mutandis to amendments to the Basic Policy.

Section 2 Measures of the State

(Support to Local Governments and Others)

Article 8 In order to support the measures for the protection of personal information formulated or implemented by local governments and the activities performed by citizens, entities, and others to ensure the proper handling of personal information, the State shall provide information, formulate guidelines to ensure the appropriate and effective implementation of measures to be taken by entities and others, and take any other necessary measures.

(Measures for the Processing of Complaints)

Article 9 The State shall take necessary measures to ensure the appropriate, prompt processing of complaints arising between a business operator and a person about the handling of personal information concerning the person.

(Measures to Ensure Proper Handling of Personal Information)

Article 10 Through the appropriate division of roles between the State and local governments, the State shall take necessary measures to ensure the proper handling of personal information by entities handling personal information provided in the next chapter.

Section 3 Measures of Local Governments

(Protection of Personal Information Held by Local Governments and Others)

Article 11 (1) A local government shall endeavor to take necessary measures in order to ensure the proper handling of the personal information it holds in consideration of the nature of the personal information, the purpose of holding the personal information concerned, and other factors.

(2) A local government shall endeavor to take necessary measures for local incorporated administrative agencies established by it in order to ensure the proper handling of the personal information they hold in accordance with the nature and affairs of them..

(Support to Entities and Others in the Area)

Article 12 In order to ensure the proper handling of personal information, a local government shall endeavor to take necessary measures for supporting entities and residents in its area.

(Mediation for the Processing of Complaints, etc.)

Article 13 In order to ensure that any complaint arising between a business operator and a person about the handling of personal information will be handled appropriately and promptly, a local government shall endeavor to mediate the processing of complaints and take other necessary measures.

Section 4 Cooperation between the State and Local governments

Article 14 The State and local governments shall cooperate in taking measures for the protection of personal information.

Chapter IV Duties of Entities Handling Personal Information, etc.

Section 1 Duties of Entities Handling Personal Information

(Specification of the Purpose of Utilization)

Article 15 (1) When handling personal information, a business operator handling personal information shall specify the purpose of utilization of personal information (hereinafter referred to as "Purpose of Utilization") as much as possible.

(2) A business operator handling personal information shall not change the Purpose of Utilization beyond the scope which is reasonably considered that the Purpose of Utilization after the change is duly related to that before the change.

(Restriction by the Purpose of Utilization)

Article 16 (1) A business operator handling personal information shall not handle personal information about a person, without obtaining the prior consent of the person, beyond the scope necessary for the achievement of the Purpose of Utilization specified pursuant to the provision of the preceding article.

(2) When a business operator handling personal information has acquired personal information as a result of taking over the business of another business operator handling personal information in a merger or otherwise, the acquiring business operator shall not handle the personal information concerned, without obtaining the prior consent of the persons, beyond the scope

necessary for the achievement of the Purpose of Utilization of the personal information concerned before the succession.

(3) The provisions of the preceding two paragraphs shall not apply to the following cases:

(i) Cases in which the handling of personal information is based on laws and regulations

(ii) Cases in which the handling of personal information is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person

(iii) Cases in which the handling of personal information is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person

(iv) Cases in which the handling of personal information is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by either of the former two in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person is likely to impede the execution of the affairs concerned

(Proper Acquisition)

Article 17 A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.

(Notice of the Purpose of Utilization at the Time of Acquisition, etc.)

Article 18 (1) When having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization.

(2) Notwithstanding the provision of the preceding paragraph, when a business operator handling personal information acquires such personal information on a person as is written in a contract or other document (including a record made by an electronic method, a magnetic method, or any other method not recognizable to human senses. hereinafter the same shall apply in this paragraph.) as a result of concluding a contract with the person or acquires such personal information on a person as is written in a document directly from the person, the business operator shall expressly show the Purpose of Utilization in advance. However, this provision shall not apply in cases in which the acquisition of personal information is urgently required for the protection of the life, body, or property of an individual.

(3) When a business operator handling personal information has changed the Purpose of Utilization, the business operator shall notify the person of the changed Purpose of Utilization or publicly

announce it.

(4) The provisions of the preceding three paragraphs shall not apply to the following cases:

(i) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the life, body, property, or other rights or interests of the person or a third party

(ii) Cases in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to harm the rights or legitimate interests of the business operator handling personal information

(iii) Cases in which it is necessary to cooperate with a state organ or a local government in executing the affairs prescribed by laws and regulations and in which notifying the person of the Purpose of Utilization or publicly announcing it are likely to impede the execution of the affairs

(iv) Cases in which it is considered that the Purpose of Utilization is clear in consideration of the circumstances of the acquisition

(Maintenance of the Accuracy of Data)

Article 19 A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization.

(Security Control Measures)

Article 20 A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.

(Supervision of Employees)

Article 21 When a business operator handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the security control of the personal data.

(Supervision of Trustees)

Article 22 When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.

(Restriction of Provision to A Third Party)

Article 23 (1) A business operator handling personal information shall not, except in the following cases, provide personal data to a third party without obtaining the prior consent of the person:

(i) Cases in which the provision of personal data is based on laws and regulations

(ii) Cases in which the provision of personal data is necessary for the protection of the life, body, or property of an individual and in which it is difficult to obtain the consent of the person

(iii) Cases in which the provision of personal data is specially necessary for improving public health or promoting the sound growth of children and in which it is difficult to obtain the consent of the person

(iv) Cases in which the provision of personal data is necessary for cooperating with a state organ, a local government, or an individual or a business operator entrusted by one in executing the affairs prescribed by laws and regulations and in which obtaining the consent of the person are likely to impede the execution of the affairs

(2) With respect to personal data intended to be provided to a third party, where a business operator handling personal information agrees to discontinue, at the request of a person, the provision of such personal data as will lead to the identification of the person, and where the business operator, in advance, notifies the person of the matters listed in the following items or put those matters in a readily accessible condition for the person, the business operator may, notwithstanding the provision of the preceding paragraph, provide such personal data to a third party:

(i) The fact that the provision to a third party is the Purpose of Utilization

(ii) The items of the personal data to be provided to a third party

(iii) The means or method of provision to a third party

(iv) The fact that the provision of such personal data as will lead to the identification of the person to a third party will be discontinued at the request of the person

(3) When a business operator handling personal information changes the matter listed in item (ii) or (iii) of the preceding paragraph, the business operator shall, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.

(4) In following the cases, the individual or business operator receiving such personal data shall not be deemed a third party for the purpose of application of the provisions of the preceding three paragraphs:

(i) Cases in which a business operator handling personal information entrust the handling of personal data in whole or in part within the scope necessary for the achievement of the Purpose of Utilization

(ii) Cases in which personal data is provided as a result of the succession of business in a merger

or otherwise

(iii) Cases in which personal data is used jointly between specific individuals or entities and in which this fact, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data is used by them, and the name of the individual or business operator responsible for the management of the personal data is, in advance, notified to the person or put in a readily accessible condition for the person

(5) When a business operator handling personal information changes the purpose for which the personal data is used or the name of the individual or business operator responsible for the management of the personal data as are provided in item (iii) of the preceding paragraph, the business operator shall, in advance, notify the person of the content of the change or put it in a readily accessible condition for the person.

(Public Announcement of Matters Concerning Retained Personal Data, etc.)

Article 24 (1) With respect to the retained personal data, a business operator handling personal information shall put the matters listed in the following items in an accessible condition for the person (such condition includes cases in which a response is made without delay at the request of the person):

(i) The name of the business operator handling personal information

(ii) The Purpose of Utilization of all retained personal data (except in cases falling under any of items (i) to (iii) of paragraph (4) of Article 18)

(iii) Procedures to meet requests made pursuant to the provisions of the next paragraph, paragraph (1) of the next article, paragraph (1) of Article 26, or paragraph (1) or paragraph (2) of Article 27 (including the amount of charges if set pursuant to the provision of paragraph (2) of Article 30)

(iv) In addition to what is listed in the preceding three items, such matters, specified by a Cabinet Order, as being necessary for ensuring the proper handling of retained personal data

(2) When a business operator handling personal information is requested by a person to notify him or her of the Purpose of Utilization of such retained personal data as may lead to the identification of the person concerned, the business operator shall meet the request without delay. However, this provision shall not apply to cases falling under either of the following items:

(i) Cases in which the Purpose of Utilization of such retained personal data as may lead to the identification of the person concerned is clear pursuant to the provision of the preceding paragraph

(ii) Cases falling under any of items (i) to (iii) of paragraph (4) of Article 18

(3) When a business operator handling personal information has decided not to notify the Purpose

of Utilization of such retained personal data as is requested under the preceding paragraph, the business operator shall notify the person of that effect without delay.

(Disclosure)

Article 25 (1) When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person (such disclosure includes notifying the person that the business operator has no such retained personal data as may lead to the identification of the person concerned. The same shall apply hereinafter.), the business operator shall disclose the retained personal data without delay by a method prescribed by a Cabinet Order. However, in falling under any of the following items, the business operator may keep all or part of the retained personal data undisclosed:

(i) Cases in which disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party

(ii) Cases in which disclosure is likely to seriously impede the proper execution of the business of the business operator handling personal information

(iii) Cases in which disclosure violates other laws and regulations

(2) When a business operator handling personal information has decided not to disclose all or part of such retained personal data as is requested pursuant to the provision of the preceding paragraph, the business operator shall notify the person of that effect without delay.

(3) If the provisions of any other laws and regulations require that all or part of such retained personal data as may lead to the identification of a person be disclosed to the person by a method equivalent to the method prescribed in the main part of paragraph (1), the provision of the paragraph shall not apply to such all or part of the retained personal data concerned.

(Correction, etc.)

Article 26 (1) When a business operator handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data is contrary to the fact, the business operator shall, except in cases in which special procedures are prescribed by any other laws and regulations for such correction, addition, or deletion, make a necessary investigation without delay within the scope necessary for the achievement of the Purpose of Utilization and, on the basis of the results, correct, add, or delete the retained personal data.

(2) When a business operator handling personal information has corrected, added, or deleted all or part of the retained personal data as requested or has decided not to make such correction, addition, or deletion, the business operator shall notify the person of that effect (including the

content of the correction, addition, or deletion if performed) without delay.

(Discontinuance of the Utilization, etc.)

Article 27 (1) Where a business operator handling personal information is requested by a person to discontinue using or to erase such retained personal data as may lead to the identification of the person on the ground that the retained personal data is being handled in violation of Article 16 or has been acquired in violation of Article 17, and where it is found that the request has a reason, the business operator shall discontinue using or erase the retained personal data concerned without delay to the extent necessary for redressing the violation. However, this provision shall not apply to cases in which it costs large amount or otherwise difficult to discontinue using or to erase the retained personal data and in which the business operator takes necessary alternative measures to protect the rights and interests of the person.

(2) Where a business operator handling personal information is requested by a person to discontinue providing to a third party such retained personal data as may lead to the identification of the person on the ground that the retained personal data is being provided to a third party in violation of paragraph (1) of Article 23, and where it is found that the request has a reason, the business operator shall discontinue providing the retained personal data to a third party without delay. However, this provision shall not apply to cases in which it costs large amount or otherwise difficult to discontinue providing the retained personal data concerned to a third party and in which the business operator takes necessary alternative measures to protect the rights and interests of the person.

(3) When a business operator handling personal information has discontinued using or has erased all or part of the retained personal data as requested under paragraph (1) or has decided not to discontinue using or not to erase the retained personal data or when a business operator handling personal information has discontinued providing all or part of the retained personal data to a third party as requested under the provision of the preceding paragraph or has decided not to discontinue providing the retained personal data to a third party, the business operator shall notify the person of that effect without delay.

(Explanation of Reasons)

Article 28 When a business operator handling personal information notifies a person requesting the business operator to take certain measures pursuant to the provisions of paragraph (3) of Article 24, paragraph (2) of Article 25, paragraph (2) of Article 26, or paragraph (3) of the preceding article that the business operator will not take all or part of the measures or that the business operator will take different measures, the business operator shall endeavor to explain the

reasons.

(Procedures to Meet Requests for Disclosure and Others)

Article 29 (1) A business operator handling personal information may, as prescribed by a Cabinet Order, determine procedures for receiving requests that may be made pursuant to the provisions of paragraph (2) of Article 24, paragraph (1) of Article 25, paragraph (1) of Article 26 or paragraph (1) or paragraph (2) of Article 27 (hereinafter referred to as "a request for disclosure and others" in this article). In such a case, any person making a request for disclosure and others shall comply with the procedures.

(2) A business operator handling personal information may request a person making a request for disclosure and others to show sufficient items to identify the retained personal data in question. In this case, the business operator shall provide the information contributing to the identification of the retained personal data in question or take any other appropriate measures in consideration of the person's convenience so that the person can easily and accurately make a request for disclosure and others.

(3) A person may, as prescribed by a Cabinet Order, make a request for disclosure and others through a representative.

(4) When a business operator determine the procedures for meeting requests for disclosure and others under the provisions of the preceding three paragraphs, the business operator shall take into consideration that the procedures will not impose excessively heavy burden on the persons making requests for disclosure and others.

(Charges)

Article 30 (1) When a business operator handling personal information is requested to notify the Purpose of Utilization under the provision of paragraph (2) of Article 24 or to make a disclosure under the provision of paragraph (1) of Article 25, the business operator may collect charges for taking the measure.

(2) When a business operator handling personal information collects charges pursuant to the provision of the preceding paragraph, the business operator shall determine the amounts of charges within the scope considered reasonable in consideration of actual costs.

(Processing of Complaints by Entities Handling Personal Information)

Article 31 (1) A business operator handling personal information shall endeavor to appropriately and promptly process complaints about the handling of personal information.

(2) A business operator handling personal information shall endeavor to establish a system

necessary for achieving the purpose set forth in the preceding paragraph.

(Collection of Reports)

Article 32 The competent minister may have a business operator handling personal information make a report on the handle of personal information to the extent necessary for implementation of the provisions of this section.

(Advice)

Article 33 The competent minister may advise a business operator handling personal information on the handle of personal information to the extent necessary for implementation of the provisions of this section.

(Recommendations and Orders)

Article 34 (1) When a business operator handling personal information has violated any of the provisions of Article 16 to Article 18, Article 20 to Article 27, or paragraph (2) of Article 30, the competent Minister may recommend that the business operator handling personal information cease the violation and take other necessary measures to correct the violation when a competent Minister finds it necessary for protecting the rights and interests of individuals.

(2) Where a business operator handling personal information having received a recommendation under the provision of the preceding paragraph does not take the recommended measures without justifiable ground, and when the competent minister finds that the serious infringement on the rights and interests of individuals is imminent, the competent minister may order the business operator handling personal information to take the recommended measures.

(3) Notwithstanding the provisions of the preceding two paragraphs, where a business operator handling personal information has violated any of the provisions of Article 16, Article 17, Articles 20 to 22, or paragraph (1) of Article 23, and when the competent minister finds it necessary to take measures urgently as there is the fact of serious infringement of the rights and interests of individuals, the competent minister may order the business operator handling personal information to cease the violation and take other necessary measures to rectify the violation.

(Restrictions of the Exercise of Authority by the Competent Minister)

Article 35 (1) In collecting a report from, or giving an advice, a recommendation or an order to a business operator handling personal information pursuant to the provisions of the preceding three articles, the competent Minister shall not disturb freedom of expression, academic freedom, freedom of religion, or freedom of political activity.

(2) In light of the purport of the provision of the preceding paragraph, with respect to the act of a business operator handling personal information to provide an individual or business operator mentioned in each item of paragraph (1) of Article 50 (limited to cases in which the personal information is handled for a purpose as respectively provided in each of such items) with personal information, the competent Minister shall not exercise its authority.

(Competent Ministers)

Article 36 (1) The competent ministers under the provisions of this section shall be as specified below. However, for specific handling of personal information by a business operator handling personal information, the Prime Minister may designate a specific minister or the National Public Safety Commission (hereinafter referred to as "minister, etc ") as a competent minister when he or she considers it necessary for smooth implementation of the provisions of this section.

(i) For such handling of personal information by a business operator handling personal information as is related to employment management, Minister of Health, Labor and Welfare (for such handling of personal information as is related to the employment management of mariners, the Minister of Land, Infrastructure, Transport and Tourism) and the minister, etc. concerned with jurisdiction over the business of the business operator handling personal information

(ii) For such handling of personal information by a business operator handling personal information as is not falling under the preceding item, the minister, etc. concerned with jurisdiction over the business of the business operator handling personal information

(2) When the Prime Minister has designated a competent minister under the provision of the proviso to the preceding paragraph, he or she shall publicly notice that effect.

(3) Competent ministers shall maintain close liaison and cooperate with each other in implementing the provisions of this section.

Section 2 Promotion of the Protection of Personal Information by Private Organizations

(Authorization)

Article 37 (1) A juridical person (which includes an association or foundation that is not a juridical person with a specified representative or manager; the same applies in (b) of item (iii) of the next article) that intends to conduct any of the businesses enumerated in the following items for the purpose of ensuring the proper handling of personal information by a business operator handling personal information, may be authorized as such by the competent minister:

(i) The processing under the provision of Article 42 of complaints about the handling of personal information of such business operations handling personal information as are the targets of the business (hereinafter referred to as "target entities")

(ii) The provision of information for target entities about the matters contributing to ensuring the proper handling of personal information

(iii) In addition to what is listed in the preceding two items, any business necessary for ensuring the proper handling of personal information by target entities

(2) A business operator intending to receive authorization set forth in the preceding paragraph shall apply to the competent minister as prescribed by a Cabinet Order.

(3) When having granted authorization under paragraph (1), the competent minister shall publicly notice that effect.

(Clause of Disqualification)

Article 38 A business operator falling under any of the following items may not receive authorization set forth in paragraph (1) of the preceding article:

(i) A business operator having received a sentence pursuant to the provisions of this Act with not exceeding two years after the business operator served out the sentence or was exempted from the execution of the sentence

(ii) A business operator whose authorization was rescinded pursuant to the provision of paragraph (1) of Article 48 with not exceeding two years after the rescission

(iii) A business operator with an officer (including the representative or manager of an association or foundation which is not a juridical person with a specified representative or manager. Hereinafter the same shall apply in this article.) conducting the business who falls under any of the following categories:

(a) An individual sentenced to imprisonment or a heavier punishment, or having received a sentence pursuant to the provision of this Act, with not exceeding two years after the individual served out the sentence or was exempted from the execution of the sentence

(b) In the case of a juridical person whose authorization was rescinded pursuant to the provision of paragraph (1) of Article 48, an individual who was an officer of the juridical person within at least 30 days before the rescission, with not exceeding two years after the rescission

(Authorization Standard)

Article 39 The competent minister shall not grant authorization unless he or she considers that an application for authorization filed under paragraph (1) of Article 37 conforms every requirement

enumerated in the following items:

(i) The applicant shall have established a business execution method necessary for properly and soundly conducting the business mentioned in any of the items of paragraph (1) of Article 37.

(ii) The applicant shall have sufficient knowledge, abilities, and financial base for properly and soundly conducting the business mentioned in any of the items of paragraph (1) of Article 37.

(iii) When the applicant conducts any business other than the businesses mentioned in the items of paragraph (1) of Article 37, by conducting the business, the applicant shall not be likely to impede the fair execution of the businesses mentioned in the same items of the same paragraph.

(Notification of Abolition)

Article 40 (1) When a business operator authorized under paragraph (1) of Article 37 (hereinafter referred to as " authorized personal information protection organization") intends to abolish the business pertaining to the authorization (hereinafter referred to as " authorized business"), it shall notify the competent minister of that effect in advance as prescribed by a Cabinet Order.

(2) When having received a notification under the provision of the preceding paragraph, the competent minister shall publicly notice to that effect.

(Target Entities)

Article 41 (1) Each target business operator of an authorized personal information protection organization shall be a business operator handling personal information that is a member of the authorized personal information protection organization or a business operator handling personal information that has agreed to become a target of the authorized businesses.

(2) Each authorized personal information protection organization shall publicly announce the names of its target entities.

(Handling of Complaints)

Article 42 (1) When an authorized personal information protection organization is requested by a person, etc. to solve a complaint about the handling of personal information by a target business operator, corresponding to the request, the organization shall give the person, etc. necessary advice, investigate the circumstances pertaining to the complaint and request the target business operator to solve the complaint promptly by notifying the target business operator of the content of the complaint.

(2) When an authorized personal information protection organization finds it necessary for settling complaints offered under the preceding paragraph, the organization may request the target

business operator to explain in writing or orally, or request it to submit relevant materials.

(3) When a target business operator has received a request under the provision of the preceding paragraph from an authorized personal information protection organization, the target business operator shall not reject the request without justifiable ground.

(Personal Information Protection Guidelines)

Article 43 (1) In order to ensure the proper handling of personal information by its target entities, each authorized personal information protection organization shall endeavor to draw up and publicly announce guidelines (hereinafter referred to as "personal information protection guidelines") in conformity with the purport of the provisions of this Act, concerning the specification of the Purpose of Utilization, security control measures, procedures for complying with individuals' requests, and other matters.

(2) When an authorized personal information protection organization has publicly announced its personal information protection guidelines pursuant to the provision of the preceding paragraph, the organization shall endeavor to provide guidance, give recommendations, and take other measures necessary in order to have its target entities observe the personal information protection guidelines.

(Prohibition of Utilization Other Than for Intended Purposes)

Article 44 An authorized personal information protection organization shall not utilize any information acquired in the course of conducting its authorized businesses for purposes other than that for the authorized business.

(Restriction on Use of the Name)

Article 45 A business operator that is not an authorized personal information protection organization shall not use the name " authorized personal information protection organization" or any other name that might be mistaken for it.

(Collection of Reports)

Article 46 The competent minister may have an authorized personal information protection organization make a report on the authorized businesses to the extent necessary for implementation of the provisions of this section.

(Orders)

Article 47 The competent minister may order an authorized personal information protection

organization to improve the method of conducting its authorized businesses, to amend its personal information protection guidelines, or to take any other necessary measures to the extent necessary for implementation of the provisions of this section.

(Rescission of Authorization)

Article 48 (1) If an authorized personal information protection organization falls under any of the following items, the competent minister may rescind its authorization:

(i) Cases of falling under item (i) or (iii) of Article 38

(ii) Cases of falling not to conform with any of the items of Article 39

(iii) Cases of violating the provisions of Article 44

(iv) Cases of not complying with orders in the preceding article

(v) Cases of having received the authorization in paragraph (1) of Article 37 by a dishonest means

(2) When having rescinded authorization pursuant to the provision of the preceding paragraph, the competent minister shall publicly notice that effect.

(Competent Ministers)

Article 49 (1) The competent ministers under the provisions of this section shall be as specified below. However, when the Prime Minister considers it necessary for smooth implementation of the provisions of this section, he or she may designate a specific minister, etc. as a competent minister for specific entities that intend to apply for authorization under paragraph (1) of Article 37.

(i) For authorized personal information protection organization (including entities that intend to be authorized under paragraph (1) of Article 37. This applies in the next item.) established under permission or approval, the competent minister shall be the minister, etc. that has granted the permission or approval.

(ii) For authorized personal information protection organization other than those mentioned in the preceding item, the competent minister shall be the minister, etc. having jurisdiction over the business conducted by the target entities of the authorized personal information protection organizations concerned.

(2) When the Prime Minister has designated a competent minister pursuant to the provision of the proviso to the preceding paragraph, he or she shall publicly notice that effect.

Chapter V Miscellaneous Provisions

(Exclusion from Application)

Article 50 (1) With respect to entities handling personal information, being the entities enumerated in each of the items below, if all or part of the purpose of handling personal information is a purpose respectively prescribed in each of the items, the provisions of the preceding chapter shall not be applied.

(i) Broadcasting institutions, newspaper publishers, communication agencies and the other press (including individuals engaged in news report as their business); the purpose for news report

(ii) A business operator who conduct literary work as their business; the purpose for literary work

(iii) Colleges, universities, other institutions or organizations engaged in academic studies, or entities belonging to them: The purpose for academic studies

(iv) Religious organizations: The purpose for religious activities (including activities incidental thereto)

(v) Political organizations: The purpose for political activities (including activities incidental thereto)

(2) "News report" as mentioned in item (i) of the preceding paragraph shall mean informing many and unspecified individuals or entities of objective facts as the facts (including to state opinions or views based on such facts).

(3) Entities handling personal information enumerated in the items of paragraph (1) shall endeavor to take by themselves the necessary and appropriate measures for controlling the security of personal data, and the necessary measures for the processing of complaints about the handling of personal information and the other necessary measures for ensuring the proper handling of personal information, and shall also endeavor to publicly announce the content of those measures concerned.

(Affairs Handled by Local Governments)

Article 51 The affairs belonging to the authority of a competent minister provided by this Act may be handled by the heads of local governments or by other executive agencies as prescribed by a Cabinet Order.

(Delegation of Authority or Affairs)

Article 52 The matters belonging to the authority or the affairs of a competent minister may be delegated to his or her staffs as prescribed by a Cabinet Order.

(Public Announcement of the Status of Enforcement)

Article 53 (1) The Prime Minister may collect reports on the status of enforcement of this Act from the heads of relevant administrative organs (the organs established in the Cabinet under the

provisions of laws (except the Cabinet Office), organs under the supervision of the Cabinet, the Cabinet Office, the Imperial Household Agency, the institutions prescribed in paragraphs (1) and (2) of Article 49 of the Act for Establishment of the Cabinet Office (Act No. 89 of 1999), and the institutions prescribed in paragraph (2) of Article 3 of the National Government Organization Law (Act No. 120 of 1948); this applies in the next article).

(2) Each year the Prime Minister shall compile the reports set forth in the preceding paragraph and publicly announce their outline.

(Liaison and Cooperation)

Article 54 The Prime Minister and the heads of the administrative organs involved in the enforcement of this Act shall maintain close liaison and cooperate with each other.

(Delegation to Cabinet Orders)

Article 55 The matters necessary for implementation of this Act, in addition to those prescribed in this Act, shall be prescribed by Cabinet Orders.

Chapter VI Penal Provisions

Article 56 A business operator who violates orders issued under paragraph (2) or (3) of Article 34 shall be sentenced to imprisonment with work of not more than six months or to a fine of not more than 300,000 yen.

Article 57 A business operator who does not make a report required by Article 32 or 46 or who has made a false report shall be sentenced to a fine of not more than 300,000 yen.

Article 58 (1) If any representative of a juridical person (which includes an association or foundation which is not a juridical person with a specified representative or manager; hereinafter the same shall apply in this paragraph), or any agent, employee or other workers of a juridical person or of an individual commits any of the violations prescribed in the preceding two articles concerning the business of the juridical person or individual, then not only shall the performer be punished but also the juridical person or individual shall be sentenced to the fine prescribed in the corresponding article.

(2) When the provision of the preceding paragraph applies to an association or foundation which is not a juridical person, its representative or manager shall represent the associaion or foundation which is not a juridical person in its procedural action, and the provisions of the acts concerning

criminal suits in which a juridical person is the accused or suspect shall be apply mutatis mutandis.

Article 59 A business operator who falls under any of the following items shall be sentenced to a civil fine of not more than 100,000 yen:

(i) A business operator who does not make a notification required by paragraph (1) of Article 40 or who has made a false notification

(ii) A business operator who violates the provision of Article 45

Supplementary Provisions [Extract]

(Effective Date)

Article 1 This Act shall come into force as from the day of promulgation. However, the provisions of Chapter IV to Chapter VI and Article 2 to Article 6 of the supplementary Provisions shall become effective as of the date specified by a Cabinet Order within a period not exceeding two years from the day of promulgation.

(Transitional Measures Concerning a Consent of a Person)

Article 2 Where a person has given consent to the handling of his or her personal information prior to enforcement of this Act, and where the consent is equivalent to the consent that allows the personal information to be handled for a purpose other than the Purpose of Utilization specified under paragraph (1) of Article 15, then it shall be deemed that there is such consent as is prescribed in paragraph (1) or (2) of Article 16.

Article 3 Where a person has given consent to the handling of his or her personal information prior to enforcement of this Act, and where the consent is equivalent to the consent that allows the personal data to be provided to a third party under paragraph (1) of Article 23, then it shall be deemed that there is such consent as is prescribed in the same paragraph.

(Transitional Measures Concerning Notices)

Article 4 If an individual has been notified, prior to enforcement of this Act, of the matters that shall be notified to the individual or be put in a readily accessible condition for the individual under paragraph (2) of Article 23, then it shall be deemed that the notice concerned has been given under the provision of the same paragraph.

Article 5 If an individual has been notified, prior to enforcement of this Act, of the matters that shall be notified to the individual or be put in a readily accessible condition for the individual under item (iii) of paragraph (4) of Article 23, then it shall be deemed that the notice concerned has been given under the provision of the same paragraph.

(Transitional Measures Concerning the Restriction on Use of the Name)

Article 6 The provisions of Article 45 shall not apply, for six months after the provision of the same article is enforced, to any business operator actually using the name " authorized personal information protection organization" or a name that might be mistaken for it at the time when this Act is enforced.

Amended Act on the Protection of Personal Information

(Tentative Translation)

This is an English translation of the amended Act on the Protection of Personal Information, to be put into full effect on May 30, 2017.

NOTICE

*This translation has neither had its texts checked by a native English speaker nor legal language editor, and thus may be subject to change.

*The Japanese original legal texts only shall remain in force, while their English translation is presented for ease of non-Japanese speakers' understanding and reference.

Table of Contents

Chapter I General Provisions

(Purpose)

Article 1

This Act aims to protect an individual's rights and interests while considering the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched

quality of life for the people of Japan; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

(Definitions)

Article 2 (1)

The term "personal information" as used in this Act means information about a living individual, and falls under one of the following items:

(i) information that can be used to identify that specific individual due to its inclusion of a name, date of birth, or other description contained (any and all matters (that excludes individual identification codes) written, recorded or otherwise expressed using voice, movement or other methods in documents, drawings or electromagnetic records (meaning records made by electromagnetic format (electronic, magnetic or any other format that cannot be recognized through the human senses; the same applies in next paragraph, item (ii)); the same applies in Article 18, paragraph (2); the same applies hereinafter) in such information (this includes any information that can be cross-checked against other information and thereby used to identify that specific individual).

(ii) Information that contains individual identification codes

(2) The term “personal identification code” as used in this Act means any character, letter, number, symbol or other marking that falls under one of the following items specified by Cabinet Order.

(i) Any character, letter, number, symbol or other marking converted from a distinguishing part of a specific individual's body so that it may be used with a computer, and any such information that can identify the specific individual.

(ii) Any character, letter, number, symbol or other marking that is allocated to an individual in regards to the use of services provided or the purchase of goods sold, or that is entered into cards or other documents issued to an individual or recorded by electromagnetic format, and any such information that can identify the using individual, the purchasing individual, or the individual being issued through the allocation of differing character, letter, number, or symbol, or writing or recording of such information so as to differentiate among said using individual, purchasing individual, or individual being issued.

(3) The term “sensitive personal information” used in this Act means a personal information that contains descriptions that have been specified by Cabinet Order to require special consideration in

handling so as to avoid any unfair discrimination, prejudice or other disadvantage to an individual based on person's race, creed, social status, medical history, criminal records or the fact that a person has incurred damages through an offense, etc.

(4) The term “personal information database etc.” used in this Act means a set of information which includes personal information as set forth below (this excludes sets of information specified by Cabinet Order to have little possibility of harming the rights and interests of an individual considering the manner such personal information is used).

(i) a set of information structurally organized to enable a computer to be used to retrieve certain personal information from it; or,

(ii) in addition to what is listed in the preceding item, a set of information specified by Cabinet Order as being structurally organized to be easily retrieved certain personal information.

(5) The term "business operator handling personal information" as used in this Act means a business operator that has a personal information database etc. for business use; however, the following entities are excluded;

(i) national government organs;

(ii) local governments;

(iii) incorporated administrative agencies and other such entities (meaning independent administrative agencies and other such entities as provided in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); the same applies hereinafter);

(iv) local incorporated administrative agencies (meaning local incorporated administrative agencies as provided in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); the same applies hereinafter);

(6) The term “personal data” as used in this Act means personal information compiled in a personal information database etc.

(7) The term “retained personal data” as used in this Act means personal data that a business operator handling personal information has the authority to disclose; to correct, add or delete content from; to discontinue use of; to erase; or to discontinue provision to a third party, other than what Cabinet Order provides for as data which is likely to harm the public interest or other interests, if its presence or absence is known and other than data that will be deleted within the period of less than one year that Cabinet Order specifies.

(8) The term “person” as used in this Act in relation to personal information means the specific individual that the personal information can be used to identify.

(9) The term “the de-identified information” as used in this Act, according to the categories of personal information set forth below, means information regarding an individual that is gained from

processing personal information so as to prevent the identification of a specific individual taking measures prescribed by the items below, and that do not allow restoring of said personal information.

(i) The deletion of a part of descriptions that contains personal information falling under paragraph (1), item (i) above (this includes replacing said part of descriptions with other descriptions through methods that do not allow for the restoring of said part of descriptions).

(ii) The deletion of all personal identification codes that contain personal information falling under paragraph (1), item (i) above (this includes replacing said personal identification code with other descriptions through methods that do not allow for the restoring of said part of personal identification codes).

(10) The term "business operator handling de-identified information" as used in this Act means a business operator using for its business a set of information which includes deidentified information, which is structurally organized to enable a computer to be used to retrieve certain de-identified information, and which is other set of de-identified information that Cabinet Order provides for as being structurally organized to enable certain deidentified information to be easily retrieved from it (this is referred to as "de-identified information database etc." in Article 36, paragraph (1)). However, the business operators set forth in one of the items of paragraph (5) are excluded.

(Basic Principle)

Article 3

The proper handling of personal information must be pursued in view of the fact that personal information should be handled cautiously based on the philosophy of respecting the autonomy of the individual.

Chapter II Responsibilities, etc. of the National and Local Governments

(Responsibilities of the National Government)

Article 4

The National Government is responsible for comprehensively formulating and implementing the necessary measures to ensure the proper handling of personal information in conformity with the purport of this Act.

(Responsibilities of Local Governments)

Article 5

Local governments are responsible for formulating and implementing the necessary measures to ensure the proper handling of personal information based on the characteristics of the area, in conformity with the purport of this Act.

(Legislative Measures etc.)

Article 6

The Government must take the necessary legislative and other measures to ensure that special measures will be taken for the protection of personal information, especially that personal information which requires the strict implementation of proper handling so that the rights and interests of individuals can be further protected in view of the nature and the method of utilization of the personal information. Concurrently, the Government must also coordinate with the governments of other countries through cooperation with international organs and other international frameworks to take the measures necessary to building a system for personal information that is internationally integrated.

Chapter III Measures for the Protection of Personal Information, etc.

Section 1 Basic Policy on the Protection of Personal Information

Article 7

(1) The Government must establish a basic policy (hereinafter referred to as a "Basic Policy") so as to further comprehensive and integrated measures to protect personal information.

(2) The Basic Policy must provide for the following matters:

(i) the basic approach of action for the promotion of measures to protect personal information.

(ii) the matters of measures to protect personal information that are to be taken by the national government;

(iii) the basic matters of the measures to protect personal information that are to be taken by local governments;

(iv) the basic matters of the measures to protect personal information that are to be taken by incorporated administrative agencies and other such entities;

(v) the basic matters of the measures to protect personal information that are to be taken by local incorporated administrative agencies;

(vi) the basic matters of the measures to protect personal information that are to be taken by business operators handling personal information, business operators handling deidentified information and accredited personal information protection organizations as provided in Article 50, paragraph (1);

(vii) matters about the smooth processing of complaints about the handling of personal information;

(viii) other material matters for the promotion of measures to protect personal information. (3) The Prime Minister must prepare a draft Basic Policy created by the Personal Information Protection Commission, and ask for Cabinet approval. (4) Following the Cabinet approval under the preceding paragraph, the Prime Minister must disclose the Basic Policy to the public without delay. (5) The provisions of the preceding two paragraphs apply mutatis mutandis to amendments to the Basic

Policy.

Section 2 National Measures

(Support for Local Governments, etc.)

Article 8

The national government must take necessary measures such as providing information and formulating guidelines to ensure the business operators and others properly and effectively implement the measures that they are required to take, in order to support action that the people, business operators and others take to ensure the proper handling of personal information.

(Complaint Processing Measures)

Article 9

The national government must take the necessary measures to ensure the appropriate, prompt processing of complaints arising between business operators and persons with regard to the handling of personal information.

(Measures to Ensure Proper Handling of Personal Information)

Article 10

The national government must take the necessary measures to ensure the proper handling of personal information by business operators handling personal information as provided in the next Chapter, by effecting an appropriate division of roles between the national and local governments.

Section 3 Local Government Measures

(Protection of Personal Information Held by Local Governments, etc.)

Article 11

(1) A local government must endeavor to take the necessary measures to ensure the proper handling of the personal information it holds, in consideration of such factors as the nature of the personal information and the purpose, etc. for which it holds that personal information.

(2) A local government must endeavor to take the necessary measures to ensure the proper handling of personal information that is held by the local incorporated administrative agencies it has established, in accordance with the nature of the agency and the content of its operations.

(Support for Area Business Operators)

Article 12

A local government must endeavor to take the necessary measures to support business operators and residents within its territory so as to ensure the proper handling of personal information.

(Mediation, etc. for Complaint Processing)

Article 13

A local government must endeavor to provide mediation for complaint processing and take other necessary measures to ensure that any complaint arising between an enterprise and a person with

regard to the handling of personal information is handled appropriately and promptly.

Section 4 Cooperation between the National and Local Governments

Article 14

National and local governments must cooperate in taking measures to protect personal information.

Chapter IV Obligations, etc. of Business Operators Handling Personal Information

Section 1 Obligations of Business Operators Handling Personal Information

(Specifying the Purpose of Use)

Article 15

(1) In handling personal information, the business operator handling personal information must specify as precise as possible about the purpose for which it uses that information (hereinafter referred to as "Purpose of Use") .

(2) A business operator handling personal information must not change the Purpose of Use beyond a scope that makes it reasonable to consider the Purpose of Use after the change to be related to what it was before the change.

(Restriction due to Purpose of Use)

Article 16

(1) A business operator handling personal information must not handle personal information beyond the scope necessary for achieving of the Purpose of Use specified pursuant to the provisions of the preceding Article without in advance obtaining the person's consent to do so.

(2) If, due to a merger or other such circumstances, a business operator handling personal information acquires personal information when succeeding to the business of another business operator handling personal information, it must not handle that personal information beyond the scope necessary for achieving pre-succession Purpose of Use for that personal information without in advance obtaining the person's consent to do so.

(3) The provisions of the preceding two paragraphs do not apply in the following cases:

(i) the business operator handles the personal information outside its Purpose of Use based on law and regulations;

(ii) it is necessary for the business operator to handle the personal information outside its purpose of use in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person;

(iii) there is a special need for the business operator to handle the personal information outside its purpose of use in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to handle the personal information outside its purpose

of use in order to cooperate with a national government organ, local government, or person or business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(Proper Acquisition)

Article 17

(1) A business operator handling personal information must not acquire personal information through deception or other wrongful means.

(2) A business operator handling personal information must not acquire sensitive personal information without in advance obtaining the person's consent to do so, except in the following cases;

(i) the business operator obtain the sensitive personal information based on law and regulations;

(ii) it is necessary for the business operator to obtain the sensitive personal information in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person;

(iii) there is a special need for the business operator to obtain the sensitive personal information in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to obtain the sensitive personal information in order to cooperate with a national government organ, local government, or person or business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(v) the sensitive personal information has been made public by the person, national government organ, local government, a business operator set forth in one of the items of Article 76, paragraph (1), and any other person or business operator prescribed by rules of the Personal Information Protection Commission;

(vi) Other cases that are prescribed by Cabinet Order as corresponding to any of the preceding cases.

(Notice, etc. of the Purpose of Use at the Time of Acquisition)

Article 18

(1) Unless the Purpose of Use has already been disclosed to the public, a business operator handling personal information must promptly notify the person of that Purpose of Use or disclose this to the public once it has acquired personal information.

(2) Notwithstanding the provision of the preceding paragraph, a business operator handling personal information must explicitly specify the purpose of use to the person in advance if acquiring, as a

result of concluding a contract with the person, personal information about the person which appears in a written contract or other document (this includes electromagnetic records; hereinafter the same applies in this paragraph); or if acquiring, directly from the person, personal information about that person which appears in a document; provided, however, that this does not apply if there is an urgent necessity to dispense with this requirement in order to protect the life, body or property of an individual.

(3) If a business operator handling personal information changes the Purpose of Use, it must notify the person of the altered Purpose of Use or disclose this to the public.

(4) The provisions of the preceding three paragraphs do not apply in the following cases:

(i) notifying the person of the Purpose of Use or disclosing this to the public is likely to harm the life, body, property, or other rights or interests of the person or a third party;

(ii) notifying the person of the Purpose of Use or disclosing this to the public is likely to harm the rights or legitimate interests of the business operator handling personal information;

(iii) it is necessary to cooperate with a national government organ or a local government in performing the affairs prescribed by laws and regulations, and notifying the person of the Purpose of Use or disclosing this to the public is likely to interfere with the performance of those affairs;

(iv) the Purpose of Use is considered to be clear, in light of the circumstances in which the personal information is acquired.

(Maintenance the Accuracy of Data)

Article 19

A business operator handling personal information must endeavor to keep the content of personal data accurate and up to date, within the scope necessary for achieving the Purpose of Use, and delete such personal data without delay when its use is no longer required.

(Security Measures)

Article 20

A business operator handling personal information must take the necessary and appropriate measures to ensure the secure management of personal information, such measures to prevent leakage, loss or damage to the personal data it handles.

(Supervision of Employees)

Article 21

In having an employee handle personal data, a business operator handling personal information must exercise the necessary and appropriate supervision over that employee to ensure the secure management of the personal data.

(Supervision of Entrusted persons)

Article 22

If a business operator handling personal information entrusts another business operator with all or part of the handling of personal data, it must exercise the necessary and appropriate supervision over the business operator it entrusts, so as to ensure the secure management of the personal data.

(Restriction of Provision to a Third Party)

Article 23

(1) A business operator handling personal information must not provide a third party with personal data without in advance obtaining the person's consent to do so, except in the following cases:

(i) the business operator provides the third party with personal data based on laws and regulations;

(ii) it is necessary for the business operator to provide the third party with the personal data in order to protect the life, body, or property of an individual, and it is difficult to obtain the consent of the person.

(iii) there is a special need for the business operator to provide the third party with the personal data in order to improve public health or promote healthy child development, and it is difficult to obtain the consent of the person;

(iv) it is necessary for the business operator to provide the third party with the personal data in order to cooperate with a national government organ, local government, or an individual or a business operator entrusted thereby with performing the affairs prescribed by laws and regulations, and obtaining the consent of the person is likely to interfere with the performance of those affairs.

(2) Notwithstanding the provisions of the preceding paragraph, if a business operator handling personal information agrees, at the request of a person, to stop providing a third party with any personal data it provides to third parties which can be used to identify the person, but then as prescribed by rules of the Personal Information Protection Commission, notifies the person of the following information in advance or makes that information readily accessible to the person in advance, and notifies the Personal Information Protection Commission in advance, the business operator may provide that personal data to a third party:

(i) the fact that providing the data to a third party constitutes the Purpose of Use;

(ii) the items of the personal data it will provide to the third party;

(iii) the means in which it will provide the data to a third party;

(iv) the fact that it will stop providing personal data that can be used to identify the person to a third party at the request of the person;

(v) the means to receive the request of the person.

(3) Before changing a particular set forth in item (ii), (iii) or (v) of the preceding paragraph, the business operator handling personal information must in advance, as prescribed by rules of the Personal Information Protection Commission, notify the person of the matters of the change or

make those details readily accessible to the person, and must notify the Personal Information Protection Commission.

(4) When the Personal Information Protection Commission receive the notification under paragraph (2), it must disclose the items of the notification to the public, as prescribed by rules of the Personal Information Protection Commission. The same applies for notifications made under the preceding paragraph.

(5) In the following cases, the individual or business operator being provided with the personal data must not be deemed to be a third party as regards the application of the provisions of each preceding paragraph:

(i) if the business operator handling personal information entrusts with all or part of the handling of personal data within the scope necessary for achieving the Purpose of Use;

(ii) if the personal data is provided when a business operator succeeds to the business of the business operator due to a merger or other such circumstances;

(iii) if personal data which is used jointly with a specific individual or business operator is provided to the individual or business operator, and the individual or business operator notify the person of this in advance as well as notify the person of the items of the personal data of which the specific individual or business operator have joint use, the extent of the joint users, the user's purposes of use, and the name of the individual or business operator responsible for managing the personal data, or the individual or business operator make the foregoing information readily accessible to the person in advance.

(6) If a user's purpose of use or the name of the individual or business operator responsible for managing the personal data provided for in item (iii) of the preceding paragraph changes, the business operator handling personal information must notify the person of the content of the change in advance or make the content readily accessible to the person in advance.

(Restrictions on Provision to a Third Parties in Other Countries)

Article 24

A business operator handling personal information must, when providing personal data to a third party (this excludes individuals or business operators that put into place a system compliant with the standards prescribed by rules of the Personal Information Protection Commission as is necessary to continuously take of measures corresponding with measures that business operators handling personal information ought to carry out pursuant to the provisions of this Section with regard to handling of personal data; the same applies in this Article hereinafter.) in a foreign country (any country or territory outside of the region of Japan; the same applies hereinafter) (excluding countries prescribed by rules of the Personal Information Protection Commission to be foreign countries possessing personal information protection systems recognized to be at the same level

as Japan's in terms of protecting the rights and interests of individuals; the same applies hereinafter in this Article), obtain the prior consent of the person for the provision of such personal data to a third party in a foreign country, except in cases set forth in each item of paragraph (1) of the preceding Article. The provisions of that the preceding Article do not apply in this case.

(Creating Records, etc. of Provisions to a Third Party)

Article 25

(1) A business operator handling personal information must, when providing personal data to a third party (this excludes business operators provided for in each item of Article 2, paragraph (5); the same applies hereinafter in this Article and the next Article), make a record of the matters as prescribed by rules of the Personal Information Protection Commission, regarding the date such personal data was provided, the name of the third party, as well as other matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision falling under any of the items of Article 23, paragraph (1) or paragraph (5) (any of the items of Article 23, paragraph (1) for the provision of personal data under the preceding Article).

(2) A business operator handling personal information must store records set forth in the preceding paragraph, from the day when the said records are created for a period of time prescribed by rules of the Personal Information Protection Commission.

(Confirmation Upon Receiving, etc.)

Article 26

(1) A business operator handling personal information must, upon being provided personal data from a third party, confirm the following matters prescribed by rules of the Personal Information Protection Commission. However, this provision does not apply to cases of such personal data provision fall under any of the items of Article 23, paragraph (1) or paragraph (5).

(i) The name and address of the third party, and the name of the representative (the representative or the manager for an association or foundation that are not juridical person) for juridical person;

(ii) The details of the acquisition of the personal data by the third party.

(2) While the business operator handling personal information carries out the confirmation under the preceding paragraph, the third party of the preceding paragraph must not falsely present to the business operator handling personal information the matters related to the confirmation.

(3) When the business operator handling personal information carries out the confirmation under the paragraph (1), the business operator must, prescribed by rules of the Personal Information Protection Commission, make records of the date on which such personal data was provided, matters related to the confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

(4) A business operator handling personal information must store such records beginning with the day on which the said records are created and for a period of time prescribes by rules of the Personal Information Protection Commission.

(Disclosure, etc. of Matters about the Retained Personal Data)

Article 27

(1) A business operator handling personal information must make the following matters about the retained personal data accessible to persons (making that matters accessible includes providing answers without delay as requested by persons):

(i) the name of the business operator handling personal information;

(ii) the Purpose of Use of all retained personal data (unless this falls under Article 18, paragraph (4). items (i) through (iii));

(iii) the procedures for dealing with requests under the provisions of the following paragraph, paragraph (1) of the next Article; Article 29, paragraph (1), or Article 30, paragraph (1) or paragraph (3) (including the amount of the fee, if one is set pursuant to the provision of Article 33, paragraph (2));

(iv) information other than as set forth in the preceding three items which is specified by Cabinet Order as needing to be made accessible in order to ensure the proper handling of retained personal data.

(2) If a business operator handling personal information is requested by a person to notify the person of the Purpose of Use of the retained personal data that can be used to identify the person, the business operator must notify the person without delay; provided, however, that this does not apply in a case falling under one of the following items:

(i) the Purpose of Use of the retained personal data that can be used to identify the person has been made clear pursuant to the provisions of the preceding paragraph;

(ii) a case falling under Article 18, paragraph (4), item (i) through (iii).

(3) If a business operator handling personal information decides not to notify the person of the Purpose of Use of the retained personal data as requested pursuant to the preceding paragraph, the business operator must notify the person of this without delay.

(Disclosure)

Article 28

(1) The person may request the business operator handling personal information to disclose the retained personal data that can be used to identify the person.

(2) When the business operator handling personal information is requested under the provision of the preceding paragraph, the business operator must disclose the retained personal data without delay using the means that Cabinet Order provides for. However, in case falling under one of the

following items, the business operator may choose not to disclose all or part of the retained personal data:

(i) if disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party;

(ii) if disclosure is likely to seriously interfere with the proper implementation of the business of the business operator handling personal information;

(iii) if disclosure would violate any other law or regulation.

(3) If a business operator handling personal information decides not to disclose all or part of the retained personal data as requested pursuant to the provision of the preceding paragraph (1), or there is no retained personal data, the business operator must notify the person of this without delay.

(4) If, pursuant to the provisions of any other law and regulation, all or part of the retained personal data that can be used to identify a person is to be disclosed to the person by a means equivalent to what is prescribed in the main clause of paragraph (2), the provisions of paragraph (1) and (2) do not apply to either the whole or the relevant part of the retained personal data.

(Corrections etc.)

Article 29

(1) The person may request the business operator handling personal information to correct, add, or delete (hereinafter referred to as "corrections etc." hereinafter in this Article) the content of the retained personal data that can be used to identify the person, when the content of the retained personal data is not factual.

(2) If a business operator handling personal information is requested under the provision of the preceding paragraph, unless another law or regulation specifies special procedures for such corrections, etc. to the data, the business operator must undertake the necessary investigations without delay within the scope that is necessary for achieving the Purpose of Use, and, on the basis of the results, correct the retained data.

(3) Once a business operator handling personal information either corrects all or part of the retained personal data that it has been requested to correct under the provision of paragraph (1), or decides not to make such a correction etc., the business operator must notify the person of this (and of the content of the corrections etc. if made) without delay.

(Discontinuance etc. of using personal data.)

Article 30

(1) The person may request the business operator handling personal information to discontinue using or delete (hereinafter referred to as "Discontinuance, etc." in this Article) the retained personal data that can be used to identify the person, when the personal data is handled in

violation of the provisions of Article 16 or was acquired in violation of the provisions of Article 17.
(2) If a business operator handling personal information receives the request under the provision of the preceding paragraph, and there are found to be grounds for that request, the business operator must discontinue of the relevant retained personal data without delay to the extent necessary to redress the violation; however, that this does not apply if the discontinuance, etc. of the relevant retained personal data would require a costly expenditure or prove otherwise difficult, and the business operator takes the necessary alternative measures to protect the rights and interests of the person.
(3) The person may request the business operator handling personal information to discontinue providing the relevant retained personal data to a third party when the retained personal data that can be used to identify the person is being provided to the third party in violation of the provisions of Article 23, paragraph (1) or Article 24.
(4) If a business operator handling personal information receives a request under the provision of the preceding paragraph and there are found to be grounds for that request, the business operator must discontinue providing the relevant retained personal data to a third party without delay; however, that this does not apply if to stop providing the third party with the relevant retained personal data would require a costly expenditure or prove otherwise difficult, and the business operator takes the necessary alternative measures to protect the rights and interests of the person.
(5) Once a business operator handling personal information either discontinues all or part of the retained personal data that it has been requested to discontinue using pursuant to the provision of paragraph (1), or decides not to discontinue the use of it, or once a business operator handling personal information either discontinues providing all or part of the retained personal data to a third party that it has been requested under the provision of the preceding paragraph (3) or decides not to discontinue providing the retained personal data to a third party, the business operator must notify the person of this without delay.

(Explanation of Reasons)

Article 31

If, pursuant to the provisions of Article 27, paragraph (3); Article 28, paragraph (3); Article 29, paragraph (3), paragraph (3), item (v) of the preceding Article, a business operator handling personal information notifies a person that has requested it to take measures that it will not take all or part of the requested measures or that it will take different measures, the business operator must endeavor to explain its reasons for this to the person.

(Procedures for Dealing with Requests for Disclosure and Other Handling)

Article 32

(1) A business operator handling personal information may establish, as prescribed by Cabinet

Order, how it will accept demands under the provision of Article 27, paragraph (2), or requests that may be made under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, this Article, paragraphs (1) or (3) (hereinafter referred to as request for disclosure etc." and Article 53, paragraph (1)). In this such case, any person making a request for disclosure etc. must comply with the procedures.

(2) A business operator handling personal information may request a person requesting disclosure or other handling to present sufficient matters to identify the retained personal data that would be subject to the disclosure or other handling. In such a case, the business operator handling personal information must provide information to help the person identify the relevant retained personal data or take other appropriate measures in consideration of the person's convenience, so as to allow the person to easily and accurately request disclosure or other handling.

(3) A person may request disclosure or other handling thorough a representative, as prescribed by Cabinet Order.

(4) In establishing procedures for dealing with requests for disclosure and other handling pursuant to the preceding three paragraphs, a business operator handling personal information must take care to ensure that the procedures do not impose an excessive burden on persons.

(Fees)

Article 33

(1) When a business operator handling personal information is requested to notify a person of the Purpose of Use under the provision of Article 27, paragraph (2), or receives a request to make disclosure under the provision of Article 28, paragraph (1), it may collect a fee for taking the relevant measures.

(2) If a business operator handling personal information collects a fee pursuant to the provisions of the preceding paragraph, it must fix the amount of that fee within a scope that can be considered reasonable in consideration of actual costs.

(Claims in Advance)

Article 34

(1) Should a person attempt to file a lawsuit regarding the request under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, paragraphs (1) or (3), such a lawsuit may not be filed unless the request is made in advance to the business operator, which the lawsuit is to be filed against, and two weeks have passed since the arrival date of the request. However, this provision does not apply when the business operator which the lawsuit is to be filed against has rejected that request.

(2) The request of the preceding paragraph is deemed to have arrived at the time that such a request should normally arrive.

(3) The provisions of the preceding two paragraphs applies mutatis mutandis regarding filings for provisional injunctions regarding the request under the provisions of Article 28, paragraph (1), Article 29, paragraph (1), Article 30, paragraphs (1) or (3).

(Processing of Complaints by Business Operators Handling Personal Information)

Article 35

(1) A business operator handling personal information must endeavor to process complaints about the handling of personal information appropriately and promptly.

(2) A business operator handling personal information must endeavor to establish the necessary systems for achieving the purpose referred to in the preceding paragraph.

Section 2 Duties of Business Operators Handling De-identified Information

(Creation of De-identified Information)

Article 36

(1) When a business operator handling personal information creates de-identified information (this is limited to information comprising the de-identified information database etc.; hereinafter the same applies), the business operator processes such personal information in accordance with the requirement of the standard prescribed by the rules of the Personal Information Protection Commission so that any person is unable to identify a specific individual and restore the personal information used in the creation of the de-identified information.

(2) When a business operator handling personal information creates de-identified information, the business operator must take measures to ensure the secure management of such information in accordance with standards prescribed by rules of the Personal Information Protection Commission in such a way that prevents the leakage of any description deleted from the personal information used in the creation of the de-identified information, as well as the leakage of any personal identification code and information regarding the processing method carried out pursuant to the preceding paragraph.

(3) When a business operator handling personal information creates de-identified information, the business operator must, as prescribed by rules of the Personal Information Protection Commission, disclose the items of the information regarding the individual included within such de-identified information to the public.

(4) When a business operator handling personal information creates de-identified information and provides a third party with such de-identified information, the business operator must disclose in advance, the items of the information regarding the individual included within such de-identified information provided to the third party and the method such information will be provided to the public, as prescribed by rules of the Personal Information Protection Commission, and must explicitly specify to the third party that the information provided is de-identified information.

(5) When a business operator handling personal information creates de-identified information and handles the de-identified information itself, the business operator must not cross reference the de-identified information against other information to identify the person related to the personal information used to create the de-identified information.

(6) When a business operator handling personal information creates de-identified information, the business operator must, itself, endeavor to take the necessary and appropriate measures for securely managing of such de-identified information, to carry out processing of complaints about the creation and other handling of such de-identified information, and to take other necessary measures for ensuring the proper handling of such de-identified information, and must also endeavor to disclose the content of those measures to the public.

(Provision of De-Identified Information)

Article 37

When a business operator handling de-identified information provides deidentified information (this excludes de-identified information created by itself; hereinafter the same applies to this Section) to a third party, the business operator must, disclose in advance the items of the information regarding the individual included within such deidentified information provided to the third party and the method such information was provided to the public, as prescribed by rules of the Personal Information Protection Commission, and must explicitly specify to the third party that the information provided is de-identified information.

(Prohibition of Actions Leading to Identification)

Article 38

In handling de-identified information, a business operator handling de-identified information must not acquire descriptions deleted from the personal information, personal identification codes, nor information related to the processing method carried out pursuant to the provisions of Article 36, paragraph (1), nor reference the de-identified information against other information for the purpose of identifying the person related to the personal information used in the creation of the de-identified information.

(Security Measures)

Article 39

A business operator handling de-identified information must, itself, endeavor to take the necessary and appropriate measures for securely managing de-identified information, to carry out processing of complaints about the handling of such de-identified information, and to take other necessary measures for ensuring the proper handling of such de-identified information, and must also endeavor to disclose the content of those measures to the public.

Section 3 Supervision

(Reports and On-Site Inspections)

Article 40

(1) The Personal Information Protection Commission may request to submit any necessary reports or documentation regarding the handling of personal information or de-identified information (hereinafter referred to as "personal information etc.") from business operators handling personal information or business operators handling de-identified information (hereinafter referred to as "business operators handling personal information etc."), and the Commission may dispatch its officers to enter the offices and other necessary locations of the business operator handling personal information etc., or inquire about the handling of personal information etc., or inspect books, document and other items to the extent that is necessary for implementing the provisions of preceding two Sections and this Section.

(2) Officers carrying out on-site inspections pursuant to the provision of the preceding paragraph must carry identification demonstrating their credentials, and, present this identification if requested to do so by a relevant person.

(3) The authority of the on-site inspection under the paragraph (1) must not be construed with the authority for a criminal investigation.

(Guidance and Advice)

Article 41

The Personal Information Protection Commission may guide or advise a business operator handling personal information etc. on the handling of personal information etc. to the extent that this is necessary for implementing the provisions of preceding two Sections.

(Recommendations and Orders)

Article 42

(1) If a business operator handling personal information violates one of the provisions of Articles 16 through 18, Articles 20 through 22, Article 23 (excluding paragraph (4)), Article 24, Article 25, Article 26 (excluding paragraph (2)), Article 27, Article 28 (excluding paragraph (1)), Article 29, paragraphs (2) or (3), Article 30, paragraphs(2), (4) or (5), Article 33, paragraph (2), or Article 36 (excluding paragraph (6)), or if a business operator handling de-identified information violates one of the provisions of Articles 37 or 38, and the Commission finds it necessary to do so in order to protect the rights and interests of an individual, the Commission may recommend a business operators handling personal information etc. to stop committing violation and to take the necessary measures to rectify the violation.

(2) If a business operator handling personal information etc. which receives a recommendation under the provisions of the preceding paragraph does not take the measures as recommended, without a legitimate reason for failing to do so, and the Personal Information Protection

Commission finds that serious harm to the rights and interests of individuals is imminent, the Commission may order the business operator handling personal information etc. to take the measures as recommended.

(3) Notwithstanding the provisions of the preceding two paragraphs, if a business operator handling personal information violates one of the provisions of Article 16, Article 17, Articles 20 through 22, Article 23, paragraph (1), Article 24, Article 36, paragraphs (1), (2) or (5), or if a business operator handling de-identified information violates the provisions of Article 38, and the Personal Information Protection Commission finds it necessary for measures to be taken urgently due to the fact that serious harm is being done to the rights and interests of an individual, the Personal Information Protection Commission may order the business operator handling personal information etc. to stop committing the violation and to take the necessary measures to rectify the violation.

(Restrictions on the Exercise of Authority by the Personal Information Protection Commission)

Article 43

(1) In collecting a report or materials from a business operator handling personal information etc. or in carrying out an on-site inspection, in guiding it, advising it, recommending it or issuing an order to it pursuant to the provisions of one of the preceding three Articles, the Personal Information Protection Commission must not interfere with the freedom of expression, academic freedom, freedom of religion, or freedom of political activity.

(2) In light of the purport of the provision of the preceding paragraph, the Personal Information Protection Commission must not exercise the authority thereof over any action of a business operator handling personal information providing a person set forth in one of the items of Article 76, paragraph (1) with personal information etc. (but only if that person will handle the personal information for the purpose prescribed in the relevant item).

(Delegation of Authority)

Article 44

(1) If the Personal Information Protection Commission finds it necessary for issuing a recommendation or an order effectively under the provisions of Article 42 to an business operator handling personal information etc., owing to a need to ensure the proper handling of personal information etc. in an urgent and intensive manner or any situation prescribed by Cabinet Order, the Commission may delegate authority to the Minister having jurisdiction over the business undertaking in which the business operator handling personal information is engaged (herein after referred to as “Minister having jurisdiction over the business”) under Article 40, paragraph (1), as prescribed by Cabinet Order,

(2) When the Minister having jurisdiction over the business exercises the authority delegated

pursuant to the provision of the preceding paragraph, the Minister must, as prescribed by Cabinet Order, report the results to the Personal Information Protection Commission.

(3) The Minister having jurisdiction over the business may, as prescribed by Cabinet Order, delegate authority all or part delegated pursuant to the provision of paragraph (1) and the authority under the preceding paragraph to the head of local branch bureaus and departments pursuant to the provisions in Article 43 of the Act for Establishment of the Cabinet Office (Act No. 89 of 1999) or other heads of departments or organs as prescribed by Cabinet Order.

(4) The Minister with jurisdiction over the issue may delegate authority (This is limited to matters related to the jurisdiction of the Financial Services Agency, and excludes matters prescribed by Cabinet Order.) delegated pursuant to the provisions of paragraph (1) and the authority under the paragraph (2) to the Commissioner of the Financial Services Agency.

(5) The Commissioner of the Financial Services Agency may, as prescribed by Cabinet Order, delegate a part of the authority delegated pursuant to the provision of the preceding paragraph to the Securities and Exchange Surveillance Commission.

(6) The Commissioner of the Financial Services Agency may, as prescribed by Cabinet Order, delegate a part of the authority (This excludes the authority delegated to the Securities and Exchange Surveillance Commission pursuant to the provision of the preceding paragraph.) delegated pursuant to the provision of paragraph (4) to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau

(7) The Securities and Exchange Surveillance Commission may, as prescribed by Cabinet Order, delegate a part of the authority delegated pursuant to the provision of paragraph (5) to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau.

(8) In regards to the affairs related to the authority delegated to the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau, pursuant to the provision of the preceding paragraph, the Securities and Exchange Surveillance Commission directs and supervises the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau.

(9) In the case of paragraph (5), the request for investigation regarding the request for submission of reports or materials (including when the Director-General of the Local Finance Bureau or the Director-General of the Local Finance Branch Bureau carry out pursuant to the provision of paragraph (7)) made by the Securities and Exchange Surveillance Commission may only be performed by the Securities and Exchange Surveillance Commission.

(Requests of the Minister Having Jurisdiction Over the Business)

Article 45

The Minister having jurisdiction over the business may request the Personal Information Protection Commission to take the appropriate measures in compliance with the provisions of this Act, when the Minister recognizes actions by an business operator handling personal information etc. that violates the provisions of the preceding two Sections, as well as other circumstances when it is recognized that there is a need to secure the appropriate handling of personal information etc. by business operators handling personal information etc.

(The Minister Having Jurisdiction Over the Business)

Article 46

The Minister having jurisdiction over the business under the provisions of this Section is as specified below.

(i) For such handling of personal information etc. by a business operator handling personal information etc. as is related to employment management: the Minister of Health, Labor and Welfare (with handling of personal information as is related to the employment management of mariners, this is the Minister of Land, Infrastructure, Transport and Tourism) and the Minister or the National Public Safety Commission concerned with jurisdiction over the business operator handling personal information etc. (hereinafter referred to as "minister, etc." in the next item);

(ii) For the handling of personal information etc. by a business operator handling personal information etc. outside of the preceding item: the Minister etc. concerned with jurisdiction over the business of the business operator handling personal information etc.. Section 4 Furthering the Protection of Personal Information in the Private Sector

(Accreditation)

Article 47

(1) A corporation (or an association or foundation without legal personality that has made provisions for a representative or manager, the same applies in (b) of item (iii) of the next Article) seeking to perform businesses as set forth in one of the following items with the aim of ensuring that the business operator handling personal information etc., handle that personal information etc. properly may be accredited to do so by the Personal Information Protection Commission:

(i) complaint processing under the provisions of Article 52 for complaints about the handling of personal information etc. by business operator handling personal information etc. which are covered by the corporation's businesses (hereinafter each such business operator is referred to as a "covered business operator");

(ii) providing covered business operators with information about matters that contribute to ensuring the proper handling of personal information etc.;

(iii) services beyond what is set forth in the preceding two items which are necessary for ensuring the proper handling of personal information etc. by covered business operators.

(2) A business operator seeking the accreditation referred to in the preceding paragraph must apply to the Personal Information Protection Commission as prescribed by Cabinet Order.

(3) After granting an accreditation as referred to in paragraph (1), the Personal Information Protection Commission must issue public notice indicating this.

(Conditions for Ineligibility)

Article 48

A person falling under one of the following items may not be accredited as referred to in paragraph (1) of the preceding Article:

(i) a business operator that has been sentenced pursuant to any provision of this Act, if two years have not yet passed since the business operator finished serving the sentence or ceased to be subject to its enforcement;

(ii) a business operator whose accreditation has been revoked pursuant to the provisions of Article 58, paragraph (1), if two years have not yet passed since the revocation;

(iii) a business operator with an executive officer (or with the representative or manager, in an association or foundation without legal personality that has made provisions for the representative or manager; hereinafter the same applies in this Article.) that falls under one of the following categories:

(a) a person that has been sentenced to imprisonment or a heavier punishment or that has been sentenced pursuant to any provisions of this Act, if two years have not yet passed since the individual served out the sentence or was exempted from the execution of the sentence;

(b) a person that, during the 30 days before the revocation, was the officer of a corporation whose accreditation has been revoked pursuant to the provisions of Article 58, paragraph (1), if two years have not yet passed since the revocation.

(Accreditation Standards)

Article 49

The Personal Information Protection Commission must not grant an accreditation unless the Commission finds the application for accreditation referred to in Article 47, paragraph (1) to conform to all of the following requirements:

(i) the applicant has established the necessary methods of business implementation to allow it to perform the businesses set forth in the items of Article 47, paragraph (1).

(ii) the applicant's knowledge, capabilities, and financial base are sufficient to allow it to perform businesses set forth properly and reliably in the items of Article 47, paragraph (1);

(iii) if the applicant engages in business other than the businesses set forth in the items of Article 47, paragraph (1), its engagement in that business is unlikely to give rise to unfairness in the businesses set forth in the items of that paragraph.

(Notification of Discontinuation)

Article 50

(1) Before discontinuing the businesses it has been accredited to perform (hereinafter referred to as "accredited businesses"),) a business operator accredited as referred to in Article 47, paragraph (1) (hereinafter referred to as an "accredited personal information protection organization") must notify in advance the Personal Information Protection Commission of this as prescribed by Cabinet Order.

(2) Upon receiving notification under the provisions of the preceding paragraph, the Personal Information Protection Commission must issue public notice indicating this.

(Covered Business Operators)

Article 51

(1) Each covered business operator of an accredited personal information protection organization must be a business operator handling personal information etc. that is a member of the accredited personal information protection organization or a business operator handling personal information etc. that has agreed to become a member of the accredited personal information protection organization.

(2) An accredited personal information protection organization must disclose the names of its covered business operators to the public.

(Complaint Processing)

Article 52

(1) If a person or other related person files for an accredited personal information protection organization to resolve a complaint about the handling of personal information etc. by a covered business operator, in addition to complying with any request for a consultation about this, providing the person or other party with the necessary advice, and investigate the circumstances to which the complaint pertains, the organization must notify the covered business operator of the substance and content of the complaint and request that it resolve the complaint expeditiously.

(2) If an accredited personal information protection organization finds that it is necessary in connection with the resolution of a complaint under a filing referred to in the preceding paragraph, the organization may request the covered business operator to provide a written or oral explanation or to submit materials.

(3) If a covered business operator has had a request under the provisions of the preceding paragraph from an accredited personal information protection organization, it must not refuse this request without a legitimate reason for doing so.

(Personal Information Protection Guidelines)

Article 53

(1) In order to ensure the proper handling of personal information etc. by its covered business operators, an accredited personal information protection organization must endeavor to hear the opinion of a person representing the consumer or other related persons and to create guidelines (hereinafter referred to as "personal information protection guidelines"), in keeping with the spirit of this Act, for how to specify the Purpose of Use related to personal information, for measures to ensure secure management of the personal information, for procedures to deal with person's requests for disclosure and other matters, for how to create de-identified information, for measures to ensure secure management of deidentified information, and for other such particulars.

(2) When an accredited personal information protection organization has created personal information protection guidelines pursuant to the provision of the preceding paragraph, they must notify the Personal Information Protection Commission prescribed by rules of the Personal Information Protection Commission, without delay, of these personal information protection guidelines. The same applies when these guidelines are changed.

(3) When the Personal Information Protection Commission receives a notification of the personal information protection guidelines under the preceding paragraph, the Personal Information Protection Commission must, as prescribed by rules of the Personal Information Protection Commission, disclose the personal information protection guidelines to the public,

(4) After personal information protection guidelines are disclosed pursuant to the provisions of the preceding paragraph, an accredited personal information protection organization must guide, recommend, and take other necessary measures to cause its covered business operators to observe the personal information protection guidelines.

(Prohibition of Use outside the Purposes)

Article 54

It is prohibited for an accredited personal information protection organization to use information acquired in the course of accredited businesses for purposes other than the authorized businesses use for which the information is provided.

(Restriction on Name Use)

Article 55

A business operator that is not an accredited personal information protection organization must not use a name referring to that business operator as an accredited personal information protection organization, and must not use any other name that is confusingly similar to this.

(Collection of Reports)

Article 56

The Personal Information Protection Commission may have an accredited personal information protection organization provide a report on accredited businesses, to the extent that this is necessary for implementing the provisions of this section.

(Orders)

Article 57

The Personal Information Protection Commission may order an accredited personal information protection organization to improve the implementation method for its accredited businesses, to amend its personal information protection guidelines, or to take any other necessary measures, to the extent that is necessary for implementing the provisions of this section.

(Revocation of Accreditation)

Article 58

(1) The Personal Information Protection Commission may revoke the accreditation of an accredited personal information protection organization if:

(i) it comes to fall under Article 48, item (i) or (iii);

(ii) it ceases to conform to a requirement referred to in one of the items of Article 49; (iii) it violates the provisions of Article 54;

(iv) it fails to comply with an order as referred to in the preceding Article;

(v) it was accredited as referred to in Article 47, paragraph (1) by wrongful means.

(2) After revoking an accreditation pursuant to the provisions of the preceding paragraph, the Personal Information Protection Commission must issue public notice indicating this. Chapter V Personal Information Protection Commission

(Establishment)

Article 59

(1) A Personal Information Protection Commission (hereinafter referred to as the “Commission”) is established pursuant to the provisions of Article 49, paragraph (3) of the Act for Establishment of the Cabinet Office.

(2) The Commission is administratively attached to the Prime Minister.

(Duties)

Article 60

The duties of the Commission are to ensure the proper handling of personal information (this includes guiding, advising and taking other measures for Persons in Charge of Affairs Using the Individual Number, etc. (Person in Charge of Affairs Using the Individual Number, etc. prescribed in Article 12 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure) (Act No. 27 of 2013; hereinafter referred to as the “Number Use Act”)) in order to protect the rights and interests of individuals while ensuring due consideration that proper and

effective use of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched lifestyle for the Japanese citizens among other usefulness of personal information.

(Jurisdictional Affairs)

Article 61

The Commission, in order to accomplish the duties set forth in preceding Article, is responsible for the following affairs:

(i) matters related to the formulation and promotion of the Basic Policy.

(ii) matters related to supervision of the handling of personal information and de-identified information; carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints (This excludes matters set forth in item (iv)).

(iii) matters related to accredited personal information protection organizations

(iv) matters related to supervision or monitoring of the handling of Specific Personal Information (Specific Personal Information prescribed in Article 2, paragraph (8) of the Number Use Act; the same applies in Article 63, paragraph (4)); carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints.

(v) matters related to the Specific Personal Information Protection Assessment (Specific Personal Information Protection Assessment prescribed in Article 27, paragraph (1) of the Number Use Act.)

(vi) matters related to public relations and awareness raising activities about the protection, and appropriate and effective use of personal information.

(vii) matters related to the necessary investigations and research for implementing the affairs set forth in the preceding items.

(viii) matters related to international cooperation pertaining to jurisdictional affairs.

(ix) in addition to those set forth in the preceding items, matters that are assigned to the Commission pursuant to the provisions of laws (this includes orders based on laws).

(Independence of Exercising Authority)

Article 62

The chairperson and members of the Commission exercise their authorities independently.

(Organization etc.)

Article 63

(1) The Commission is composed of the chairperson and eight Commission members. (2) Four of the Commission members are part-time members.

(3) The chairperson and members of the Commission are appointed from among the people of good character and sound knowledge, with the consent of both Houses of the Diet, by the Prime Minister.

(4) The chairperson and members of the Commission include a person who has knowledge and experience in the protection of, and appropriate and effective use of personal information, a person who has knowledge and experience in the protection of consumers, a person who has knowledge and experience in information processing technology, a person who has knowledge and experience in administrative fields used in specific personal information, a person who has sufficient knowledge and experience in matters related to the practice of private enterprises, and a person recommended by a federation, (meaning a federation under Article 263-3, paragraph (1) of the Local Autonomy Act (Act No. 67 of 1947) that has made notification under the provisions of said paragraph).

(Term of office, etc.)

Article 64

(1) The term of office of the chairperson and members of the Commission is five years; provided, however, that the term of office of the chairperson or a member chosen filling a vacancy is the remaining term of office of the predecessor.

(2) The chairperson and members of the Commission may be reappointed.

(3) When the term of office of the chairperson or a member of the Commission expires, said chairperson or member continues to perform their duties until their successor is appointed.

(4) When the term of office of a chairperson or a member of the Commission expires, if the Prime Minister is unable to obtain the consent of both Houses because the Diet is not in session or the House of Representatives has been dissolved, notwithstanding the provisions of paragraph (3) of the preceding Article, the Prime Minister may appoint a chairperson or a member of the Commission from among those people who have the qualifications prescribed in said paragraph.

(5) In the case of the preceding paragraph, the later approval of both Houses of the Diet must be obtained at the first Diet after the appointment. In this case, if the later approval of both Houses of the Diet cannot be obtained, the Prime Minister must, immediately, dismiss the chairperson or member of the Commission.

(Guarantee of Status)

Article 65

The chairperson and members of the Commission, except if they fall under any of the following items, are not dismissed against their will while holding office:

(i) they receive an order to commence bankruptcy proceedings;

(ii) they are punished for violation of this Act or Number Use Act;

(iii) they are punished by imprisonment without required labor or a heavier punishment; or

(iv) the Commission finds that the chairperson or a member of the Commission is incapable of executing his/her duties due to a mental or physical disorder, or , has contravened the duties of

his/her position or has committed misconducts inappropriate for a chairperson or a member of the Commission.

(Dismissal)

Article 66

The Prime Minister, if the chairperson or a member of the Commission falls under one of the items of the preceding Article, must dismiss said chairperson or member of the Commission.

(Chairperson of the Commission)

Article 67

(1) The chairperson of the Commission presides over the business of the Commission and represents the Commission.

(2) The Commission must in advance and from among the full-time members of the Commission, designate a person to substitute the chairperson in case the chairperson is prevented from attending to duties.

(Meetings)

Article 68

(1) The meetings of the Commission are called by the chairperson of the Commission.

(2) The Commission may not, unless four or more members of the Commission are present, hold a meeting nor make any decision.

(3) Any matter before the Commission is decided by a majority of members present and in case of a tie, by the chairperson.

(4) Findings pursuant to the provision of Article 65, item (iv), notwithstanding the provisions of the preceding paragraph, must be made by the unanimous consent of all members present except the member concerned.

(5) With regard to application of the provisions of paragraph (2) of this Article if the chairperson is prevented from attending to duties, the person who substitutes the chairperson as set forth in paragraph (2) of the preceding Article is deemed to be the chairperson.

(Expert Advisors)

Article 69

(1) Expert advisors may be appointed on the Commission to conduct investigations of specialized matters.

(2) Expert advisors are appointed by the Prime Minister based on a request made by the Commission.

(3) Expert advisors are relieved from their position when their investigation regarding the specialized matter is complete.

(4) Expert advisors are on a part-time basis.

(Secretariat)

Article 70

(1) In order to handle the affairs of the Commission, a secretariat is established for the Commission.

(2) The secretariat consists of the secretary-general and other officials.

(3) The secretary-general, under the direction of the chairperson of the Commission, administers the affairs of the secretariat.

(Prohibition of Political Campaigning etc.)

Article 71

(1) The chairperson and members of the Commission, while holding office, must not become an officer of political parties and other political organizations, or actively carry out a political campaign.

(2) The chairperson and full-time members of the Commission, while holding office, must not engage in other jobs with remuneration, run business for profit or operate other businesses seeking monetary profit unless they are authorized by the Prime Minister.

(Confidentiality)

Article 72

The chairperson, members of the Commission, Expert Advisors and officials of the secretariat must not leak or steal any secret that may have come to their knowledge in the course of their duties. The same applies after they retire from their duties.

(Remuneration)

Article 73

The remuneration of the chairperson and members of the Commission is specified separately by law.

(Establishment of Rules)

Article 74

The Commission may establish Rules on Personal Information Protection Commission in order to enforce laws or Cabinet Orders with regard to the affairs under its jurisdiction or based on a special delegation by law or Cabinet Orders. Chapter VI Miscellaneous Provisions

(Scope of Applicability)

Article 75

The provisions of Article 15, Article 16, Article 18 (This excludes paragraph (2).), Articles 19 through 25, Articles 27 through 36, Article 41, Article 42, paragraph (1), Article 43, and Article 76 also applies when a business operator handling personal information acquires personal information of an individual in Japan regarding the provisions of goods or service, and that personal information or the de-identified information created using that personal information is handled outside of Japan.

(Exclusion from Application)

Article 76

(1) The provisions of Chapter IV do not apply to a business operator handling personal information etc. which is set forth in one of the following items if all or part of the purpose for which it handles that personal information is the purpose prescribed in each item:

(i) broadcasting organizations, newspapers, news services, and other journalistic organizations (this includes individuals who work in news reporting): use in news reporting;

(ii) a business operator in the business of creating literary works: use in the creation of literary works;

(iii) a college, university, or other academic ore research-oriented institution or organization, or any business operator belonging to the same: use in academics or research;

(iv) a religious organizations: use in a religious activity (this includes activities incidental thereto);

(v) a political organization: use in a political activity (this includes activities incidental thereto).

(2) The "News reporting" prescribed in item (i) of the preceding paragraph means informing the general public objective facts by presenting them as the truth (this includes stating an opinion or position based on such facts).

(3) A business operator handling personal information etc. as set forth in one of the terms of paragraph (1) must, itself, endeavor to take the necessary and appropriate measures for securely managing personal data or de-identified information, to carry out processing of complaints about the handling of personal information etc., and to take other necessary measures for ensuring the proper handling of personal information etc., and must also endeavor to disclose the content of those measures to the public.

(Affairs Handled by Local Governments)

Article 77

It may be decided, as prescribed by Cabinet Order, that the affairs that this Act prescribes as being part of the authority of the Commission or Article 44, paragraph (1) or (4) prescribes as being part of an authority of a Minister having jurisdiction over the business or the Commissioner of the Financial Services Agency may be handled by the heads of local governments or by other executive agencies.

(Provision of Information to Foreign Authorities)

Article 78

(1) The Commission may provide information, which they deem to be helpful to the duties (this limits to the duties corresponding to the duties of the Commission prescribed in this Act; the same applies in the subsequent paragraph) of foreign authorities (hereinafter referred to as "Foreign Authorities" in this Article) executing foreign laws and regulations equivalent to the Act.

(2) When disseminating information under the preceding paragraph, appropriate measures must be taken so that said information is not used for purposes other than for performing the duties of

Foreign Authorities, and is not used for the investigation into criminal cases (this limits when the fact of a crime has already been specified) or inquiries (hereinafter collectively referred to as "investigations etc.") in foreign countries without the consent under the following paragraph.

(3) The Commission may, having received a request from a Foreign Authority, give consent for the information which it has provided pursuant to the provision of paragraph (1) to be used for the investigation into criminal cases pertaining to said request, except for cases falling under one of the following items:

(i) When a crime subject to the investigation into criminal cases pertaining to said request is a political crime, or when it is found that said request has been made for the purpose of conducting an investigation into a political crime;

(ii) When the action that is subject to the criminal offense investigation etc. related to the request was committed in Japan, and this action does not constitute a criminal offense according to the laws of Japan;

(iii) When the requesting country has not ensured that it will accept a similar request from Japan;

(4) The Commission must, before giving the consent set forth in the preceding paragraph, obtain confirmation from the Minister of Justice that the request does not fall under items (i) and (ii) of the preceding paragraph, and the confirmation from the Minister of Foreign Affairs for the request that does not fall under item (iii) of the preceding paragraph.

(Reporting to the Diet)

Article 79

The Commission must, through the Prime Minister, annually report the progress of its jurisdictional affairs to the Diet and must also make public its outline.

(Communication and Cooperation)

Article 80

The Prime Minister and heads of the administrative organs (meaning the organs established in the Cabinet pursuant to law (other than the Cabinet Office), organs under the supervision of the Cabinet, the Cabinet Office, the Imperial Household Agency, the institutions prescribed in Article 49, paragraphs (1) and (2) of the Act for Establishment of the Cabinet Office, and the institutions prescribed in Article 3, paragraph (2) of the National Government Organization Act (Act No. 120 of 1948)) involved in putting this Act into effect must be in close communication and cooperate with one another.

(Delegation to Cabinet Order)

Article 81

Beyond what is prescribed in this Act, particulars that need to be provided for in order for this Act to be implemented are prescribed by Cabinet Order.

Chapter VII Penal Provisions

Article 82

A person who leaks or steals secrets violating the provisions of Article 72 is subject to imprisonment with required labor for not more than two years or to a fine of not more than 1,000,000 yen.

Article 83

A business operator handling personal information (this includes executives, representatives or managers when the business operator is a corporation (or of an association or foundation without legal personality that has made provisions for a representative or manager; hereinafter the same applies in Article 87, paragraph (1)), its employees or former employees who provides the handled personal information database etc. (this includes copies or processed versions all or part), handled regarding their duties, for wrongful gain for either themselves or a third party, or steals such, is subject to imprisonment with required labor for not more than one year or to a fine of not more than 500,000 yen.

Article 84

A business operator violating an order under Article 42, paragraphs (2) or (3) is subject to imprisonment with required labor for not more than six months or to a fine of not more than 300,000 yen.

Article 85

A business operator falling under one of the following items is subject to a fine of not more than 300,000 yen.

(i) a business operator failing to report or to submit documentations under Article 40, paragraph (1), or making a false report, or submitting falsified documentations, or failing to answer the questions of the investigating officer or gives false testimony for such, or refusing, abstracting or avoiding the investigation;

(ii) A business operator failing to report under Article 56, or making a false report.

Article 86

The provisions of Articles 82 and 83 applies to any person or business operator outside of Japan who commits the criminal offenses of this Articles.

Article 87

(1) If the representative of a corporation, or the agent, employee or other workers of a corporation or individual commits a violation referred to in Articles 83 through 85 in connection with the business of the corporation or individual, in addition to the offender being subject to punishment, the corporation or individual is subject to the fine prescribed in the relevant Article.

(2) When the provisions of the preceding paragraph apply to an association or foundation without legal personality, the representative or manager of the association or foundation represents it in

respect of procedural actions, and the provisions of law on criminal proceedings that have a corporation as the defendant or suspect apply mutatis mutandis.

Article 88

A business operator falling under one of the following items is subject to a noncriminal fine of not more than 100,000 yen:

(i) A business operator violating the provisions of Article 26, paragraph (2), or Article 55;

(ii) A business operator failing to make a notification under Article 50, paragraph (1), or making a false notification.

ภาคผนวก ง
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเยอรมนี (Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680)

Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680

(DSAnpUG-EU)

of 30 June 2017

The Bundestag has adopted the following Act with the approval of the Bundesrat:

Article 1

Federal Data Protection Act

(BDSG)

Table of Contents

Chapter 3

Rights of the data subject

Chapter 4

Obligations of controllers and processors

Part I

Common provisions

Chapter 1

Scope and definitions

Section 1

Scope of the Act

(1) This Act shall apply to the processing of personal data by

1. public bodies of the Federation,
2. public bodies of the *Länder*, where data protection is not governed by *Land* law and where they
   a) carry out federal law or

b) act in the capacity of judicial bodies in matters other than administrative matters.

For private bodies, this Act shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system un-less such processing is conducted by natural persons in the course of a purely personal or domestic activity.

(2) Other federal data protection legislation shall take precedence over the provi-sions of this Act. If such legislation does not govern a matter conclusively or at all which is covered by this Act, then this Act shall apply. The duty to observe the legal obligation of maintaining secrecy or professional or special official confidentiality not based on legal provisions shall remain unaffected.

(3) The provisions of this Act shall take precedence over those of the Administrative Procedure Act where personal data are processed to establish the facts.

(4) This Act shall apply to public bodies. It shall apply to private bodies if

1. the controller or processor processes personal data in Germany,
2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany, or if,
3. although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it does fall within the scope of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the pro-cessing of personal data and on the free movement of such data, and repealing Di-rective 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4 May 2016, p. 1; L 314 of 22 November 2016, p. 72).

If this Act does not apply in accordance with the second sentence, only Sections 8 to 21 and 39 to 44 shall apply to the controller or processor.

(5) The provisions of this Act shall not apply where the law of the European Union, in particular Regulation (EU) 2016/679 in the applicable version, directly applies.

(6) The contracting states of the European Economic Area and Switzerland shall have equal status with the Member States of the European Union with regard to pro-cessing for purposes in accordance with Article 2 of Regulation (EU) 2016/679. Other states shall be regarded as third countries.

(7) With regard to processing for purposes in accordance with Article 1 (1) of Di-rective (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119 of 4 May 2016, p. 89), the states associated with the implementation, application and development of the Schengen Acquis shall have equal status with the Member States of the European Union. Other states shall be regarded as third countries.

(8) Regulation (EU) 2016/679 and Parts 1 and 2 of this Act shall apply accordingly to processing of personal data by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 unless otherwise provided for in this or another Act.

Section 2

Definitions

(1) Public bodies of the Federation are the authorities, judicial bodies and other pub-lic law institutions of the Federation, of direct federal corporations, statutory bodies and foundations established under public law and of their associations irrespective of their legal form.

(2) Public bodies of the *Länder* are the authorities, judicial bodies and other public law institutions of a *Land*, a municipality, an association of municipalities or of other legal persons under public law subject to *Land* supervision and of their associations irrespective of their legal form.

(3) Associations of public bodies of the Federation and the *Länder* which are estab-lished under private law and perform tasks of public administration shall be regarded as public bodies of the Federation irrespective of the participation of private bodies if

1. they operate beyond the borders of a *Land*, or
2. the Federation holds the absolute majority of shares or controls the absolute majority of votes.

Otherwise they shall be regarded as public bodies of the *Länder*.

(4) Private bodies are natural and legal persons, societies and other associations es-tablished under private law unless they are covered by subsections 1 to 3. If a private body performs sovereign tasks of the public administration, it shall be a public body as defined in this Act.

(5) Public bodies of the Federation shall be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law. Public bod-ies of the *Länder* shall also be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law and carry out federal law, and if data protection is not governed by *Land* law.

Chapter 2

Legal basis for processing personal data

Section 3

Processing of personal data by public bodies

Public bodies shall be permitted to process personal data if such processing is nec-essary to perform the task for which the controller is responsible or to exercise official au-thority which has been vested in the controller.

Section 4

Video surveillance of publicly accessible spaces

(1) Monitoring publicly accessible areas with optical-electronic devices (video surveil-lance) shall be permitted only as far as it is necessary

1. for public bodies to perform their tasks,
2. to exercise the right to determine who shall be allowed or denied access or

3. to safeguard legitimate interests for specifically defined purposes

and if there is nothing to indicate legitimate overriding interests of the data subjects. For video surveillance of

1. large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks, or
2. vehicles and large publicly accessible facilities of public rail, ship or bus transport, protecting the lives, health and freedom of persons present shall be regarded as a very important interest.

(2) Appropriate measures shall be taken to make the surveillance and the controller's name and contact details identifiable as early as possible.

(3) Storing or using data collected pursuant to subsection 1 shall be permitted if nec-essary to achieve the intended purpose and if there is nothing to indicate legitimate over-riding interests of the data subjects. Subsection 1, second sentence, shall apply accord-ingly. The data may be further processed for another purpose only if necessary to prevent threats to state and public security and to prosecute crimes.

(4) If data collected from video surveillance are attributed to a particular person, that person shall be informed of the processing in accordance with Articles 13 and 14 of Regu-lation (EU) 2016/679. Section 32 shall apply accordingly.

(5) The data shall be deleted without delay, if they are no longer needed for the in-tended purpose or if the data subject's legitimate interests stand in the way of any further storage.

Chapter 3

Data protection officers of public bodies

Section 5

Designation

(1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Section 2 (5) which take part in competition.

(2) A single data protection officer may be designated for several public bodies, tak-ing account of their organizational structure and size.

(3) The data protection officer shall be designated on the basis of professional quali-ties and, in particular, expert knowledge of data protection law and practices and the abil-ity to fulfil the tasks referred to in Section 7.

(4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

(5) The public body shall publish the contact details of the data protection officer and communicate them to the Federal Commissioner for Data Protection and Freedom of In-formation.

Section 6

Position

(1) The public body shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The public body shall support the data protection officer in performing the tasks referred to in Section 7 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The public body shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall directly report to the highest management level of the public body. The data protection officer shall not be dismissed or penalized by the public body for performing his or her tasks.

(4) The dismissal of the data protection officer shall be permitted only by applying Section 626 of the Civil Code accordingly. The data protection officer's employment shall not be terminated unless there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the pub-lic body has just cause to terminate without notice.

(5) Data subjects may contact the data protection officer with regard to all issues re-lated to processing of their personal data and to the exercise of their rights under Regula-tion (EU) 2016/679, this Act and other data protection legislation. The data protection of-ficer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject.

(6) Where in the course of their activities data protection officers become aware of data for which the head of a public body or a person employed by such a body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and his or her assistants. The person to whom the right to refuse to give evidence applies for employment-related reasons shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable fu-ture. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Section 7

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection of-ficer shall have at least the following tasks:

1. to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680;
2. to monitor compliance with this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing opera-tions, and the related audits;

3. to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Section 67 of this Act;
4. to cooperate with the supervisory authority;
5. to act as the contact point for the supervisory authority on issues relating to pro-cessing, including the prior consultation referred to in Section 69 of this Act, and to consult, where appropriate, with regard to any other matter.

In the case of a data protection officer ordered by a court, these tasks shall not refer to the action of the court acting in its judicial capacity.

(2) The data protection officer may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of inter-ests.

(3) The data protection officer shall in the performance of his or her tasks give due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Chapter 4

Federal Commissioner for Data Protection and Freedom of Information

Section 8

Establishment

(1) The Federal Commissioner for Data Protection and Freedom of Information (Federal Commissioner) shall be a supreme federal authority. It is located in Bonn.

(2) Civil servants of the Federal Commissioner shall be federal civil servants.

(3) The Federal Commissioner may delegate human resources administration and management tasks to other federal bodies as long as doing so does not affect the Federal Commissioner's independence. Personal data of staff members may be transmitted to these bodies as needed for them to perform their delegated tasks.

Section 9

Competence

(1) The Federal Commissioner shall be competent to supervise the public bodies of the Federation, also if they take part in competition as enterprises governed by public law. The provisions of this chapter shall also apply to processors if they are private bodies in which the Federation holds the absolute majority of shares or controls the absolute majori-ty of votes and they process data on behalf of a public body of the Federation

(2) The Federal Commissioner shall not be competent to supervise processing oper-ations of federal courts acting in their judicial capacity.

Section 10

Independence

(1) The Federal Commissioner shall act with complete independence in performing his or her tasks and exercising his or her powers. The Federal Commissioner shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

(2) The Federal Commissioner shall be subject to audit by the Bundesrechnungshof as long as this does not affect his or her independence.

Section 11

Appointment and term of office

(1) At the proposal of the Federal Government, the German Bundestag shall elect without debate the Federal Commissioner with more than half of the statutory number of its members. The person elected shall be appointed by the Federal President. The Feder-al Commissioner must be at least 35 years old at the time of election. He or she shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers. In particular, the Federal Commissioner must have knowledge of data protection law ac-quired from the relevant professional experience and be qualified for judicial office or higher administrative service.

(2) The Federal Commissioner shall swear the following oath before the Federal President: "I swear to do everything in my power to further the good and the benefit of the German people, to protect them from harm and to defend the Basic Law and the laws of the Federation, to perform my duties conscientiously and to exercise justice in all my deal-ings, so help me God." The reference to God may be omitted from the oath.

(3) The Federal Commissioner's term of office shall be five years. It may be renewed once.

Section 12

Official relationship

(1) The Federal Commissioner shall, in accordance with this Act, have official federal status under public law.

(2) The official relationship shall begin upon delivery of the certificate of appointment. It shall end upon expiry of the term of office or upon resignation. The Federal President shall remove the Federal Commissioner from office at the request of the President of the Bundestag if the Federal Commissioner has committed serious misconduct or no longer meets the requirements for performing his or her tasks. If the official relationship is ended or the Federal Commissioner is removed from office, the Federal Commissioner shall be given a document signed by the Federal President. Removal from office shall be effective upon delivery of this document. If the official relationship ends upon expiry of the term of office, at the request of the President of the Bundestag the Federal Commissioner shall be obligated to continue his or her work for no more than six months until a successor has been appointed.

(3) The senior civil servant shall exercise the rights of the Federal Commissioner if the latter is unable to perform his or her duties or if his or her term of office has expired and he or she is no longer obligated to continue his or her work. Section 10 (1) shall apply accordingly.

(4) From the start of the calendar month in which the official relationship commences until the end of the calendar month in which it ends, or, in the case of subsection 2, sixth sentence, until the end of the month in which he or she ceases his or her work, the Feder-al Commissioner shall be paid at the level of a federal civil servant in pay grade B 11 plus the family allowance according to Annex V of the Federal Civil Servants' Remuneration Act. The Federal Travel Expenses Act and the Federal Relocation Expenses Act shall apply accordingly. In all other respects, Section 12 (6), Sections 13 through 20 and 21a (5) of the Act on Federal Ministers shall apply, except that the four-year term of office stip-ulated in Section 15 (1) of the Act on Federal Ministers shall be replaced by a five-year term. By way of derogation from the third sentence in conjunction with Sections 15 through 17 and 21a (5) of the Act on Federal Ministers, the Federal Commissioner's pen-sion shall be calculated, counting his or her term as Federal Commissioner as a pension-able period of service, on the basis of the Federal Act Governing Civil Servants' Pensions and Allowances, if this is more favourable and if, before his or election as Federal Com-missioner, he or she was a civil servant or judge in at least the last position to be held before reaching pay grade B 11.

Section 13

Rights and obligations

(1) The Federal Commissioner shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any incompatible occu-pation, whether gainful or not. In particular, the Federal Commissioner shall not hold any other paid office or pursue any commercial activity or occupation in addition to his or her official duties and shall not belong to the management or supervisory board of a profit-oriented enterprise, nor to a government or legislative body of the Federation or a *Land*. The Federal Commissioner shall not deliver extra-judicial opinions in exchange for pay-ment.

(2) The Federal Commissioner shall inform the President of the Bundestag of any gifts received in connection with his or her office. The President of the Bundestag shall decide how such gifts shall be used. He or she may issue procedural rules and regula-tions.

(3) The Federal Commissioner shall have the right to refuse to give testimony con-cerning persons who have confided in him or her in his or her capacity as Federal Com-missioner and concerning the information confided. This shall also apply to the staff of the Federal Commissioner, on the condition that the Federal Commissioner decides on the exercise of this right. Within the scope of the Federal Commissioner's right of refusal to give testimony, he or she shall not be required to submit or surrender files or other docu-ments.

(4) Even after his or her official relationship has ended, the Federal Commissioner shall be obligated to secrecy concerning matters of which he or she is aware by reason of his or her official duties. This obligation shall not apply to official communications or to matters which are common knowledge or which by their nature do not require confidential-ity. The Federal Commissioner shall decide at his or her due discretion whether and to what extent he or she will testify in or outside

court or make statements concerning such matters; if he or she is no longer in office, the permission of the Federal Commissioner in office shall be required. This shall not affect the legal obligation to report crimes and to uphold the free and democratic order wherever it is threatened. Sections 93, 97, 105 (1), Section 111 (5) in conjunction with Section 105 (1) and Section 116 (1) of the German Fiscal Code shall not apply to the Federal Commissioner or his or her staff. The fifth sen-tence shall not apply where the financial authorities require such knowledge in order to conduct legal proceedings due to a tax offence and related tax proceedings, in the prose-cution of which there is compelling public interest, or where the person required to provide information or persons acting on his or her behalf have intentionally provided false infor-mation. If the Federal Commissioner determines that data protection provisions have been violated, he or she shall be authorized to report the violation and inform the data subject accordingly.

(5) The Federal Commissioner may testify as a witness unless such testimony would

1. be detrimental to the welfare of the Federation or a *Land*, in particular to the security of the Federal Republic of Germany or its relations with other countries, or
2. would violate fundamental rights.

If the testimony concerns ongoing or completed processes which are or could be consid-ered core aspects of executive responsibility, the Federal Commissioner may testify only with the approval of the Federal Government. Section 28 of the Federal Constitutional Court Act shall remain unaffected.

(6) Subsections 3 and 4, fifth to seventh sentences, shall apply accordingly to the public bodies responsible for monitoring compliance with the data protection provisions in the *Länder*.

Section 14

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the Federal Commis-sioner shall have the following tasks:

1. to monitor and enforce the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
2. to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, paying special attention to measures specifically for children;
3. to advise the German Bundestag, the Bundesrat, the Federal Government, and other institutions and bodies on legislative and administrative measures relating to the pro-tection of natural persons' rights and freedoms with regard to the processing of per-sonal data;
4. to promote the awareness of controllers and processors of their obligations under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
5. upon request, to provide information to any data subject concerning the exercise of their rights under this Act and other data protection legislation, including legislation adopted to implement

Directive (EU) 2016/680, and if appropriate, to cooperate with the supervisory authorities in other Member States to that end;

6. to handle complaints lodged by a data subject, or by a body, organization or associa-tion in accordance with Article 55 of Directive (EU) 2016/680, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in par-ticular if further investigation or coordination with another supervisory authority is necessary;
7. to cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, to ensure the consistency of application and enforce-ment of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
8. to conduct investigations on the application of this Act and other data protection legis-lation, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from another supervisory authority or other public au-thority;
9. to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication tech-nologies and commercial practices;
10. to provide advice on the processing operations referred to in Section 69; and
11. to contribute to the activities of the European Data Protection Board.

Within the scope of Directive (EU) 2016/680, the Federal Commissioner shall also perform the task pursuant to Section 60.

(2) To carry out the task listed in subsection 1, first sentence, no. 3, the Federal Commissioner may, on request or at its own initiative, make recommendations to the German Bundestag or one of its committees, the Bundesrat, the Federal Government, other institutions and bodies and the public concerning all matters related to the protection of personal data. At the request of the German Bundestag, one of its committees or of the Federal Government, the Federal Commissioner shall also investigate data protection matters and incidents at public bodies of the Federation.

(3) The Federal Commissioner shall facilitate the submission of complaints referred to in subsection 1, first sentence, no. 6 by measures such as providing a complaint sub-mission form which can also be completed electronically, without excluding other means of communication.

(4) The performance of the duties of the Federal Commissioner shall be free of charge for the data subject. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Federal Commissioner may charge a reasonable fee based on administrative costs, or refuse to act on the request. The Federal Commissioner shall bear the burden of demonstrating the manifestly unfounded or exces-sive character of the request.

Section 15

Activity reports

The Federal Commissioner shall produce an annual activity report which may contain a list of the types of violations reported and the types of measures taken, including penal-ties and measures taken in accordance with Article 58 (2) of Regulation (EU) 2016/679. The Federal Commissioner shall submit this report to the German Bundestag, the Bundesrat and the Federal Government and shall make it available to the public, the Europe-an Commission and the European Data Protection Board.

Section 16

Powers

(1) The Federal Commissioner shall have, within the scope of Regulation (EU) 2016/679, the powers referred to in Article 58 of Regulation (EU) 2016/679. If the Federal Commissioner concludes that data protection legislation has been violated or that there are other problems with the processing of personal data, he or she shall inform the com-petent authority for legal or technical matters and, before exercising the powers referred to in Article 58 (2) (b) to (g), (i) and (j) of Regulation (EU) 2016/679, shall give this authority the opportunity to provide its opinion to the controller within a reasonable period. The op-portunity to provide an opinion may be dispensed with if an immediate decision seems necessary due to imminent danger or in the public interest, or if it would conflict with com-pelling public interests. The opinion should also include a description of the measures taken on the basis of the information from the Federal Commissioner.

(2) If the Federal Commissioner finds that, in data processing for purposes beyond the scope of Regulation (EU) 2016/679, public bodies of the Federation have violated this Act or other data protection legislation or there are other insufficiencies with their pro-cessing or use of personal data, the Federal Commissioner shall lodge a complaint with the competent supreme federal authority and shall require this authority to respond within a period to be determined by the Federal Commissioner. The Federal Commissioner may dispense with a complaint or a response, especially if the problems involved are insignifi-cant or have been remedied in the meantime. The response should also describe the measures taken as a result of the Federal Commissioner's complaint. The Federal Com-missioner may also warn a controller that intended processing operations are likely to vio-late provisions of this Act and other data protection provisions which apply to the data processing in question.

(3) The powers of the Federal Commissioner shall also extend to

1. personal data obtained by public bodies of the Federation concerning the contents of and specific circumstances relating to postal communications and telecommunica-tions, and
2. personal data subject to professional or special official secrecy, especially tax secrecy under Section 30 of the German Fiscal Code.

The fundamental right to privacy of correspondence, posts and telecommunications in Article 10 of the Basic Law shall be limited accordingly.

(4) The public bodies of the Federation shall be obligated to provide the Federal Commissioner and his or her assistants with the following:

1. access to all official premises at all times, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and
2. all information necessary to perform their tasks.

(5) The Federal Commissioner shall work to cooperate with the public bodies re-sponsible for monitoring compliance with data protection provisions in the *Länder* and with the supervisory authorities under Section 40. Section 40 (3), first sentence, second half-sentence, shall apply accordingly.

Chapter 5

Representation on the European Data Protection Board, single contact point, cooperation among the federal supervisory authorities and those of the *Länder* concerning European Union matters

Section 17

Representation on the European Data Protection Board, single contact point

(1) The Federal Commissioner shall serve as the joint representative on the Europe-an Data Protection Board and single contact point (joint representative). The Bundesrat shall elect the head of the supervisory authority of a *Land* to serve as the joint representa-tive's deputy (deputy). The term shall be five years. When the head of the supervisory authority of a *Land* leaves office, his or her function as deputy shall end at the same time. The deputy may be re-elected.

(2) At the deputy's request, the joint representative shall delegate to him or her the leadership of negotiations and the voting right in the European Data Protection Board in matters dealing with the performance of a task for which the *Länder* alone have the right to legislate, or which affect the establishment or procedures of *Land* authorities.

Section 18

Procedures for cooperation among the federal and *Länder* supervisory authorities

(1) The Federal Commissioner and the supervisory authorities of the *Länder* (super-visory authorities of the Federation and the *Länder*) shall work together in European Union matters with the aim of consistently applying Regulation (EU) 2016/679 and Directive (EU) 2016/680. Before submitting a common position to the supervisory authorities of the other Member States, the European Commission or the European Data Protection Board, the supervisory authorities of the Federation and the *Länder* shall give each other the oppor-tunity to comment at an early stage. For this purpose, they shall share all relevant infor-mation. The supervisory authorities of the Federation and the *Länder* shall consult the specific supervisory authorities established under Articles 85 and 91 of Regulation (EU) 2016/679 if these authorities are affected by the matter.

(2) If the supervisory authorities of the Federation and the *Länder* fail to achieve agreement on a common position, the lead supervisory authority, or, in the absence of a lead authority, the joint representative and his or her deputy, shall present a recommenda-tion for a common position. If the joint representative and his or her deputy fail to agree on a recommendation for a common position, the deputy shall determine the recommenda-tion for a common position in matters dealing with the performance of a task for which the *Länder* alone have the right to legislate, or which affect the

establishment or procedures of *Land* authorities. For matters other than those referred to in the second sentence in which the joint representative and deputy fail to agree, the joint representative shall determine the common position. The negotiations shall be based on the position recommended pursuant to the first to third sentences unless the supervisory authorities of the Federation and the *Länder* adopt a different position with a simple majority. The Federation and each *Land* each have one vote. Abstentions shall not be counted.

(3) The joint representative and his or her deputy shall be bound by the common po-sition pursuant to subsections 1 and 2 and shall determine by mutual agreement the con-duct of negotiations according to this common position. Should they fail to reach agree-ment, the deputy shall decide the further conduct of negotiations for the matters referred to in Section 18 (2), second sentence. For other matters, the joint representative shall have the deciding vote.

Section 19

Responsibilities

(1) The lead supervisory authority of a *Land* in the one-stop-shop mechanism pursu-ant to Chapter VII of Regulation (EU) 2016/679 shall be the supervisory authority of the *Land* in which the controller or processor has its main establishment, as referred to in Arti-cle 4 no. 16 of Regulation (EU) 2016/679 or its single establishment in the European Un-ion, as referred to in Article 56 (1) of Regulation (EU) 2016/679. Article 56 (1) in conjunc-tion with Article 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly within the Federal Commissioner's area of responsibility. If there is no agreement on determining the lead supervisory authority, the procedure described in Section 18 (2) shall be applied ac-cordingly.

(2) The supervisory authority with which a data subject has lodged a complaint shall forward the complaint to the lead supervisory authority referred to in subsection 1; in the absence of such a lead supervisory authority, the complaint shall be forwarded to the su-pervisory authority of a *Land* in which the controller or processor has an establishment. If a complaint is lodged with a supervisory authority which is not responsible for the matter, this authority shall forward the complaint to the supervisory authority where the applicant resides, if it is not possible to forward the complaint as referred to in the first sentence. The receiving supervisory authority shall be regarded as the supervisory authority accord-ing to Chapter VII of Regulation (EU) 2016/679 with whom the complaint was lodged, and shall fulfil the obligations referred to in Article 60 (7) to (9) and Article 65 (6) of Regulation (EU) 2016/679.

Chapter 6

Legal remedies

Section 20

Judicial remedy

(1) Recourse to the administrative courts shall be provided for disputes between nat-ural or legal persons and a supervisory authority of the Federation or a *Land* concerning rights according to Article

78 (1) and (2) of Regulation (EU) 2016/679 and Section 61. The first sentence shall not apply to administrative fine proceedings.

(2) The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 7.

(3) For proceedings pursuant to subsection 1, first sentence, the administrative court in whose district the supervisory authority is located shall be locally competent.

(4) In proceedings pursuant to subsection 1, first sentence, the supervisory authority shall be competent to take part.

(5) Parties to proceedings pursuant to subsection 1, first sentence, shall be

1. the natural or legal person as plaintiff or applicant, and
2. the supervisory authority as defendant or respondent.

Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaf-fected.

(6) No preliminary proceedings shall take place.

(7) With respect to an authority or its legal entity, the supervisory authority shall not order immediate execution in accordance with Section 80 (2), first sentence, no. 4 of the Code of Administrative Court Procedure.

Section 21

Application of the supervisory authority for a court decision if it believes that an adequacy decision by the European Commission violates the law

(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pursuant to subsection 1. The Code of Administrative Court Procedure shall be applied in compli-ance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be com-petent to take part. The supervisory authority shall be a party to proceedings pursuant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected. The Federal Administrative Court may give the Euro-pean Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursu-ant to subsection 1 is pending at the European Court of Justice, the Federal Administra-tive Court may order

its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Admin-istrative Court finds that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the Eu-ropean Union to the European Court of Justice.

Part 2
Implementing provisions for processing for pur-poses in accordance with Article 2 of Regulation(EU) 2016/679

Chapter 1
Legal basis for processing personal data

Sub-chapter 1
Processing andof special categories of personal dataprocessing for other purposes

Section 22

Processing of special categories of personal data

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

1. by public and private bodies if
   a) processing is necessary to exercise the rights derived from the right of social se-curity and social protection and to meet the related obligations;
   b) processing is necessary for the purposes of preventive medicine, for the assess-ment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care sys-tems and services or pursuant to the data subject's contract with a health profes-sional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision; or
   c) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medi-cal devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with;
2. by public bodies if

a) processing is urgently necessary for reasons of substantial public interest;

b) processing is necessary to prevent a substantial threat to public security;

c) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or

d) processing is necessary for urgent reasons of defence or to fulfil supra- or inter-governmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures;

and as far as the interests of the controller in data processing in the cases of no. 2 outweigh the interests of the data subject.

(2) In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
3. measures to increase awareness of staff involved in processing operations;
4. designation of a data protection officer;
5. restrictions on access to personal data within the controller and by processors;
6. the pseudonymization of personal data;
7. the encryption of personal data;
8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or tech-nical incident;
9. a process for regularly testing, assessing and evaluating the effectiveness of tech-nical and organizational measures for ensuring the security of the processing;
10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Section 23

Processing for other purposes by public bodies

(1) Public bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected where such processing is necessary for them to perform their duties and if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;

2. it is necessary to check information provided by the data subject because there is reason to believe that this information is incorrect;
3. processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;
4. processing is necessary to prosecute criminal or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Crim-inal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines;
5. processing is necessary to prevent serious harm to the rights of another person; or
6. processing is necessary to exercise powers of supervision and monitoring, to conduct audits or organizational analyses of the controller; this shall also apply to processing for training and examination purposes by the controller, as long as it does not conflict with the legitimate interests of the data subject.

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 24

Processing for other purposes by private bodies

(1) Private bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected if

1. processing is necessary to prevent threats to state or public security or to prosecute criminal offences; or
2. processing is necessary for the establishment, exercise or defence of legal claims,

unless the data subject has an overriding interest in not having the data processed.

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 25

Transfer of data by public bodies

(1) The transfer of personal data by public bodies to public bodies shall be permitted if it is necessary for the transferring body or the third party to whom the data are trans-ferred to perform their duties and the conditions are met which would permit processing pursuant to Section 23. The third party to whom the data are transferred shall process the transferred data only for the purpose for which they were transferred. Processing for other purposes shall be permitted only if the conditions of Section 23 are met.

(2) Public bodies shall be permitted to transfer personal data to private bodies if

1. transfer is necessary for the transferring body to perform its duties and the conditions are met which would permit processing pursuant to Section 23;
2. the third party to whom the data are transferred credibly presents a legitimate interest in knowledge of the data to be transferred and the data subject does not have a legit-imate interest in not having the data transferred; or
3. processing is necessary for the establishment, exercise or defence of legal claims;

and the third party has promised the public body transferring the data that it will process them only for the purpose for which they were transferred. Processing for other purposes shall be permitted if transfer pursuant to the first sentence would be permitted and the transferring body has consented to the transfer.

(3) The transfer of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if the conditions of subsection 1 or 2 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Sub-chapter 2

Special processing situations

Section 26

Data processing for employment-related purposes

(1) Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' repre-sentation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

(2) If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. Consent shall be given in written form, unless a different form is appropriate because of special circumstances. The employer shall inform the em-ployee in text form of the purpose of data processing and of the employee's right to with-draw consent pursuant to Article 7 (3) of Regulation (EU) 2016/679.

(3) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for employment-related purposes shall be permitted if it is necessary to exercise rights or comply with legal

obligations derived from labour law, social security and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data. Subsection 2 shall also apply to consent to the processing of special categories of personal data; consent must explicitly refer to these data. Section 22 (2) shall apply accordingly.

(4) The processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements. The negotiating partners shall comply with Article 88 (2) of Regulation (EU) 2016/679.

(5) The controller must take appropriate measures to ensure compliance in particular with the principles for processing personal data described in Article 5 of Regulation (EU) 2016/679.

(6) The rights of participation of staff councils shall remain unaffected.

(7) Subsections 1 to 6 shall also apply when personal data, including special catego-ries of personal data, of employees are processed without forming or being intended to form part of a filing system.

(8) For the purposes of this Act, employees are

1. dependently employed workers, including temporary workers contracted to the bor-rowing employer;
2. persons employed for occupational training purposes;
3. participants in benefits to take part in working life, in assessments of occupational aptitude or work trials (persons undergoing rehabilitation);
4. persons employed in accredited workshops for persons with disabilities;
5. volunteers working pursuant to the Youth Volunteer Service Act or the Federal Volun-teer Service Act;
6. persons who should be regarded as equivalent to dependently employed workers because of their economic dependence; these include persons working at home and their equivalents;
7. federal civil servants, federal judges, military personnel and persons in the alternative civilian service.

Applicants for employment and persons whose employment has been terminated shall be regarded as employees.

Section 27

Data processing for purposes of scientific or historical research and for statistical purposes

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research pur-poses or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sen-tence.

(2) The rights of data subjects provided in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are likely to render impossi-ble or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

(3) In addition to the measures listed in Section 22 (2), special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose.

(4) The controller may publish personal data only if the data subject has provided consent or if doing so is indispensable for the presentation of research findings on con-temporary events.

Section 28

Data processing for archiving purposes in the public interest

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.

(3) The right of the data subject to rectification according to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add this version to the files.

(4) The rights provided in Article 18 (1) (a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as these rights are likely to render impos-sible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes.

Section 29

Rights of the data subject and powers of the supervisory authorities in the case of secrecy obligations

(1) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the ob-ligation to provide information to the data subject according to Article 14 (1) to (4) of Regu-lation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose in-formation which by its nature must be kept secret, in particular because of overriding legit-imate interests of a third party. The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from the exception pursuant to the third sentence, the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

(2) If in the context of a client-lawyer relationship the data of third persons are trans-ferred to persons subject to a legal obligation of professional secrecy, the transferring body shall not be obligated to inform the data subject according to Article 13 (3) of Regu-lation (EU) 2016/679 unless the data subject has an overriding interest in being informed.

(3) The supervisory authorities shall not have the investigative powers according to Article 58 (1) (e) and (f) of Regulation (EU) 2016/679 with regard to the persons listed in Section 203 (1), (2a) and (3) of the Criminal Code or their processors as far as exercising these powers would violate these persons' obligations to secrecy. If in the context of an investigation a supervisory authority becomes aware of data subject to an obligation of secrecy as referred to in the first sentence, the obligation of secrecy shall also apply to the supervisory authority.

Section 30

Consumer loans

(1) Any body which for the purpose of transfer commercially collects, stores or modi-fies personal data which may be used to evaluate the creditworthiness of consumers shall treat requests for information from lenders in other European Union Member States the same way it treats information requests from domestic lenders.

(2) Anyone who refuses to conclude a consumer loan contract or a contract concern-ing financial assistance for payment with a consumer as the result of information provided by a body as referred to in subsection 1 shall immediately notify the consumer of this re-fusal and the information received. Such notification shall not be made if doing so would endanger public security or order. Section 37 shall remain unaffected.

Section 31

Protection of commercial transactions in the case of scoring and credit reports

(1) For the purpose of deciding on the creation, execution or termination of a con-tractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if

1. the provisions of data protection law have been followed;
2. the data used to calculate the probability value are demonstrably essential for calcu-lating the probability of the action on the basis of a scientifically recognized mathe-matic-statistical procedure;
3. other data in addition to address data are used to calculated the probability value; and
4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented.

(2) The use of a probability value calculated by credit reporting agencies to deter-mine a natural person's ability and willingness to pay shall be permitted in the case of in-cluding information on claims only as far as the conditions of subsection 1 are met and only claims concerning a performance owed which has not been rendered on time are considered

1. which have been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedures,
2. which have been established under Section 178 of the Insolvency Act and have not been disputed by the debtor at the verification meeting,
3. which the debtor has explicitly acknowledged,
4. for which
   a) the debtor has received at least two written reminders after the due date of the claim,
   b) at least four weeks have elapsed since the first reminder,
   c) the debtor was previously informed, at least in the first reminder, of possible con-sideration by a credit reporting agency and
   d) the debtor has not disputed the claim, or
5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the debtor has been informed of possible con-sideration by a credit reporting agency.

The lawfulness of processing, including the calculation of probability values, other data relevant for credit reports pursuant to general data protection law shall remain unaffected.

Chapter 2

Rights of the data subject

Section 32

Information to be provided where personal data are collected from the data subject

(1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the ob-ligation to provide information to the data subject according to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use

1. concerns the further processing of data stored in analogue form, for which the control-ler directly contacts the data subject through the further processing; the purpose is compatible with the original purpose for which the data were collected in accordance with Regulation (EU) 2016/679; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the infor-mation can be regarded as minimal, given the circumstances of the individual case, in particular with regard to the context in which the data were collected;
2. would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;
3. would endanger public security or order or would otherwise be detrimental to the wel-fare of the Federation or a *Land*, and the controller's interests in not providing the in-formation outweigh the interests of the data subject;
4. would interfere with the establishment, exercise or defence of legal claims, and the controller's interests in not providing the information outweigh the interests of the data subject; or
5. would endanger a confidential transfer of data to public bodies.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 13 (1) and (2) of Regula-tion (EU) 2016/679 for the public in precise, transparent, understandable and easily ac-cessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information. The first and second sentences shall not apply in the cases of subsection 1 nos. 4 and 5.

(3) If notification is not provided in the cases of subsection 1 because of a temporary obstacle, the controller shall meet the obligation to provide information, while taking into account the specific circumstances of processing, within an appropriate period after the obstacle has ceased to exist, but no later than two weeks.

Section 33

Information to be provided where personal data have not been obtained from the data subject

(1) In addition to the exception in Article 14 (5) of Regulation (EU) 2016/679 and in Section 29 (1), first sentence, the obligation to provide information to the data subject ac-cording to Article 14 (1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if provid-ing information

1. in the case of a public body
   a) would endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, or
   b) would threaten the public security or order or otherwise be detrimental to the Federation or a *Land*,

and therefore the data subject's interest in receiving the information must not take prece-dence;

2. in the case of a private body

a) would interfere with the establishment, exercise or defence of legal claims, or processing includes data from contracts under private law and is intended to pre-vent harm from criminal offences, unless the data subject has an overriding legit-imate interest in receiving the information; or

b) the responsible public body has determined with respect to the controller that dis-closing the data would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a *Land*; in the case of data pro-cessing for purposes of law enforcement, no determination pursuant to the first half-sentence shall be required.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 14 (1) and (2) of Regula-tion (EU) 2016/679 for the public in precise, transparent, understandable and easily ac-cessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information.

(3) If the provision of information relates to the transfer by public bodies of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Ser-vice, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

Section 34

Right of access by the data subject

(1) In addition to the exceptions in Section 27 (2), 28 (2) and 29 (1), second sen-tence, the data subject's right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if

1. the data subject shall not be informed pursuant to Section 33 (1) no. 1, no. 2 (b) or (3), or

2. the data

a) were recorded only because they may not be erased due to legal or statutory provisions on retention, or

b) only serve purposes of monitoring data protection or safeguarding data,

and providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossi-ble.

(2) The reasons for the refusal to provide information shall be documented. The data subject shall be informed of the reasons for refusing to provide information, unless provid-ing the reasons in law and in fact on which the decision is based would undermine the intended purpose of refusing to provide the information. Data stored for the purpose of providing information to the data subject and preparing such provision may be processed only for this purpose and for purposes of data protection

monitoring; processing for other purposes shall be restricted according to Article 18 of Regulation (EU) 2016/679.

(3) If a public body of the Federation does not provide information to a data subject, such information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would endanger the security of the Federation or a *Land*. The notifica-tion from the Federal Commissioner to the data subject with the results of the data protec-tion assessment shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive infor-mation.

(4) The data subject shall have the right to information about personal data pro-cessed by a public body neither in automated nor in non-automated form and stored in a filing system only if the data subject provides information enabling the data to be located and if the effort required is not disproportionate to the data subject's interest in the infor-mation.

Section 35

Right to erasure

(1) If in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in ac-cordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure. The first and second sentences shall not apply if the personal data were processed unlaw-fully.

(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, subsection 1, first and second sentences shall apply accordingly in the case of Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.

(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, subsection 1 shall apply accordingly in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

Section 36

Right to object

The right to object according to Article 21 (1) of Regulation (EU) 2016/679 with regard to a public body shall not apply if there is an urgent public interest in the processing which outweighs the interests of the data subject or if processing is required by law.

Section 37

Automated individual decision-making, including profiling

(1) In addition to the exceptions given in Article 22 (2) (a) and (c) of Regulation (EU) 2016/679, the right according to Article 22 (1) of Regulation (EU) 2016/679 not to be sub-ject to a decision based solely on automated processing shall not apply if the decision is made in the context of providing services pursuant to an insurance contract and

1. the request of the data subject was fulfilled, or
2. the decision is based on the application of binding rules of remuneration for therapeu-tic treatment and the controller takes suitable measures, in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision; the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full.

(2) Decisions pursuant to subsection 1 may be based on the processing of health da-ta as referred to in Article 4 no. 15 of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in ac-cordance with Section 22 (2), second sentence.

Chapter 3

Obligations of controllers and processors

Section 38

Data protection officers of private bodies

(1) In addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ as a rule at least ten persons dealing with the automated processing of personal data. If the control-ler or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process per-sonal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, they shall designate a data protection officer regardless of the number of persons employed in processing.

(2) Section 6 (4), (5), second sentence, and (6) shall apply, Section 6 (4) however shall apply only if designating a data protection officer is mandatory.

Section 39

Accreditation

The power to act as a certification body in accordance with Article 43 (1), first sen-tence of Regulation (EU) 2016/679 shall be granted by the supervisory authority of the Federation or the *Länder* responsible for data protection supervision of the certification body on the basis of accreditation by the German accreditation body. Section 2 (3), sec-ond sentence, Section 4 (3) and Section 10 (1), first sentence, no. 3 of the Accreditation Body Act shall apply on the condition that data protection falls within the scope of Section 1 (2), second sentence.

Chapter 4

Supervisory authorities for data processing by private bodies

Section 40

Supervisory authorities of the *Länder*

(1) The authorities pursuant to *Land* law shall monitor the application by private bod-ies of data protection legislation within the scope of Regulation (EU) 2016/679.

(2) If the controller or processor has more than one establishment in Germany, Arti-cle 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly in determining which supervisory authority is competent. If more than one authority considers itself competent or not competent, or when the competence is unclear for other reasons, the supervisory authorities shall make a joint decision in accordance with Section 18 (2). Section 3 (3) and (4) of the Administrative Procedure Act shall apply accordingly.

(3) The supervisory authority may process the data it has stored only for purposes of supervision; to this end, it may transfer data to other supervisory authorities. Processing for another purpose shall be permitted in addition to Article 6 (4) of Regulation (EU) 2016/679 if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;
2. processing is necessary to prevent substantial harm to the common good or a threat to public security or to safeguard substantial concerns of the common good; or
3. processing is necessary to prosecute crimes or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Crim-inal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines.

If the supervisory authority determines that data protection legislation has been violated, it shall have the power to inform the data subjects concerned, to report the violation to other bodies responsible for prosecution or punishment and, in the case of serious violations, to notify the trade supervisory authority to take measures under trade and industry law. Sec-tion 13 (4), fourth to seventh sentences shall apply accordingly.

(4) The bodies subject to monitoring and the persons responsible for their manage-ment shall provide a supervisory authority on request with the information necessary to perform their tasks. The person required to provide information may refuse to answer those questions which would expose him- or herself or a relative as referred to in Section 383 (1) nos. 1 to 3 of the Code of Civil Procedure to the risk of criminal prosecution or proceedings under the Administrative Offences Act. The person required to provide infor-mation shall be informed accordingly.

(5) Persons assigned by the supervisory authority to monitor compliance with data protection legislation shall be authorized, as needed to perform their tasks, to enter the property and premises of the body and to have access to all data processing equipment and means. The body shall be obligated to tolerate such access. Section 16 (4) shall ap-ply accordingly.

(6) The supervisory authorities shall advise and support the data protection officers to meet their typical needs. They may demand the dismissal of a data protection officer if he or she does not have the expert knowledge needed to perform his or her tasks or if there is a serious conflict of interests as referred to in Article 38 (6) of Regulation (EU) 2016/679.

(7) The application of the Trade Regulation Code shall remain unaffected.

Chapter 5

Penalties

Section 41

Application of provisions concerning criminal proceedings and proceedings to im-pose administrative fines

(1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 17, 35 and 36 of the Administrative Offences Act shall not apply. Sec-tion 68 of the Administrative Offences Act shall apply on the condition that the regional court shall decide if the administrative fine exceeds the amount of one hundred thousand euros.

(2) Unless this Act provides otherwise, the provisions of the Administrative Offences Act and the general laws on criminal procedures, namely the Code of Criminal Procedure and the Judicature Act, shall apply accordingly in proceedings for violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 56 to 58, 87, 88, 99 and 100 of the Administrative Offences Act shall not apply. Section 69 (4), second sentence of the Administrative Offences Act shall apply on the condition that the public prosecutor's office may stop the proceedings only with the approval of the supervisory authority which issued the administrative decision imposing a fine.

Section 42

Penal provisions

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. transferring the data to a third party or
2. otherwise making them accessible for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or
2. fraudulently acquiringand doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communi-cation pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal pro-ceedings against the person required to provide a notification or a communication or rela-tives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the con-sent of the person required to provide a notification or a communication.

Section 43

Provisions on administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an adminis-trative offence:

1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

(3) Authorities and other public bodies as referred to in Section 2 (1) shall not be subject to any administrative fines.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communi-cation pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a noti-fication or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

Chapter 6

Legal remedies

Section 44

Proceedings against a controller or processor

(1) Proceedings against a controller or a processor for a violation of data protection law within the scope of Regulation (EU) 2016/679 or the rights of the data subject con-tained therein may be brought by a data subject before the court in the place where the controller or processor has an establishment. Proceedings pursuant to the first sentence may also be brought before the court in the place where the data subject has his or her habitual residence.

(2) Subsection 1 shall not apply to proceedings against public authorities acting in the exercise of their sovereign powers.

(3) If the controller or processor has designated a representative pursuant to Article 27 (1) of Regulation (EU) 2016/679, this representative shall also be an authorized recipi-ent in civil law proceedings pursuant to subsection 1. Section 184 of the Code of Civil Procedure shall remain unaffected.

Part 3

Implementing provisions for processing for purposes in accordance with Article 1(1) of Directive (EU) 2016/680

Chapter 1

Scope, definitions and general principles for processing personal data

Section 45

Scope

The provisions of this Part shall apply to the processing of personal data by public bodies competent for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, as far as they process data for the purpose of carrying out these tasks. The public bodies shall be regarded in that case as controllers. The prevention of criminal offences as referred to in the first sentence shall include protection against and prevention of threats to public secu-rity. The first and second sentences shall also apply to those public bodies responsible for executing penalties, measures as referred to in Section 11 (1) no. 8 of the Criminal Code, educational or disciplinary measures as referred to in the Juvenile Court Act or fines. As far as this Part contains provisions for processors, it shall also apply to them.

Section 46

Definitions

For the purposes of this Act

1. ‘personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, di-rectly or indirectly, in particular by reference to an identifier such as a name, an identi-fication number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collec-tion, recording, organization, structuring, storage, adaptation, alteration, retrieval,consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;
3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
4. ‘profiling’ means any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behav-iour, location or movements;
5. ‘pseudonymization’ means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of addition-al information, provided that such additional information is kept separately and is sub-ject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible accord-ing to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
7. ‘controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;
8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. ‘recipient’ means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or other law shall not be regarded as recipients; the pro-cessing of those data by those public authorities shall be in compliance with the ap-plicable data protection rules according to the purposes of the processing;
10. ‘personal data breach’ means a breach of security leading to the accidental or unlaw-ful destruction, loss, alteration, unauthorized disclosure of, or access to, personal da-ta processed;
11. ‘genetic data’ means personal data, relating to the inherited or acquired genetic char-acteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
12. ‘biometric data’ means personal data resulting from specific technical processing re-lating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, in particular fa-cial images or dactyloscopic data;
13. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal in-formation about his or her health status;
14. ‘special categories of personal data’
    a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
    b) genetic data;
    c) biometric data for the purpose of uniquely identifying a natural person;
    d) data concerning health; and
    e) data concerning a natural person’s sex life or sexual orientation;
15. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;
16. ‘international organization’ means an organization and its subordinate bodies gov-erned by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

17. ‘consent’ means any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relat-ing to him or her.

Section 47

General principles for processing personal data

Personal data shall be

18. processed lawfully and fairly;
19. collected for specified, explicit and legitimate purposes and not processed in a man-ner that is incompatible with those purposes;
20. adequate, relevant and not excessive in relation to the purposes for which they are processed;
21. accurate and, where necessary, kept up to date; every reasonable step must be tak-en to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
22. kept in a form which permits identification of data subjects for no longer than is nec-essary for the purposes for which they are processed;
23. processed in a manner that ensures appropriate security of the personal data, includ-ing protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Chapter 2

Legal basis for processing personal data

Section 48

Processing of special categories of personal data

(1) The processing of special categories of personal data shall be allowed only where strictly necessary for the performance of the controller's tasks.

(2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safe-guards may be in particular

1. specific requirements for data security or data protection monitoring;
2. special time limits within which data must be reviewed for relevance and erasure;
3. measures to increase awareness of staff involved in processing operations;
4. restrictions on access to personal data within the controller;
5. separate processing of such data;
6. the pseudonymization of personal data;
7. the encryption of personal data; or
8. specific codes of conduct to ensure lawful processing in case of transfer or pro-cessing for other purposes.

Section 49

Processing for other purposes

Processing personal data for a purpose other than the one for which they were col-lected shall be permitted if the other purpose is one of the purposes listed in Section 45, the controller is authorized to process data for this purpose, and processing is necessary and proportionate to this purpose. Processing personal data for another purpose not listed in Section 45 shall be permitted if it is allowed by law.

Section 50

Processing for archiving, scientific and statistical purposes

Personal data may be processed in the context of purposes listed in Section 45 in ar-chival, scientific or statistical form if doing so is in the public interest and appropriate safe-guards for the legally protected interests of data subjects are implemented. Such safe-guards may consist of rendering the personal data anonymous as quickly as possible, taking measures to prevent unauthorized disclosure to third parties, or in processing them organizationally and spatially separate from other tasks.

Section 51

Consent

(1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject's consent.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily acces-sible form, using clear and plain language.

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.

(4) Consent shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was giv-en must be taken into account. The data subject shall be informed of the intended pur-pose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

(5) If special categories of personal data are to be processed, the consent must ex-plicitly refer to these data.

Section 52

Processing on instructions from the controller

Any person acting under the authority of the controller or of the processor who has access to personal data shall not process those data except on instructions from the con-troller, unless required to do so by law.

Section 53

Confidentiality

Persons employed in data processing shall not process personal data without author-ization (confidentiality). They shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Section 54

Automated individual decision

(1) A decision based solely on automated processing which produces an adverse le-gal effect concerning the data subject or significantly affects him or her shall be permitted only when authorized by law.

(2) Decisions referred to in subsection 1 shall not be based on special categories of personal data unless suitable measures to safeguard the data subject's legally protected and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of spe-cial categories of personal data shall be prohibited.

Chapter 3

Rights of the data subject

Section 55

General information on data processing

The controller shall provide general and publicly accessible information on

1. the purposes of the processing,
2. the rights of data subjects with regard to the processing of their personal data to ac-cess, rectification, erasure and restriction of processing,
3. the names and contact details of the controller and the data protection officer,
4. the right to lodge a complaint with the Federal Commissioner, and
5. the contact details of the Federal Commissioner.

Section 56

Notification of data subjects

(1) If special legislation provides for or requires notifying data subjects of the pro-cessing of their personal data, especially in the case of undercover operations, such noti-fication shall include at least the following information:

1. the information listed in Section 55;
2. the legal basis for the processing;
3. the period for which the personal data will be stored, or if that is not possible, the cri-teria used to determine that period;
4. the categories of recipients of the personal data, if any;
5. where necessary, further information, in particular where the personal data were col-lected without the knowledge of the data subject.

(2) In the cases of subsection 1, the controller may postpone, limit or refrain from no-tification if and so long as

1. the performance of the tasks listed in Section 45,
2. public security, or
3. the legally protected interests of third parties would otherwise be threatened, if the interest in avoiding these threats overrides the inter-est of the data subject in the information.

(3) If the notification relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelli-gence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such notification shall be permitted only with the approval of these bodies.

(4) Section 57 (7) shall apply accordingly in case of restriction pursuant to subsection 2.

Section 57

Right of access

(1) The controller shall inform data subjects on request whether data concerning them are being processed. Data subjects shall also have the right to information about

1. the personal data being processed and the categories to which they belong;
2. The available information on the origin of the data;

3. the purposes of and legal basis for the processing;
4. the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organizations;
5. the period for which the data will be stored, or if that is not possible, the criteria used to determine that period;
6. the existence of the right to rectification or erasure of data or restriction of processing of data by the controller;
7. the right pursuant to Section 60 to lodge a complaint with the Federal Commissioner, and
8. the contact details of the Federal Commissioner.

(2) Subsection 1 shall not apply to personal data recorded only because they may not be erased due to legal or statutory provisions on retention, or only for purposes of monitoring data protection or safeguarding data, if providing information would require a disproportionate effort, and appropriate technical and organizational measures make pro-cessing for other purposes impossible.

(3) No information shall be provided if the data subject does not provide information enabling the data to be located and if the effort required is therefore disproportionate to the data subject's interest in the information.

(4) Subject to the conditions of Section 56 (2), the controller may dispense with the provision of information pursuant to subsection 1, first sentence, or restrict, wholly or part-ly, the provision of information pursuant to subsection 1, second sentence.

(5) If the information to be provided relates to the transfer of personal data to the au-thorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

(6) The controller shall notify the data subject, without delay, in writing of any refusal or restriction of access. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The notification pursuant to the first sentence shallinclude the reasons for the refusal or the restriction unless providing the reasons would undermine the intended purpose of the refusal or restriction of access.

(7) If the data subject is notified pursuant to subsection 6 of the refusal or restriction of access, he or she may exercise his or her right of access also via the Federal Commis-sioner. The controller shall inform the data subject of this possibility and that, in accord-ance with Section 60, the data subject may lodge a complaint with the Federal Commis-sioner or seek a judicial remedy. If the data subject exercises his or her right pursuant to the first sentence, the information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would threaten the security of the Federation or a *Land*. The Federal Commissioner shall at least inform the data subject that all necessary checks have been conducted or that the Federal Commissioner has conducted a review. This notification

may include information as to whether violations of data protection law were found. The notification from the Federal Commissioner to the data subject shall not permit any conclusions to be drawn concerning the information held by the controller un-less the latter agrees to the provision of more extensive information. The controller may refuse to such provision only as far as and for as long as he or she could dispense with or restrict information pursuant to subsection 4. The Federal Commissioner shall also inform the data subject of his or her right to seek a judicial remedy.

(8) The controller shall document the factual or legal reasons on which the decision is based.

Section 58

Right to rectification and erasure and to restriction of processing

(1) The data subject shall have the right to obtain from the controller without delay the rectification of inaccurate data concerning him or her. In particular in the case of statements or assessments, the question of accuracy is not relevant for the content of the statement or assessment. If the accuracy or inaccuracy of the data cannot be ascertained, the controller shall restrict processing instead of erasing the data. In this case, the control-ler shall inform the data subject before lifting the restriction of processing. The data sub-ject may also ask to have incomplete personal data completed, if doing so is appropriate when taking into account the purposes of processing.

(2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without delay where processing such data is unlaw-ful, knowledge of the data is no longer necessary for the performance of tasks, or the data must be erased to comply with a legal obligation.

(3) Instead of erasure, the controller may restrict processing where

1. there is reason to assume that erasure would adversely affect legitimate interests of the data subject,
2. the data must be retained for the purposes of evidence in proceedings serving the purposes of Section 45, or
3. erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage.

Data subject to restricted processing pursuant to the first sentence may be processed only for the purpose which prevented their erasure.

(4) In automated filing systems, technical measures shall ensure that the restriction of processing is clearly recognizable and processing for other purposes is not possible without further examination.

(5) If the controller has rectified inaccurate data, he or she shall communicate the rectification to the body from which he or she received the personal data. In cases of recti-fication, erasure or restriction of processing pursuant to subsections 1 to 3, the controller shall inform recipients to whom the data were transferred about these measures. The re-cipient shall rectify or erase the data or restrict their processing.

(6) The controller shall inform the data subject in writing of any refusal to rectify or erase personal data or restrict its processing. This shall not apply if providing this infor-mation would entail a threat as referred to in Section 56 (2). The information pursuant to the first sentence shall include the reasons for the refusal unless providing the reasons would undermine the intended purpose of the refusal.

(7) Section 57 (7) and (8) shall apply accordingly.

Section 59

Modalities for exercising the rights of the data subject

(1) The controller shall communicate with data subjects in a concise, intelligible and easily accessible form, using clear and plain language. Regardless of special formal re-quirements, when responding to requests, the controller shall provide the information in the same form as the request.

(2) When responding to requests, without prejudice to Section 57 (6) and Section 58 (6) the controller shall inform the data subject in writing about the follow-up to his or her request without delay.

(3) Information provided pursuant to Section 55, any communication made pursuant to Sections 56 and 66, and requests processed pursuant to Sections 57 and 58 shall be free of charge. Where a request pursuant to Sections 57 and 58 is manifestly unfounded or excessive, the controller may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request.

(4) Where the controller has reasonable doubts concerning the identity of a data sub-ject making the request pursuant to Sections 57 or 58, the controller may request the pro-vision of additional information necessary to confirm the identity of the data subject.

Section 60

Right to lodge a complaint with the Federal Commissioner

(1) Without prejudice to any other administrative or judicial remedy, every data sub-ject shall have the right to lodge a complaint with the Federal Commissioner, if the data subject believes that the processing by public bodies of personal data relating to him or her for the purposes listed in Section 45 infringes his or her rights. This shall not apply to the processing of personal data by courts, if they have processed these data in the con-text of their judicial activities. The Federal Commissioner shall inform the data subject of the progress and the outcome of the complaint and of the possibility of a judicial remedy pursuant to Section 61.

(2) If a complaint about processing is lodged with the Federal Commissioner instead of the competent supervisory authority in another Member State of the European Union, the Federal Commissioner shall transmit the complaint to the competent supervisory au-thority without delay. In this case, the Federal Commissioner shall inform the data subject about the transmission of his or her complaint and shall provide further support at the data subject’s request.

Section 61

Legal remedies against decisions of the Federal Commissioner or if he or she fails to take action

(1) Without prejudice to any other legal remedy, every natural or legal person shall have the right to take legal action against a legally binding decision of the Federal Com-missioner.

(2) Subsection 1 shall apply accordingly to data subjects if the Federal Commission-er does not handle a complaint pursuant to Section 60 or does not inform the data subject within three months of the progress or outcome of the complaint.

Chapter 4

Obligations of controllers and processors

Section 62

Processing carried out on behalf of a controller

(1) Where personal data are processed by other persons or bodies on behalf of a controller, the controller shall ensure compliance with the provisions of this Act and other data protection provisions. The data subject shall assert his or her rights to access, rectifi-cation, erasure, restriction of processing and the right to receive compensation against the controller.

(2) A controller may use only processors providing sufficient guarantees to imple-ment appropriate technical and organizational measures in such a manner that the pro-cessing will meet the requirements of the law and ensure the protection of the rights of the data subjects.

(3) Processors shall not engage other processors without prior written authorization by the controller. If the controller has given the processor general authorization to engage other processors, the processor shall inform the controller of any intended changes con-cerning the addition or replacement of other processors. In this case, the controller may object to such changes.

(4) Where a processor engages another processor, the former shall impose on the latter the same data protection obligations as set out in the contract between the controller and the processor as referred to in subsection 5 if these obligations are not already bind-ing for the latter processor because of other legislation. Where that other processor fails to fulfil these obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Processing by a processor shall be governed by a contract or other legal instru-ment that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal instrument shall stipulate, in particular, that the processor

1. acts only on instructions from the controller; if the processor believes that an instruc-tion is unlawful, the processor shall inform the controller without delay;
2. ensures that persons authorized to process the personal data have committed them-selves to confidentiality or are under an appropriate statutory obligation of confidenti-ality;

3. assists the controller by any appropriate means to ensure compliance with the provi-sions on the data subject's rights;
4. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless law requires storage of the personal data;
5. makes available to the controller all information necessary, in particular the logs kept in accordance with Section 76, to demonstrate compliance with these obligations;
6. allows for and contributes to audits conducted by the controller or another auditor mandated by the controller;
7. complies with the conditions referred to in subsections 3 and 4 for engaging another processor;
8. takes all measures required pursuant to Section 64; and
9. assists the controller in ensuring compliance with the obligations pursuant to Sec-tions 64 to 67 and 69 taking into account the nature of processing and the information available to the processor.

(6) The contract referred to in subsection 5 shall be in writing or in an electronic form.

(7) A processor that determines, in violation of this provision, the purposes and means of processing, shall be considered a controller in respect of that processing.

Section 63

Joint controllers

Where two or more controllers jointly determine the purposes and means of pro-cessing, they shall be considered joint controllers. Joint controllers shall determine their respective tasks and responsibilities under data protection law in a transparent manner in an agreement, unless these tasks and responsibilities are already determined by law. In particular, this agreement must indicate which of them must meet which information obli-gations, and how and with respect to whom data subjects may exercise their rights. Such an agreement shall not prevent data subjects from asserting their rights against each of the joint controllers.

Section 64

Requirements for the security of data processing

(1) The controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the legally protected interests of natu-ral persons, shall implement the necessary technical and organizational measures to en-sure a level of security appropriate to the risk when processing personal data, in particular as regards the processing of special categories of personal data. In doing so, the control-ler shall take into account the relevant Technical Guidelines and recommendations from the Federal Office for Information Security.

(2) The measures referred to in subsection 1 may include pseudonymization and en-cryption of personal data, if such means are possible in view of the purposes of pro-cessing. The measures pursuant to subsection 1 should ensure

1. the ongoing confidentiality, integrity, availability and resilience of processing systems and services in connection with processing; and
2. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

(3) In respect of automated processing, the controller and processor, following an evaluation of the risks, shall implement measures designed to

1. deny unauthorized persons access to processing equipment used for processing (‘equipment access control’);
2. prevent the unauthorized reading, copying, modification or erasure of data media (‘data media control’);
3. prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data (‘storage control’);
4. prevent the use of automated processing systems by unauthorized persons using data communication equipment (‘user control’);
5. ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization (‘data access con-trol’);
6. ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘communication control’);
7. ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the per-sonal data were input (‘input control’);
8. ensure that the confidentiality and integrity of personal data are protected during transfers of personal data or during transport of data media (‘transport control’);
9. ensure that installed systems may, in the case of interruption, be restored (‘recovery’);
10. ensure that all system functions perform and that the appearance of faults in the func-tions is reported (‘reliability’);
11. ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system (‘integrity’);
12. ensure that personal data processed on behalf of the controller can only be pro-cessed in compliance with the controller’s instructions (‘processing control’);
13. ensure that personal data are protected against loss and destruction (‘availability con-trol’);
14. ensure that personal data collected for different purposes can be processed separate-ly (‘separability’).

A purpose pursuant to the first sentence, nos. 2 to 5 may be achieved in particular by us-ing state-of-the-art encryption.

Section 65

Notifying the Federal Commissioner of a personal data breach

(1) In the case of a personal data breach, the controller shall notify the Federal Commissioner without delay and, if possible, not later than 72 hours after having become aware of it, of the personal data breach, unless the personal data breach is unlikely to result in a risk to the legally protected interests of natural persons. If the Federal Commis-sioner is not notified within 72 hours, the notification shall be accompanied by reasons for the delay.

(2) A processor shall notify the controller of a personal data breach without delay.

(3) The notification referred to in subsection 1 shall include at least the following in-formation:

1. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. a description of the likely consequences of the personal data breach; and
4. a description of the measures taken or proposed by the controller to address the per-sonal data breach, including measures to mitigate its possible adverse effects.

(4) If it is not possible to provide the information pursuant to subsection 3 with the notification, the controller shall provide this information as soon as it is available.

(5) The controller shall document any personal data breaches. This documentation shall include all the facts relating to the personal data breach, its effects and the remedial action taken.

(6) If the personal data breach involves personal data that have been transmitted by or to a controller in another Member State of the European Union, the information referred to in subsection 3 shall be communicated to the controller in that Member State without delay.

(7) Section 42 (4) shall apply accordingly.

(8) Additional obligations of the controller regarding notifications of personal data breaches shall remain unaffected.

Section 66

Notifying data subjects affected by a personal data breach

(1) If a personal data breach is likely to result in a substantial risk to the legally pro-tected interests of natural persons, the controller shall notify the data subject of the per-sonal data breach without delay.

(2) The notification of the data subject pursuant to subsection 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Section 65 (3) nos. 2 to 4.

(3) Notification shall not be required if any of the following conditions are met:

1. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access them, such as encryption;
2. the controller has taken subsequent measures which ensure that the substantial risk referred to in subsection 1 is no longer likely to exist;
3. it would involve a disproportionate effort; in this case, a public communication shall be made or a similar measure taken to inform the data subjects in an equally effective manner.

(4) If the controller has not informed the data subjects of a personal data breach, the Federal Commissioner may formally determine that, in his or her opinion, the conditions referred to in subsection 3 have not been met. In doing so, the Federal Commissioner shall consider the likelihood of the personal data breach resulting in a high risk as referred to in subsection 1.

(5) The notification of data subjects pursuant to subsection 1 may be delayed, re-stricted or omitted under the conditions referred to in Section 56 (2) unless the interests of the data subjects outweigh those of the controller owing to the high risk resulting from the personal data breach as referred to in subsection 1.

(6) Section 42 (4) shall apply accordingly.

Section 67

Conducting a data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a substantial risk to the legally protected interests of data subjects, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the data subjects.

(2) A joint assessment may address a set of similar processing operations that pre-sent similar substantial risks.

(3) The controller shall involve the Federal Commissioner in carrying out the impact assessment.

(4) The impact assessment shall take the rights of the data subjects affected by the processing into account and shall contain at least the following:

1. a systematic description of the envisaged processing operations and the purposes of the processing;
2. an assessment of the necessity and proportionality of the processing operations in relation to their purposes;
3. an assessment of the risks to the legally protected interests of the data subjects; and
4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demon-strate compliance with the law.

(5) Where necessary, the controller shall carry out a review to assess whether pro-cessing is performed in accordance with the data protection impact assessment.

Section 68

Cooperation with the Federal Commissioner

The controller shall cooperate with the Federal Commissioner in carrying out the lat-ter's tasks.

Section 69

Prior consultation of the Federal Commissioner

(1) The controller shall consult the supervisory authority prior to processing which will form part of a new filing system if

1. a data protection impact assessment pursuant to Section 67 indicates that the pro-cessing would result in a substantial risk to the legally protected interests of data sub-jects in the absence of measures taken by the controller to mitigate the risk; or
2. the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a substantial risk to the legally protected interests of data sub-jects.

The Federal Commissioner may draw up a list of the processing operations which are subject to prior consultation pursuant to the first sentence.

(2) In the case of subsection 1, the Federal Commissioner shall be presented with

1. the data protection impact assessment carried out pursuant to Section 67;
2. where applicable, information on the respective responsibilities of the controller, joint controllers and processors involved in the processing;
3. information on the purposes and means of the envisaged processing;
4. information on the measures and safeguards intended to protect the legally protected interests of the data subjects; and
5. the name and contact details of the data protection officer.

On request, the Federal Commissioner shall be given any other information he or she requires to assess the lawfulness of the processing and, in particular, the existing risks to the protection of the data subjects' personal data and the related safeguards.

(3) If the Federal Commissioner believes that the planned processing would violate the law, in particular because the controller has not sufficiently identified the risk or has not taken sufficient measures to mitigate the risk, he or she may provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, as to which additional measures should be taken. The Federal Commissioner may extend this period by a month, if the planned processing is especially complex. In this case, the Federal Commissioner shall inform the controller and, where applicable, the processor of the extension within one month of receipt of the request for consultation.

(4) If the envisaged processing has substantial significance for the controller's per-formance of tasks and is therefore especially urgent, the controller may initiate processing after the consultation has started but before the period referred to in subsection 3, first sentence, has expired. In this case, the recommendations of the Federal Commissioner shall be taken into account after the fact, and the way the processing is carried out shall be adjusted where applicable.

Section 70

Records of processing activities

(1) The controller shall keep a record of all categories of processing activities under its responsibility. This record shall contain all of the following information:

1. the name and contact details of the controller and, where applicable, of the joint con-troller; and the name and contact details of the data protection officer;
2. the purposes of the processing;
3. the categories of recipients to whom the personal data have been or are to be dis-closed;
4. a description of the categories of data subjects and of the categories of personal data;
5. where applicable, the use of profiling;
6. where applicable, the categories of transfers of personal data to bodies in a third country or to an international organization;
7. information about the legal basis for the processing;
8. the envisaged time limits for the erasure or for a review of the need to store the vari-ous categories of personal data; and
9. a general description of the technical and organizational security measures referred to in Section 64.

(2) The processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing

1. the name and contact details of the processor, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;
2. where applicable, transfers of personal data to bodies in a third country or to an inter-national organization, including the identification of that third country or international organization; and
3. a general description of the technical and organizational security measures according to Section 64.

(3) The records referred to in subsections 1 and 2 shall be in writing or in electronic form.

(4) Controllers and processors shall make these records available to the Federal Commissioner on request.

Section 71

Data protection by design and by default

(1) The controller, both at the time the means of processing are determined and at the time of the processing itself, shall take appropriate measures to implement data pro-tection principles, such as data minimization, in an effective manner, to ensure compli-ance with legal requirements and to

protect the rights of data subjects. In doing so, the controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likeli-hood and severity for the legally protected interests of the data subject posed by the pro-cessing. In particular, personal data shall be processed, and processing systems shall be selected and designed in accordance with the aim of processing as few personal data as possible. Personal data shall be rendered anonymous or pseudonymized as early as pos-sible, as far as possible in accordance with the purpose of processing.

(2) The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific pur-pose of the processing are processed. That applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, the measures must ensure that by default the data are not made accessible by automated means to an indefinite number of persons.

Section 72

Distinction between different categories of data subjects

When processing personal data, the controller shall, as far as possible, make a clear distinction between different categories of data subjects. This applies in particular to the following categories:

1. persons with regard to whom there are serious grounds for believing that they have committed a criminal offence;
2. persons with regard to whom there are serious grounds for believing that they are about to commit a criminal offence;
3. persons convicted of a criminal offence;
4. victims of a criminal offence or persons with regard to whom certain facts indicate that they could be the victim of a criminal offence; and
5. other persons, such as witnesses, persons who can provide information, or contacts or associates of the persons referred to in nos. 1 to 4.

Section 73

Distinction between facts and personal assessments

In processing, the controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments. To this end, the controller shall identify evaluations based on personal assessments as such, as far as possible and reasonable in the context of the processing in question. It must also be possible to deter-mine which body keeps the records on which an evaluation based on a personal assess-ment is based.

Section 74

Procedures for data transfers

(1) The controller shall take appropriate measures to ensure that personal data which are inaccurate or no longer up to date are not transmitted or otherwise made avail-able. To that end, the controller shall, as far as possible with reasonable effort, verify the quality of the data before they are

transmitted or made available. The controller shall also, as far as possible and reasonable, in all transmissions of personal data include the nec-essary information to enable the recipient to assess the degree of accuracy, complete-ness and reliability of the data, and the extent to which they are up to date.

(2) If the processing of personal data is subject to special conditions, in transmis-sions of data the transmitting body shall inform the recipient of these conditions and the requirement to respect them. The obligation of providing information may be met by mark-ing the data accordingly.

(3) The transmitting body shall not apply conditions to recipients in other Member States of the European Union or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Third Part of the Treaty on the Functioning of the Euro-pean Union other than those applicable to similar domestic transmissions.

Section 75

Rectification and erasure of personal data and restriction of processing

(1) The controller shall rectify inaccurate personal data.

(2) The controller shall erase personal data without delay if their processing is unlaw-ful, they must be erased to comply with a legal obligation, or knowledge of the data is no longer necessary for the controller to perform its tasks.

(3) Section 58 (3) to (5) shall apply accordingly. The recipient shall also be informed if inaccurate personal data have been transmitted, or if personal data have been transmit-ted unlawfully.

(4) Without prejudice to any time limits for storing or erasing data defined in law, the controller shall provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data and shall take procedural measures to ensure that these time limits are observed.

Section 76

Logging

(1) Controllers and processors shall provide for logs to be kept for at least the following processing operations in automated processing systems:

1. collection,
2. alteration,
3. consultation,
4. disclosure including transfers,
5. combination, and
6. erasure.

(2) The logs of consultation and disclosure must make it possible to ascertain the justification, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of the data.

(3) The logs may be used only by the data protection officer, the Federal Commis-sioner or the data subject to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for criminal pro-ceedings.

(4) The log data shall be erased at the end of the year following the year in which they were generated.

(5) The controller and the processor shall make the logs available to the Federal Commissioner on request.

Section 77

Confidential reporting of violations

The controller shall ensure that it is able to receive confidential reports of violations of data protection law which have occurred in its area of responsibility.

Chapter 5

Transfers of data to third countries and to international organizations

Section 78

General requirements

(1) If all other conditions applicable to data transfers are met, the transfer of personal data to bodies in third countries or to international organizations shall be permitted if

1. the body or international organization is responsible for the purposes referred to in Section 45, and
2. the European Commission has adopted an adequacy decision pursuant to Article 36 (3) of Directive (EU) 2016/680.

(2) No transfer of personal data shall be permitted, despite an adequacy decision as referred to in subsection 1 no. 2 and the public interest in the data transfer to be taken into account, if in the individual case it cannot be ensured that the data will be handled appro-priately in terms of data protection law and in accordance with fundamental human rights in the area of responsibility of the recipient, or if a transfer would conflict with other over-riding legitimate interests of a data subject. The controller shall base its assessment on whether the recipient in the individual case guarantees appropriate protection of the trans-ferred data.

(3) If personal data which have been transmitted or made available from another Eu-ropean Union Member State are to be transferred pursuant to subsection 1, the compe-tent body of the other Member State must provide prior authorization of the transfer. Transfers without the prior authorization shall be permitted only if the transfer is necessary to prevent an immediate and serious threat to the public security of a country or to essen-tial interests of a Member State and the prior authorization cannot be obtained in time. In the case of the second sentence, the other Member State's body responsible for giving prior authorization shall be informed of the transfer without delay.

(4) The controller transferring data pursuant to subsection 1 shall take appropriate measures to ensure that the recipient will transfer the data onward to other third countries or other international

organizations only with the prior authorization of the controller. When deciding whether to authorize the transfer, the controller shall take into account all rele-vant factors, including the seriousness of the criminal offence, the purpose for which the personal data were originally transferred and the level of personal data protection in the third country or international organization to which the data are to be transferred onward. The transfer shall be authorized only if a direct transfer to the other third country or inter-national organization would be lawful. The responsibility for issuing authorization may also be otherwise provided for.

Section 79

Data transfers with appropriate safeguards

(1) In the absence of a decision pursuant to Article 36 (3) of Directive (EU) 2016/680, transfers which meet the remaining requirements of Section 78 shall be permitted also if

1. appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or
2. the controller has assessed all the circumstances surrounding the transfer and con-cludes that appropriate safeguards exist for the protection of personal data.

(2) The controller shall document transfers pursuant to subsection 1 no. 2. The doc-umentation shall include the date and time of the transfer, the identity of the recipient, the reason for the transfer and the personal data transferred. It shall be provided to the Fed-eral Commissioner on request.

(3) The controller shall file a report to the Federal Commissioner at least once a year covering transfers conducted on the basis of an assessment pursuant to subsection 1 no. 2. In this report, the controller may categorize the recipients and the purpose of the trans-fers appropriately.

Section 80

Data transfers without appropriate safeguards

(1) If in derogation from Section 78 (1) no. 2, no decision pursuant to Article 36 (3) of Directive (EU) 2016/680 or appropriate safeguards as referred to in Section 79 (1) exist, transfers which meet the remaining requirements of Section 78 shall be permitted also if they are necessary

1. to protect the vital interests of a natural person;
2. to safeguard legitimate interests of the data subject;
3. to prevent an immediate and serious threat to the public security of a country;
4. in individual cases for the purposes referred to in Section 45; or
5. in an individual case for the establishment, exercise or defence of legal claims relat-ing to the purposes referred to in Section 45.

(2) The controller shall not transfer data pursuant to subsection 1 if the fundamental rights of the data subject override the public interest in the transfer.

(3) Section 79 (2) shall apply accordingly to transfers pursuant to subsection 1.

Section 81

Other data transfers to recipients in third countries

(1) In special individual cases and if all other requirements for data transfers to third countries are met, controllers may transfer personal data directly to recipients in third countries not referred to in Section 78 (1) no. 1 if the transfer is strictly necessary for the performance of their tasks and

1. in the specific case no fundamental rights of the data subject override the public in-terest in the transfer;
2. transfer to the bodies referred to in Section 78 (1) no. 1 would be ineffective or inap-propriate, in particular because the transfer cannot be carried out in time; and
3. the controller informs the recipient of the purposes of processing and instructs the recipient that the transferred data may be processed only to the extent necessary for these purposes.

(2) In the case of subsection 1, the controller shall inform the bodies referred to in Section 78 (1) no. 1 of the transfer without delay, unless this is ineffective or inappropriate.

(3) Section 79 (2) and (3) shall apply accordingly to transfers pursuant to subsection 1.

(4) In the case of transfers pursuant to subsection 1, the transmitting controller shall obligate the recipient to process the transferred personal data without the controller's con-sent only for the purpose for which they were transferred.

(5) Agreements in the field of judicial cooperation in criminal matters and police co-operation shall remain unaffected.

Chapter 6

Cooperation among supervisory authorities

Section 82

Mutual assistance

(1) The Federal Commissioner shall provide the supervisory authorities in other Eu-ropean Union Member States with information and mutual assistance as far as necessary to implement and apply Directive (EU) 2016/680 in a consistent manner. Mutual assis-tance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

(2) The Federal Commissioner shall take all appropriate measures required to reply to a request for mutual assistance without delay and no later than one month after receiv-ing the request.

(3) The Federal Commissioner may refuse to comply with the request only if

1. he or she is not competent for the subject matter of the request or for the measures he or she is asked to execute; or
2. compliance with the request would violate the law.

(4) The Federal Commissioner shall inform the other state's requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in response to the request. In the case of subsection 3, he or she shall provide reasons for refusing to comply with the request.

(5) The Federal Commissioner shall, as a rule, supply the information requested by the other state's supervisory authority by electronic means and using a standardized for-mat.

(6) The Federal Commissioner shall not charge a fee for action taken pursuant to a request for mutual assistance unless he or she has agreed with the other state's supervi-sory authority in the individual case on the reimbursement of expenses incurred.

(7) The Federal Commissioner's requests for assistance shall contain all the neces-sary information, including in particular the purpose of and reasons for the request. Infor-mation exchanged shall be used only for the purpose for which it was requested.

Chapter 7

Liability and penalties

Section 83

Compensation

(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to de-termine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation.

Section 84

Penal provisions

Section 42 shall apply accordingly to the processing of personal data by public bodies in the context of activities pursuant to Section 45, first, third or fourth sentences.

Part 4

Special provisions for processing in the context of actibities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

Section 85

Processing of personal data in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

(1) The transfer of personal data to a third country, to supranational or intergovernmental bodies or to international organizations in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall be permitted in addition to the cases permitted under Regulation (EU) 2016/679 also if the processing is necessary to perform tasks for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures. The recipient shall be instructed that the transferred data may be used only for the purpose for which they were transferred.

(2) Section 16 (4) shall not apply to processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 by workplaces within the remit of the Federal Ministry of Defence if the Federal Ministry of Defence determines in the individual case that meeting the obligations referred to in that provision would endanger the security of the Federation.

(3) Processing by public bodies of the Federation in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall not be subject to the obligation to provide information in accordance with Article 13 (1) and (2) of Regula-tion (EU) 2016/679

1. in the cases referred to in Section 32 (1) nos. 1 to 3, or
2. if meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of legitimate interests of a third party which outweigh the interests of the data subject in obtaining the information.

If the data subject is not to be informed in the cases of the first sentence, no right of access shall apply. Sections 32 (2) and 33 (2) shall not apply.

Article 2

Amendment of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Pro-tection of the Constitution and on the Federal Office for the Pro-tection of the Constitution

The Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution of 20 December 1990 (*Bundesverfassungsschutzgesetz*, BVerfSchG) (Federal Law Gazette I p. 2954, 2970), last amended by Article 2 (1) of the Act of 16 June 2017 (Federal Gazette I, p. 1634), shall be amended as follows:

[...]

Article 3

Amendment of the Military Counterintelligence Service Act

The Military Counterintelligence Service Act of 20 December 1990 (*Gesetz über den Militärischen Abschirmdienst*, MADG) (Federal Gazette I, p. 2954, 2977), last amended by Article 6 of the Act of 27 March 2017 (Federal Gazette I, p. 562), shall be amended as follows:

[...]

Article 4

Amendment of the Federal Intelligence Service Act

The Federal Intelligence Service Act of 20 December 1990 (*BND-Gesetz*, BNDG) (Federal Law Gazette I p. 2954, 2979), last amended by Article 3 of the Act of 10 March 2017 (Federal Gazette I, p. 410), shall be amended as follows:

[...]

Article 5

Amendment of the Act on Prerequisites and Procedures for Secu-rity Clearance Checks Undertaken by the Federal Government

The Act on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government 20 April 1994 (*Sicherheitsüberprüfungsgesetz*, SÜG) (Federal Law Gazette I p. 867), last amended by Article 1 of the Act of 16 June 2017 (Federal Ga-zette I, p. 1634), shall be amended as follows:

[...]

Article 6

Amendment of the Act to restrict the Privacy of Correspondence, Posts and Telecommunications

The Act to restrict the Privacy of Correspondence, Posts and Telecommunications of 26 June 2001 (*Artikel 10-Gesetz*, G 10) (Federal Law Gazette I, p. 1254, 2298; 2017 I,p.

154), last amended by Article 2 (2) of the Act of 16 June 2017 (Federal Gazette I, p. 1634), shall be amended as follows:

Article 7

Amendment of the Federal Data Protection Act

The Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) in the version published on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 28 April 2017 (Federal Law Gazette I, p. 968), shall be amended as follows:

3. In the table of contents, the following text shall be inserted after the reference to Section 42a:

"Section 42b Application of the supervisory authority for a court decision if it believes that a decision by the Commis-sion violates European law"

4. The following subsection 5a shall be added after Section 22 (5):

"(5a) The Federal Commissioner may delegate human resources administration and management tasks to other federal bodies as long as doing so does not affect the Federal Commissioner's independence. Personal data of staff members may be transferred to these bodies as needed for them to perform their delegated tasks."

5. The following Section 42b shall be added after Section 42a:

"Section 42b

Application of the supervisory authority for a court decision if it believes that a deci-sion by the European Commission violates the law

(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pur-suant to subsection 1. The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be competent to take part. The supervisory authority shall be a party to proceedings pur-suant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Adminis-trative Court Procedure shall remain unaffected. The Federal Administrative Court may give the

European Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursuant to subsection 1 is pending at the European Court of Justice, the Federal Administrative Court may order its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Fed-eral Administrative Court finds that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the ques-tion as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice."

Article 8

Entry into force and expiry

(1) This Act shall enter into force on 25 May 2018, subject to subsection 2. The Fed-eral Data Protection Act in the version published on 14 January 2003 (Federal Law Ga-zette I, p. 66), last amended by Article 7 of this Act shall expire at the same time.

(2) Article 7 shall enter into force on the day following its promulgation.

ภาคผนวก จ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแม็กซิโก (Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties)

THIRD SECTION

EXECUTIVE BRANCH

MINISTRY OF THE ECONOMY

REGULATIONS to the Federal Law on the Protection of Personal Data Held by Private Parties

---

In the margin, a seal with the National Coat of Arms that reads: United Mexican States.- Office of the President of the Republic.

FELIPE DE JESUS CALDERÓN HINOJOSA, President of the United Mexican States, in the exercise of the power vested in me by Article 89(I) of the Constitution of the United Mexican States, pursuant to Article 34 of the Federal Public Administration Organizational Law and Articles 3(X), 18, last paragraph, 45, last paragraph, 46, second paragraph, 54, last paragraph, 60, last paragraph, and 62, last paragraph, of the Law on the Protection of Personal Data Held by Private Parties, hereby issues the following:

REGULATIONS TO THE FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

Chapter I

General Provisions

Purpose

Article 1.

The purpose of this law is to regulate the provisions of the Federal Law on the Protection of Personal Data Held by Private Parties.

Definitions

Article 2.

In addition to the definitions established in Article 3 of the Federal Law on the Protection of Personal Data Held by Private Parties, for the purposes of these Regulations, the following definitions shall apply:

I. Departments: Those indicated in Article 26 of the Federal Public Administration Organizational Law;

II. ARCO rights: The rights of access, rectification, cancellation and objection;

III. Digital environment: The environment made up of the combination of hardware, software, networks, applications, services, or any other technology of the information society that allows for the exchange or computerized or digitalized processing of data;

IV. Exclusion list: Database intended to record free-of-charge the refusal of the data subject to have his personal data processed;

V. Administrative security measures: Combination of actions and mechanisms to establish the management, support, and review of the security of information at an organizational level, the identification and classification of information, as well as the creation of an awareness by personnel and their education and training in the area of protection of personal information;

VI. Physical security measures: Combination of actions and mechanisms, whether or not using technology, intended to:

a) Prevent unauthorized access or damage to or interference with physical installations, critical areas of the organization, equipment and information;

b) Protect mobile, portable, or easily removable equipment located inside or outside installations;

c) Provide maintenance to equipment containing or storing personal data so as to ensure their availability, proper working order, and integrity, and

d) Guarantee the elimination of data in a secure manner;

VII. Technical security measures: Combination of activities, controls, and mechanisms with measurable results that use technology to ensure that:

a) Access to logical data bases or to information in logical format is by identified and authorized users;

b) The access referred to in the previous paragraph is only so that the user may carry out the activities required by his position;

c) Actions to acquire, operate, develop, and maintain secure systems are included, and

d) The management of communications and computerized resources used in the processing of personal data is carried out

VIII. Identifiable individual: Any individual whose identity can be determined, directly or indirectly, by any information. An individual will not be deemed identifiable when to obtain the identification, disproportionate periods of time or activities are required;

IX. Transmission: Communicating personal data between a data controller and a data processor, within or outside of Mexico;

X. Electronic media: Storage medium that can be accessed only by means of the use of a device with electronic circuits that processes its contents in order to examine, modify or store personal data, microfilms included;

XI. Physical media: Storage medium intelligible by sight, in other words, which does not require any device to process its content in order to examine, modify or store the personal data, and Translation from Spanish 26/1/12 Wednesday, December 21, 2011 FEDERAL OFFICIAL GAZETTE (Third Section) 2

XII. Suppression: Activity consisting in eliminating, erasing, or destroying personal data, once the blocking period has elapsed, under security measures previously established by a data controller.

Subject Matter

Article 3.

These Regulations apply to the processing of personal data found on physical or electronic media that make possible, access to personal data according to specific criteria, regardless of the form or method of its creation, type of media, processing, storage, or organization.

These Regulations do not apply when, in order to obtain access to personal data, disproportionate periods of time or activities are required.

Pursuant to Article 3(V) of the Law, personal data may be in numerical, alphabetical, graphic, photographic, acoustic or other any other form, concerning an identified or identifiable individual.

Territorial Scope

Article 4.

These Regulations will be obligatory for all processing when:

I. It is carried out in an establishment of the data controller located in Mexico;

II. It is carried out by a data processor, regardless of its location, on behalf of a data controller established in Mexico;

III. The data controller is not established in Mexico but is subject to Mexican laws as a consequence of entering into a contract or under international law, and

IV. The data controller is not established in Mexico and uses media located in Mexico, unless such media are used only for transit purposes that do not involve processing. For purposes of this subsection, the data controller shall provide the media necessary to comply with the obligations imposed by the Law, its Regulations, and other applicable rules and regulations with respect to the processing of personal data. For this purpose, it shall designate a representative or implement the mechanism that it considers appropriate, provided that by means of this, it is ensured that the

data controller will be able to effectively comply with the obligations that are imposed by law on individuals and corporate bodies that deal with personal data in Mexico.

When the data controller is not located in Mexico, but the data processor is, the latter shall be subject to the provisions related to the security measures contained in Chapter III of these Regulations.

In the case of individuals, the establishment shall mean the location of their main place of business or that used to perform their activities or their home.

In case of corporate bodies, the establishment shall mean the location of the principal management of the business; in case of corporate bodies residing abroad, the location of the principal management of the business in Mexico, or in the absence thereof, that designated by them or any stable installation that allows actual or real performance of an activity.

Information About Individuals Carrying on Business and Data About Their Representatives and Contacts

Article 5.

These Regulations shall not be applicable to the following information:

I. With respect to corporate bodies;

II. With respect to individuals as businessmen and women and professionals, and

III. With respect to individuals who provide services for a corporate body or individual engaged in business and/or providing services consisting only of their first names and surnames, the position or post they hold, as well as some of the following employment data: physical address, electronic address, telephone and fax numbers; provided that this information is used only for purposes of representing the employer or contractor.

Processing Arising from a Legal Relationship

Article 6.

When the processing has as its purpose that of complying with an obligation arising from a legal relationship, it will not be considered as for exclusive personal use.

Public Access Source

Article 7.

For the purposes of Article 3(X) of the Law, the following shall be considered as a public access source:

I. Remote or local electronic, optical and by other technological means of communication, provided that the location of the personal data is intended to facilitate providing information to the public and is open for general consultation;

II. Telephone directories as provided in applicable rules and regulations;

III. Official newspapers, gazettes and/or bulletins as provided in applicable rules and regulations, and

IV. Social communication media. Translation from Spanish 26/1/12 Wednesday, December 21, 2011 FEDERAL OFFICIAL GAZETTE (Third Section) 3

For the cases listed in this Article to be considered public access sources, it will be necessary for them to be able to be consulted by any person not prevented from doing so by any rule or regulation, or without any requirement other than, if applicable, the payment of consideration, a fee or charge.

A public access source shall not be considered as such when the information contained in it is illicit or has an illicit origin.

The processing of personal data from a public access source shall respect the reasonable expectation of privacy to which Article 7, third paragraph, of the Law refers.

Groups Without Legal Status

Article 8.

Those forming part of a group that acts without legal status and that deals with personal data for specific purposes or for purposes of the group shall also be considered as data controllers or data processors, as the case may be.

Chapter II

Principles of Protection of Personal Data

Section I

Principles

Principles of Data Protection

Article 9.

Pursuant to Article 6 of the Law, data controllers shall comply with the following principles governing the protection of personal data:

I. Legitimacy;

II. Consent;

III. Information;

IV. Quality;

V. Purpose;

VI. Loyalty;

VII. Proportionality, and

VIII. Accountability.

In addition, the data controller shall observe the duties of security and confidentiality to which Articles 19 and 21 of the Law refer.

Principle of Legitimacy

Article 10.

The principle of legitimacy requires the data controller to ensure that processing follows and complies with the provisions of Mexican and international law.

Principle of Consent

Article 11.

The data controller must obtain consent for the processing of personal data unless it is not required under Article 10 of the Law. The request for consent shall refer to a specific purpose or purposes, contemplated in the privacy notice.

When personal data are obtained personally or directly from the data subject consent shall be prior to the processing.

Characteristics of Consent

Article 12.

Obtaining consent, tacitly or explicitly, shall be:

I. Free: without error, bad faith, violence or fraud that may affect the expression of the will of the data subject;

II. Specific: refer to one or several specific purposes that justify the processing, and

III. Informed: the data subject must previously know from the privacy notice, the processing to be done with his personal data and the consequences of granting his consent.

Express consent must also be unequivocal, in other words, that there are elements that unquestionably demonstrate that it was given.

Tacit Consent

Article 13.

Unless the Law requires the express consent of the data subject, tacit consent will be valid, as a general rule, pursuant to Articles 12 and 13 of these Regulations.

Request for Tacit Consent

Article 14.

When the data controller seeks to collect personal data directly or personally from the data subject, it shall previously make available to the data subject a privacy notice which shall contain a mechanism by which, as the case may be, the data subject may state his refusal to allow the processing of his personal data for purposes different from those that are necessary and that create a legal relationship between the data controller and the data subject.

In those cases in which personal data is obtained indirectly from the data subject and cause a change in the purposes that were consented to in the transfer, the data controller shall make available to the data subject a privacy notice prior to using the personal data. When the privacy notice is not brought to the notice of the data subject directly or personally, the data subject shall have a period of five day to state, as the case may be, his refusal to allow the processing of his personal data for purposes which are different from those that are necessary and that create a legal relationship between the data controller and the data subject. If the data subject does not state his refusal to the processing of his data in accordance with the foregoing, it shall be understood that he has given his consent to the processing of the same, unless there is evidence to the contrary.

When the data controller uses remote or local electronic, optical or other technological means of communication mechanisms that allow personal data to be obtained automatically and simultaneously at the time the data subject has contact with the mechanisms, at the same time the data subject must be informed of the use of such technology, that through these mechanisms personal data will be obtained, and of the manner in which this can be disabled.

Express Consent

Article 15.

The data controller must obtain the express consent of the data subject when:

I. It is required by law;

II. In the case of financial or property data;

III. In the case of sensitive data;

IV. It is requested by the data controller to prove the same, or

V. It is so agreed by the data subject and the data controller.

Request for Express Consent

Article 16.

When express consent is required by law, the data controller shall provide the data subject with a simple and free-of-charge means of stating this, if he so wishes.

Exceptions to the Principle of Consent

Article 17.

As provided in Articles 10(IV) and 37(VII) of the Law, tacit or express consent will not be required for the processing of personal data when this arises from a legal relationship between the data subject and the data controller.

The previous paragraph shall not apply when the processing of personal data is for purposes different from those that are necessary and create the legal relationship between the data controller and the data subject. In this case, to obtain tacit consent, the data controller shall observe the provisions of Article 8, third paragraph, of the Law and Articles 11, 12, and 13 of these Regulations, and with respect to sensitive, financial, or property data, it shall obtain express consent, or as required by the Law, express and written consent.

Verbal Consent

Article 18.

It is considered that express consent was given verbally when the data subject gives it orally to the data controller in the latter's presence of by the use of any technology that permits oral dialogue.

Written Consent

Article 19.

It will be considered that express consent was given in writing when the data subject provides it in a document bearing his hand-written signature, fingerprint, or any other mechanism authorized by law. In a digital environment, an electronic signature may be used or any mechanism or procedure that is established for this purpose and permits the identification of the data subject and the obtaining of his consent.

Proof of Obtaining Consent

Article 20.

To show that consent has been obtained, the burden of proof always rests upon the data controller.

Withdrawal of Consent

Article 21.

At any time, the data subject may revoke his consent for the processing of his personal data and the data controller shall establish simple and free-of-charge mechanisms to permit the data subject to revoke his consent using at least the same media that he used to provide it, provided that the law does not prevent this.

The mechanisms or procedure established by the data controller to deal with consent revocation requests may not exceed the period contemplated in Article 32 of the Law.

When the data subject requests confirmation that the processing of his personal data has stopped, the data controller shall expressly respond to such request.

If the personal data has been transmitted prior to the date of the revocation of consent and continue to be processed by the data processor, the data controller shall bring the revocation to the attention of the data processor so that he takes the necessary steps to deal with it.

Procedure in the Case of a Refusal to Stop Processing

Article 22.

In case of refusal by the data controller to stop the processing of personal data in the event of a withdrawal of consent, the data subject may file with the Institute the complaint to which Chapter IX of these Regulations refers.

Principle of Information

Article 23.

The data controller must bring to the attention of the data subject the information related to the existence and main characteristics of the processing to which his personal data will be submitted, through a privacy notice, pursuant to the Law and this Regulations.

Characteristics of the Privacy Notice

Article 24.

The privacy notice must be simple, with the necessary information, written in a clear and understandable language, and with a structure and design that facilitates its understanding.

Means of Divulging

Article 25.

For the divulging of privacy notices, the data controller may use physical or electronic formats, verbal means or any other technology, provided it complies with the duty to inform the data subject.

Contents of the Privacy Notice

Article 26.

A privacy notice must contain the items referred to in Articles 8, 15, 16, 33, and 36 of the Law, as well as those established in the guidelines referred to in Article 43(III) of the Law.

Privacy Notice to Obtain Personal Data Directly

Article 27.

As provided in Article 17(II) of the Law, when personal data is obtained directly from the data subject, the data controller must immediately provide at least the following information:

I. The identity and address of the data controller;

II. The purposes of the processing, and

III. The mechanisms offered by the data controller so that the data subject will be aware of the privacy notice in accordance with Article 26 of these Regulations.

The immediate divulging of the above information does not exempt the data controller from the obligation to provide mechanisms for the data subject to become aware of the content of the privacy notice, pursuant to Article 26 of these Regulations.

Privacy Notice in Formats with Limited Space

Article 28.

The data controller may bring a privacy notice to the attention of the data subject, as provided in the previous Article, when it obtains personal data by printed means, provided the space used to obtain the personal data is minimal and limited so that the personal data obtained is also the minimum.

Privacy Notice to Obtain Persona Data Indirectly

Article 29.

When personal data is obtained indirectly from the data subject, the data controller must observe the following in order to bring the privacy notice to the attention of the data subject:

I. When the personal data are processed for the purpose contemplated in the consent to transfer or have been obtained from a public access source, the privacy notice shall be made known in the first contact with the data subject, or

II. When the data controller wishes to use the data for a purpose different from that consented to, in other words, there will be a change of purpose, the privacy notice must be made known prior to the use of the data.

Processing for Marketing, Advertising, or Commercial Exploration

Article 30.

Among the purposes of processing referred to in Article 16(II) of the Law, as applicable, there must be included those concerning processing for marketing, advertising, or commercial exploration. The above is without prejudice to current law which regulates processing for the purposes set out in the previous paragraph when this contemplates higher protection for the data subject than that provided in the Law and these Regulations.

Proof of Privacy Notice

Article 31.

To show that a privacy notice has been given in accordance with the principle of information, the burden of proof shall always rest upon the data controller.

Compensatory Measures

Article 32.

In accordance with Article 18, third paragraph, of the Law, when it is impossible to communicate the privacy notice to the data subject or this requires disproportionate efforts given the number of data subjects or the age of the data, the data controller may implement compensatory measures using mass communication media in accordance with the guidelines issued by the Institute and published in the Federal Official Gazette under which it is possible to use the measures established in Article 35 of these Regulations.

The cases not included in the guidelines issued by the Institute shall require the express authorization of the latter, prior to the implementation of the compensatory measure, in accordance with the procedure established in Articles 33 and 34 of these Regulations.

Request for Authorization of Compensatory Measures

Article 33.

The procedure to obtain authorization from the Institute for the use of compensatory measures using mass communication media to which the previous Article refers, shall always be initiated at the request of the data controller.

The data controller shall submit the request directly to the Institute or by any other means that the latter has authorized for this purpose. The request shall contain the following information:

I. The name of the data controller making the application, and as applicable, of its representative, as well as a copy of the official identification proving legal status and the original for comparison. In the case of a representative, a copy of the document proving his right to represent the data controller must be submitted, as well as the original for comparison;

II. Address to receive notifications and name of person authorized to receive them;

III. The processing to which it is intended to apply the compensatory measure and its principal features, such as purpose; type of personal data processed; if transfers are to take place; details of the data subjects, among them age, geographic location, educational and socio-economic level, among others;

IV. Causes or justification for the impossibility of bringing a privacy notice to the attention of the data subjects or the disproportionate efforts that this would require. The data controller shall state the number of data subjects involved, age of the data, whether or not there is direct contact with the data subjects, and their economic situation;

V. Type of compensatory measure sought to be used and for what period of time it will be published;

VI. Proposed text for the compensatory measure, and

VII. Documents that the data controller considers necessary to submit to the Institute.

Procedure for Authorization of Compensatory Measures

Article 34.

The Institute shall have a period of ten days following receipt of the request for compensatory measures to issue its decision on the matter.

If the Institute does not issue a decision within the period established, the compensatory measure request will be considered as authorized.

Once the request is submitted by the data controller to the Institute, the latter shall weigh the disproportionate efforts to make known the privacy notice, taking the following into account:

I. The number of data subjects;

II. The age of the data;

III. The economic situation of the data controller;

IV. The geographic area and sector in which the data controller operates, and

V. The compensatory measure to be adopted.

When weighing the request, if the Institute considers that the compensatory measure proposed does not comply with the principle of information, it may propose to the data controller

the adoption of a compensatory measure different from that suggested by the data controller in its request.

The proposal of the Institute shall be brought to the attention of the data controller so that it may take such action as it considers appropriate within a period of no more than five days, calculated from the day following that on which it received notification.

If the data controller does not respond within the period mentioned in the previous paragraph, the Institute shall resolve the matter based on the file of the matter.

When the Institute decides that the data controller does not justify the impossibility of bringing the privacy notice to the attention of the data subject or that this requires disproportionate efforts, the use of compensatory measures shall not be authorized.

Any authorization given by the Institute shall be valid unless the circumstances under which the compensatory measure was authorized change.

Features of Compensatory Measures

Article 35.

Mass communication compensatory measures must contain the information provided in Article 27 of these Regulations and shall be made known by means of privacy notices published in any of the following media:

I. Newspapers with national circulation;

II. Local newspapers or specialized journals when it is proven that the data subjects reside in a particular federative entity or are part of a particular activity; III. Web site of the data controller;

IV. On a hyperlink on an web site of the Institute, set up for this purposes, when the data controller does not have its own web site;

V. Informational posters; VI. Information spots on the radio, or

VII. Other alternative mass communication media.

Quality Principle

Article 36.

The personal data processed by the data controller will meet the principle of quality when they are exact, complete, pertinent, correct, and up-to-date as required to comply with the purpose for which they are processed.

Personal data are presumed to comply with quality when they are directly provided by the data subject until he declares and proves otherwise, or the data controller has objective evidence contradicting this.

When the personal data were not obtained directly from the data subject, the data controller must take reasonable measures for it to meet the principle of quality in accordance with the type of personal data and the processing conditions.

The data controller must adopt the mechanisms that it considers necessary to ensure that personal data dealt with are exact, complete, pertinent, correct, and up-to-date so that the truth of the data are not altered and the data subject thereby prejudiced by this.

Preservation Periods

Article 37.

The preservation periods for personal data may not exceed those necessary to achieve the purposes that justify the processing and shall comply with the law applicable to the subject matter involved and take into account the administrative, accounting, tax, legal, and historical aspects of the information. After the purpose or purposes of processing have been achieved, the data controller must cancel the data in its collection after blocking them for subsequent suppression.

Procedure for Preserving, Blocking, and Suppression of Personal Data

Article 38.

Data controllers must establish and document procedures for the preservation, and if necessary, blockage and suppression of personal data, including periods of preservation thereof, in accordance with the previous Article.

Proof of Compliance with Preservation Periods

Article 39.

The data controller must show that personal data is preserved, or if applicable, blocked, suppressed, or cancelled in accordance with the periods set out in Article 37 of these Regulations or taking into account a request of the right to cancelation.

Principle of Purpose

Article 40.

Personal data may be processed only to comply with the purpose or purposes set out in the privacy notice, as provided in Article 12 of the Law.

For purposes of the previous paragraph, the purpose or purposes set out in the privacy notice shall be determined, something which will be achieved when with clarity, and without giving rise to confusion and in an objective manner, the purpose for which personal data will be processed is specified.

Differentiation of Purposes

Article 41.

The data controller shall identify and distinguish in the privacy notice between the purposes that give rise to and are necessary for the legal relationship between the data controller and the data subject from those that are not.

Objection to Processing for Different Purpose

Article 42.

The data subject may refuse or revoke his consent, as well as object to the processing of his personal data for purposes different from those that are necessary or that gave rise to the legal relationship between the data controller and the data subject, without this having as a consequence, the termination of the processing for the latter two purposes.

Processing for Different Purpose

Article 43.

The data controller may not carry out processing for different purposes that are not compatible or analogous to those for which the personal data was originally collected and which were mentioned in the privacy notice unless:

I. A law or regulation explicitly permits it, or

II. The data controller has obtained consent for the new processing.

Principle of Loyalty

Article 44.

The principle of loyalty establishes the obligation to process personal data giving priority to the protection of the interests of the data subject and the reasonable expectation of privacy, as provided in Article 7 of the Law. Misleading or fraudulent means may not be used to collect and process personal data. It will be considered that the behavior is fraudulent or misleading when:

I. There is fraud, bad faith or negligence in the information provided to the data subject about the processing;

II. The reasonable expectation of privacy of the data subject referred to in Article 7 of the Law is violated, or

III. The purposes were not established in the privacy notice.

Principle of Proportionality

Article 45.

Only personal data that are necessary, appropriate, and relevant in connection with the purposes for which they were obtained may be processed.

Principle of Minimization

Article 46.

The data controller must make reasonable efforts to limit the personal data processed to the minimum necessary in accordance with the purpose of the processing taking place.

Principle of Accountability

Article 47.

Pursuant to Articles 6 and 14 of the Law, the data controller has the obligation to protect and be responsible for the processing of personal data found in its custody or in its possession or for those it communicated to a data processor, whether or not the latter is located in Mexico.

To comply with this obligation, the data controller may use standards, best international practices, corporate policies, self-regulation arrangements, or any other mechanism that it determines is adequate for such purpose.

Measures for the Principle of Accountability

Article 48.

Pursuant to Article 14 of the Law, the data controller must adopt measures to guarantee the proper processing of personal data, giving priority to the interests of the data subject and the reasonable expectation of privacy.

The measures that may be adopted by the data controller include at least the following:

I. Prepare privacy policies and programs that are binding and enforceable within the organization of the data controller;

II. Implement a program of training, updating, and raising the awareness of personnel about obligations in matters of protection of personal data;

III. Establish an internal supervision and monitoring system, as well as external inspections or audits to verify compliance with privacy policies;

IV. Dedicate resources for the implementation of privacy programs and policies;

V. Implement a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them;

VI. Periodically review the security policies and programs to determine modifications required;

VII. Establish procedures to receive and respond the questions and complaints of data subjects;

VIII. Have mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof;

IX. Establish measures to protect personal data, in other words, a group of technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Law and these Regulations, or

X. Establish measures to trace personal data, in other words, actions, measures, and technical procedures that will allow the tracing of personal data while being processed.

Data Processor

Article 49.

The data processor is the individual or corporate body, public or private, not a part of the organization of the data controller, that alone or together with others, processes personal data on behalf of a data controller as a result of a legal relationship linking the same and setting out the scope of service to be provided.

Obligations of the Data Processor

Article 50.

The data processor shall have the following obligations with respect to the processing carried out on behalf of the data controller:

I. Process personal data only according to the instructions of the data controller;

II. Not to process personal data for a purpose other than as instructed by the data controller;

III. Implement the security measures required by the Law, these Regulations, and other applicable laws and regulations;

IV. Maintain confidentiality regarding the personal data subject to processing;

V. Eliminate personal data that were processed after the legal relationship with the data controller is concluded or upon instructions of the data controller, provided there is no legal requirement for the preservation of the personal data, and

VI. Not to transfer personal data unless the data controller so determines, the communication arises from subcontracting, or if so required by a competent authority.

The agreements between the data controller and data processor related to the processing of personal data must be in accordance with the corresponding privacy notice.

Relationship between the Data Controller and Data Processor

Article 51.

The relationship between the data controller and data processor must be established by contract or other legal instrument decided upon by the data controller and that permits its existence, scope, and contents to be proven.

Processing of Personal Data in Cloud Computing

Article 52.

For the processing of personal data in services, applications, and infrastructure in what is called "cloud computing," in which the data controller adheres to the same by general contractual conditions or clauses, such services may only be used when the provider:

I. Complies at least with the following:

a) Has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;

b) Makes transparent subcontracting that involves information about the service which is provided;

c) Abstains from including conditions in providing the service that authorize or permits it to assume the ownership of the information about which the service is provided, and

d) Maintains confidentiality with respect to the personal data about which it provides the service, and

II. Has mechanisms at least for:

a) Disclosing changes in its privacy policies or conditions of the service it provides;

b) Permitting the data controller to limit the type of processing of personal data about which it provides the service;

c) Establishing and maintaining adequate security measures to protect the personal data about which it provides the service;

d) Ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it, and

e) Impeding access to personal data by those who do not have proper access or in the event of a request duly made by a competent authority, so inform the data controller.

In any case, the data controller may not use services that do not ensure the proper protection of personal data.

For purposes of these Regulations, cloud computing shall mean the model for the external provision of computer services on demand that involves the supply of infrastructure, platform, or

software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. Regulatory agencies, within the scope of their authority, and assisting the Institute, shall issue guidelines for the proper processing of personal data in what is called “cloud computing.”

Transmission of Personal Data

Article 53.

National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or his consent obtained.

The data processor shall be considered as a data controller, together with its own obligations, when it:

I. Uses the personal data for a purpose different from that authorized by the data controller, or

II. Makes a transfer without complying with the instructions of the data controller.

The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to these Regulations.

Subcontracting Services

Article 54.

Any subcontracting of services by the data processor implying the processing of personal data must be authorized by the data controller and shall be made in the name and on behalf of the latter.

After obtaining authorization, the data processor must formalize the relationship with the subcontractor by contract or other instrument that permits its existence, scope, and contents to be proven.

The subcontracted individual or corporate body will assume the same obligations that are established for the data processor under the Law, these Regulations, and other applicable laws and regulations.

The data processor shall have the obligation of proving that the subcontracting was done with the authorization of the data controller.

Subcontracting Authorization

Article 55.

When the contract or legal instruments that have formalized the relationship between the data controller and the data processor contemplates that the latter may subcontract services, the authorization referred to in the previous Article will be understood to be given through the stipulations in those.

If subcontracting is not contemplated in the contract or legal instruments to which the previous paragraph refers, the data processor must obtain authorization from the data controller prior to subcontracting. In both cases, the provisions of the previous article must be observed.

Section II Sensitive Personal Data

Situations Giving Rise to the Creation of Sensitive Personal Databases

Article 56.

Pursuant to Article 9, second paragraph, of the Law, databases containing sensitive personal data may be created only when:

I. The law so requires;

II. It is justified under Article 4 of the Law, or

III. The data controller requires it for legitimate, concrete purposes in accordance with its explicit activities or purposes.

Chapter III Security Measures for Processing Personal Data

Scope

Article 57.

The data controller, and as applicable, the data processor, must establish and maintain administrative, physical, and if applicable technical, security measures for the protection of personal data pursuant to the Law and this Chapter, regardless of the processing system. For the purposes of this Chapter, security measures mean security control or group of controls to protect personal data.

The above is without prejudice to the laws and regulations in force with respect to security issued by the competent authorities in the corresponding sector when they contemplate greater protection for data subjects than that provided in the Law and these Regulations.

Reduction in Penalties

Article 58.

Pursuant to Article 65 (III) of the Law, whenever there is a breach of personal data security, the Institute may take into consideration compliance with its recommendations in determining a reduction in a penalty.

Security Measures

Article 59.

To establish and ensure effective security measures, the data controller may take its own security measures or may contract these to an individual or corporate body.

Factors to Determine Security Measures

Article 60.

The data controller shall determine the security measures applicable to personal data, taking into account the following factors:

I. The inherent risk by type of personal data;

II. The sensitivity of the personal data processed;

III. Technological development, and

IV. The possible consequences of a violation for the data subjects.

In addition, the data controller shall try to take the following factors into account:

I. The number of data subjects;

II. The vulnerabilities previously encountered in the processing systems;

III. The risk as a result of the potential quantitative or qualitative value that the personal data may have to an unauthorized third party having possession of the data, and

IV. Other factors that may have an impact upon the level of risk or which result from other laws or regulations applicable to the data controller.

Actions to Take for the Security of Personal Data

Article 61.

In order to establish and maintain the security of personal data, the data controller must take into account the following actions:

I. Prepare an inventory of personal data and processing systems;

II. Determine the duties and obligations of those who process personal data;

III. Have a risk analysis of personal data consisting of identifying dangers and estimating the risks to the personal data;

IV. Establish the security measures applicable to personal data and identify those implemented effectively;

V. Analyze the gap between existing security measures and those missing that are necessary for the protection of personal data;

VI. Prepare a work plan for the implementation of the missing security measures arising from the gap analysis;

VII. Carry out reviews and audits;

VIII. Train personnel who process personal data, and

IX. Keep a record of personal data storage media.

The data controller shall prepare a document setting out security measures arising from the previous paragraphs.

Updating Security Measures

Article 62.

Data controllers must update the document setting out security measures when the following events occur:

I. Modifications to the security measures or processes are made for their continuous improvement, arising from revisions of the security policy of the data controller;

II. Substantial modifications are made in the processing arising from a change in the level of risk;

III. Processing systems are violated, as provided in Article 20 of the Law and Article 63 of these Regulations, or

IV. There is an impact upon the personal data other than the above. In the case of sensitive personal data, the data controller shall review, and if necessary update the security document once a year.

Security Breaches

Article 63.

Breaches of the security of personal data which occur in each processing phase are:

I. Loss or unauthorized destruction;

II. Theft, misplacement or unauthorized copying;

III. Unauthorized use, access or processing, or

IV. Unauthorized damage, alteration or modification.

Notification of Security Breaches

Article 64.

The data controller must inform the data subject, without delay, of breaches that significantly prejudice the property or nonpecuniary rights of the data subjects upon confirming the breach and having taken action to trigger an exhaustive review of the magnitude of the breach so that the prejudiced data subjects may take the appropriate measures.

Minimum Information for Data Subject in the Event of Security Breaches

Article 65.

The data controller must inform the data subject of at least the following:

I. The nature of the breach;

II. The personal data compromised;

III. Recommendations to the data subject concerning measures that the latter can adopt to protect his interests;

IV. Corrective actions implemented immediately, and

V. The means by which he may obtain more information in this regard.

Corrective Measures in the Event of Security Breaches

Article 66.

In case of a breach of the personal data, the data controller must analyze the causes of its occurrence and implement the corrective, preventive and improvement steps to make the security measures adequate in order to avoid a repetition of the breach.

Chapter IV T
Transfers of Personal Data
Section I
General Provisions

Scope

Article 67.

A transfer refers to the communication of personal data to a person other than the data subject, data controller or data processor, within or outside Mexico.

Conditions for a Transfer

Article 68.

Any transfer of personal data, whether national or international, is subject to the consent of the data subject, with the exceptions provided in Article 37 of the Law; the data subject must be so informed by a privacy notice and the transfer be limited to the purposes that justify it.

Proof of Compliance with Transfer Obligations

Article 69.

For purposes of demonstrating that the transfer, whether national or international, took place in accordance with the Law and these Regulations, the burden of proof in all cases rests upon the data controller that made the transfer and on the receiver of the personal data.

Transfers within the Data Controller's Group

Article 70.

In the case of transfers of personal data among holding companies, subsidiaries, or affiliates under the common control of the same group as that of the data controller, or to a parent company or to any company belonging to the same group as that of the data controller, the mechanism to ensure that the receiver of the personal data complies with the provisions of the Law, these Regulations, and other applicable laws and regulations, may be the existence of internal rules to protect personal data whose observance is obligatory, provided that these comply with the requirements of the Law, these Regulations, and other applicable laws and regulations.

Section II

National Transfers Specific

Conditions Applicable to National Transfers

Article 71.

To carry out a transfer of persona data within Mexico, it shall be necessary for the data controller to comply with the provisions of Article 36 of the Law and Article 68 of these Regulations.

Receiver of Personal Data

Article 72.

The receiver of personal data will be subject to the Law and these Regulations as a data controller and shall deal with personal data in accordance with that agreed upon in the privacy notice communicated to it by the transferring data controller.

Formalization of National Transfers

Article 73.

A transfer shall be formalized by a mechanism that allows it to be shown that the transferring data controller communicated to the receiving data controller the conditions under which the data subject consented to the processing of his personal data.

Section III

International Transfers

Specific Conditions Applicable to International Transfers

Article 74.

Without prejudice to the provisions of Article 37 of the Law, international transfers of personal data will be possible when the receiver of the personal data assumes the same obligations as those of the data controller transferring the personal data.

Formalization of International Transfers

Article 75.

For such purposes, a data controller that transfers personal data may use contracts and other legal instruments which contain at least the same obligations as those to which the data controller transferring personal data is subject, as well as the conditions under which the data subject consented to the processing of his personal data.

Opinion of the Institute Concerning Transfers

Article 76.

Data controllers, if considered necessary, may request the opinion of the Institute as to whether an international transfer that they are carrying out complies with the Law and these Regulations.

Chapter V Coordination among Authorities

Issuing Secondary Regulations

Article 77.

When the competent government department or agency, responding to the needs of which it has become aware in the area it regulates, determines the need to regulate the processing of personal data held by private parties, within the ambit of its jurisdiction it may issue or modify specific regulations, in cooperation with the Institute.

Furthermore, when the Institute, as a consequence of the performance of its duties, becomes aware of the need to issue or modify specific regulations to regulate the processing of personal data in a certain sector or activity, it may propose to the competent department or agency the preparation of a preliminary draft.

Coordination Mechanisms

Article 78.

For the preparation, issuance, and publication of the regulation referred to in Article 40 of the Law, the department or agency and the Institute shall establish the appropriate coordination mechanisms.

In all cases, the department or agency and the Institute, within their respective jurisdictions, shall determine the provisions of the regulation of the processing of personal data in the corresponding sector or activity.

Chapter VII

Binding Self-Regulation

Scope of Self-Regulation

Article 79.

Pursuant to Article 44 of the Law, individuals or corporate bodies may agree among themselves or with civil or government organizations, national or foreign, on binding self-regulation arrangements in matters of personal data protection, complementing the provisions of the Law, these Regulations, and the regulations issued by departments or agencies in this matter and within their jurisdiction. Furthermore, through such arrangements, the data controller may prove to the Institute compliance with the obligations set forth in said regulations.

The above is in order to harmonize the processing carried out by those who become bound by the arrangements and facilitate the exercise of the rights of the data subjects.

Specific Objectives of Self-Regulation

Article 80.

Self-regulation arrangements may be codes of ethics or of good professional practice, seals of confidence, privacy policies, corporate privacy rules, and other mechanisms, that include specific rules or standards and have the following main objectives:

I. Cooperate in compliance with the principle of accountability to which the Law and these Regulations refer;

II. Establish qualitative processes and practices in the field of protection of personal data to supplement the provisions of the Law;

III. Encourage data controllers to establish policies, processes and best practices for compliance with the principles of the protection of personal data, guaranteeing privacy and confidentiality of the personal data in their possession;

IV. Encourage data controllers to voluntarily keep records or certifications regarding compliance with the provisions of the Law, and show to data subjects their commitment to the protection of personal data;

V. Identify data controllers that have privacy policies aligned with the implementation of the principles and rights of the Law, as well as workforce competence for the proper performance of their obligations in this regard;

VI. Facilitate coordination among different self-regulation arrangements recognized internationally;

VII. Facilitate transfers among data controllers that have self-regulation arrangements such as safe harbor;

VIII. Promote the commitment of data controllers to render accounts and adopt internal policies consistent with external criteria, as well as to support mechanisms to implement privacy policies, including tools, transparency, continuous internal supervision, risk assessment, external inspections and remediation systems, and

IX. Channel mechanisms for alternative dispute resolution among data controllers, data subjects and third parties, such as conciliation and mediation.

These arrangements shall be binding upon those who join them; nevertheless, joining will be voluntary.

Incentives for Self-Regulation

Article 81.

When a data controller adopts and complies with a self-regulation arrangement, this will be taken into consideration by the institute in deciding upon any reduction in a penalty in the event of a finding of a failure to comply with the Law or these Regulations. In addition, the Institute may decide upon other incentives for the adoption of self-regulation arrangements, as well as mechanisms to facilitate administrative proceedings before it.

Minimum Content of Self-Regulation Arrangements

Article 82.

Self-regulation arrangements must take into account the parameters issued by the Ministry, in cooperation with the Institute, for the proper development of this type of self-regulation mechanisms and measures, considering at least the following:

I. The agreed upon arrangement, which may be ethics codes, good professional practice code, seals of confidence, or others that enable data subjects to identify the data controllers committed to protecting their personal data;

II. The extent of the application of the self-regulation arrangements;

III. The procedures or mechanisms to be used to ensure effective personal data protection by those adhering to them, as well as to measure such effectiveness; IV. Internal and external systems to supervise and monitor;

V. Training programs for those processing personal data;

VI. Mechanisms to facilitate the rights of the data subjects;

VII. Identification of adhering individuals or corporate bodies to make it possible to recognize data controllers that meet the requirements of a given self-regulation arrangement and are committed to the protection of the personal data they hold, and

VIII. Effective corrective measures in case of a failure to comply.

Certification in Personal Data Protection

Article 83.

Binding self-regulation arrangements may include the certification of data controllers in the area of protection of personal data.

If a data controller decides to submit to a certification process, this shall be granted by a certifying individual or corporate body apart from the data controller in accordance with the guidelines that the parameters referred to in Article 43(V) set for this purpose.

Accredited Individuals and Corporate Bodies

Article 84.

The individuals and corporate bodies who are accredited as certifiers shall have as their principal duty that of certifying that the privacy policies, programs, and procedures voluntarily put into place by data controllers are followed in practice and ensuring proper processing and that the security measures adopted are adequate for their protection. For this purpose, certifiers may adopt mechanisms such as inspections and audits.

The procedure for accrediting the certifiers to which the previous paragraph refers shall be carried out in accordance with the parameters contemplated by Article 43 (V) of the Law. The certifiers shall guarantee their independence and impartiality in granting certificates, as well as compliance with the requirements and guidelines established in such parameters.

Self-Regulation Parameters

Article 85.

The self-regulation parameters referred to in Article 43 (V) of the Law shall contain mechanisms for the accreditation and revocation of the accreditation of individuals and corporate bodies as

certifiers, as well as their duties; general guidelines for granting certificates in the protection of personal data, and the procedure for the notification of binding self-regulation arrangements.

Registration of Self-Regulation Arrangements

Article 86.

The self-regulation arrangements notice of which has been given in accordance with Article 44, last paragraph, of the Law form part of a registry to be administered by the Institute and in which all those complying with the requirements established in the parameters contemplated in Article 43 (V) of the Law will be included.

Chapter VII
Rights of Personal Data Subjects and their Exercise
Section I General Provisions

Exercise of Rights

Article 87.

The exercise of any of the ARCO rights does not exclude the possibility of exercising another of them nor of this being a requirement to be fulfilled prior to exercising any of these rights.

Restrictions on the Exercise of Rights

Article 88.

The exercise of ARCO rights may be restricted for reasons of national security, by laws and regulations of a public policy nature, for reasons of public health and safety, or to protect the rights of third parties in those cases and to the extent contemplated in the laws applicable to the matter, or by a decision of a competent authority well-founded in law and fact.

Persons Authorized to Exercise Rights

Article 89.

ARCO rights may be exercised:

I. By the data subject, after proving his identity through the presentation of a copy of his identity document and having shown the original for comparison. Also admissible will be the electronic instruments by which it is possible to reliably identify the data subject and other authentication mechanisms permitted by law or previously established by the data controller. The use of an advanced electronic signature or the electronic instrument replacing it will exempt the data subject from the need to present a copy of the identification document, and

II. By the representative of the data subject, after proving:

a) the identity of the data subject;

b) the identity of the representative, and

c) the existence of the representation by means of a public instrument or simple power of attorney signed before two witnesses or by personal attendance by the data subject.

For the exercise of ARCO rights by minors or by a person under interdiction or without legal capacity, the representation rules of the Federal Civil Code shall apply.

Means to Exercise Rights

Article 90.

For the exercise of ARCO rights, the data subject may submit, personally or through a representative, a request to the data controller using the means established in the privacy notice. For such purpose, the data controller shall make available to the data subject remote or local electronic communication means or such others as it considers appropriate.

In addition, the data controller may establish forms, systems, and other simplified methods to help data subjects exercise the ARCO rights and these must be mentioned in the privacy notice.

Customer Service

Article 91.

When the data controller has customer service of any type or services for the resolution of claims related to the service rendered or the products offered, the data controller may resolve requests for the exercise of ARCO rights through such services, provided that the periods do not contradict those set out in Article 32 of the Law. In this case, the identity of the data subject is deemed proven by the means established by the data controller for the identification of the data subjects in providing its services or contracting for its products, provided that such means guarantee the identity of the data subject.

Specific Procedure for the Exercise of ARCO Rights

Article 92.

When the law applicable to certain databases or processing establishes a specific procedure for requesting the exercise of ARCO rights, the provisions that offer the better guarantees to the data subject and that do not contradict the provisions of the Law, shall apply.

Costs

Article 93.

The exercise of ARCO rights shall be simple and free-of-charge and the data subject need only pay expenses for shipping, reproduction, and if applicable, certification of documents, with the exception provided in Article 35, second paragraph, of the Law.

The costs of reproduction may not be higher than the costs of recovery of the corresponding material.

The data controller may not establish, as the only way to present requests to exercise ARCO rights, any service or means with a cost.

Address of the data subject

Article 94.

For the purposes of Article 29 (I) of the Law, the request for access must show an address or some other means for notification of the response to the request. If this requirement is not complied with, the data controller shall deem the request not presented, and note this for the record.

Request Registry

Article 95.

The data controller must process any request for the exercise of ARCO rights. The period to resolve the request will be calculated from the day it was received by the data controller and it will record the latter on the acknowledgement of receipt given to the data subject.

The period stated shall be interrupted if the data controller requires information from the data subject, as provided in the following Article.

Request for Additional Information

Article 96.

If the information provided in the request is insufficient or inaccurate and so cannot be dealt with, or if the documents referred to in Articles 29 (II) and 31 of the Law are not attached, the data controller may ask the data subject once, within five days after receipt of the request, to provide the items or documents necessary for its processing. The data subject shall have ten days to attend to the request, calculated from the day following the date on which it was received. If no response is provided within this period, the request will be considered as not having been submitted.

If the data subject attends to the request for information, the period that the data controller has to respond to the request begins to run from the day following that on which the data subject attends to the request.

If the data controller does not request additional documentation from the data subject to prove his identity or the legal status of his representative, the same shall be considered as proven by the documentation provided by the data subject in his request.

Extension of Periods

Article 97.

Pursuant to Article 32, second paragraph of the Law, if the data controller decides to extend the period to respond a request for the exercise of ARCO rights or the period for implementing the response, it must notify the applicant of the justification for the extension, within either of the following periods:

I. In the case of an extension of twenty days to communicate the decision adopted on the admissibility of the request, the justification for the extension must be communicated within the same period, calculated from the date the request is received, or

II. In the case of an extension of fifteen days to enforce the right in question, the justification of the extension must be communicated within the same period, calculated from the date of the notification of the admissibility of the request.

Response from the Data Controller

Article 98.

In all cases, the data controller must respond the request for the exercise of ARCO rights that it receives, regardless of whether or not the personal data of the data subject appear in its databases, within the periods established in Article 32 of the Law.

The response from the data controller shall only refer to the personal data that have been specifically mentioned in the request and must be presented in a legible and understandable format with easy access. In case of the use of codes, initials, or keys, the corresponding meanings must be provided.

On Site Access to Personal Data

Article 99.

When access to the personal data is on site, the data controller must determine the period during which the data subject may come to consult them, which may not be less than fifteen days. If this period lapses and the data subject has not come to obtain access to his personal data, it will be necessary to submit a new request.

Refusal by Data Controller

Article 100.

A data controller must justify its refusal to grant the exercise of ARCO rights and inform the data subject of his right to request the commencement of proceedings for the protection of rights with the Institute.

Section II
Right to Access and its Exercise

Right of Access

Article 101.

Pursuant to Article 23 of the Law, the data subject has the right to obtain his personal data from the data controller, as well as information regarding the conditions and general features of the processing.

Means of Complying with Right of Access

Article 102.

The obligation to give access will be considered as complied with when the data controller makes available to the data subject personal data on site, respecting the period set out in Article 99 of these Regulations, or by issuing photocopies or using magnetic, optical, sound, visual, or holographic media, as well as other information technologies contemplated in the privacy notice. In all cases access must be granted in formats which are readable and comprehensive to the data subject.

When the data controller considers it appropriate, it may agree with the data subject upon reproduction media for the information different from that mentioned in the privacy notice.

Section III
Right to Rectification and its Exercise

Right to Rectification

Article 103.

Pursuant to Article 24 of the Law, the data subject may request, at any time, from the data controller, a rectification or correction of his personal data that are inaccurate or incomplete.

Requirement to Exercise Right to Rectification

Article 104.

The request for rectification must indicate to what personal data it refers, as well as the rectification or correction to be made, and must be accompanied by the documentation proving the admissibility of the request. The data controller may offer mechanisms for the benefit of the data subject to facilitate the exercise of this right.

Section IV
Right of Cancellation and its Exercise

Right of Cancellation

Article 105.

Pursuant to Article 25 of the Law, cancellation means stopping the processing of personal data by the data controller, starting from their blockage and subsequent supression.

Exercise of Right of Cancellation

Article 106.

The data subject may request, at any time, that the data controller cancel the personal data when he considers that they are not being processed in accordance with the principles and duties established by the Law and these Regulations.

The cancellation shall proceed with respect to all personal data of the data subject contained in a database, or only part thereof, as requested.

Blockage

Article 107.

If the cancellation is warranted, and without prejudice to the provisions of Article 32 of the Law, the data controller shall:

I. Establish a blockage period only for the purpose of determining possible liability with respect to the processing, up to the legal or contractual limitation period, and so notify the data subject or his representative in the reply to the request for cancellation to be issued within the period of twenty days set out in Article 32 of the Law;

II. Take appropriate security measures for the blockage;

III. Put the blockage into effect within the period of fifteen days set out in Article 32 of the Law, and

IV. After the blockage period, carry out the supression using the security measures previously established by the data controller.

Purpose of Blockage

Article 108.

Pursuant to Article 3 (III) of the Law, the blockage has as its purpose the prevention of processing, with the exception of storage, or possible access by any person, unless otherwise established by law.

The blockage period will be until the limitation period or contractual period.

Section V

Right of Objection and its Exercise

Right of Objection

Article 109.

Pursuant to Article 27 of the Law, the data subject may, at any time, object to the processing of his personal data or require it to stop when:

I. There is a legitimate reason for doing so and his specific situation so requires, in which case, he must justify the fact that, even though the processing is lawful, it must stop in order to avoid its continuation causing prejudice to the data subject, or

II. He needs to state his objection to the processing of his personal data in order to avoid processing for specific purposes.

The exercise of the right to object may not be exercised in those cases where the processing is necessary to comply with a legal obligation imposed on the data controller.

Exclusion Lists

Article 110.

In order to exercise the right to object, data controllers may prepare their own exclusion lists, including in them the data of the people who have stated their refusal to allow the processing of their personal data, either for their products or those of third parties.

Furthermore, data controllers may prepare common exclusion lists by industry or in general.

In both cases, the recording of the data subject in such lists must be free-of-charge and give to the data subject proof of being recorded on the list by the means established by the data controller.

Public Registry of Consumers and Public Registry of Users

Article 111.

The Public Register of Consumers referred to in the Federal Law for Consumer Protection and the Public Register of Users referred to in the Law for the Protection and Defense of Users of Financial Services continue in force and will be governed in accordance with the laws referred to and any rules and regulations arising therefrom.

Section VI
Decisions Made without Human Intervention

Processing in Decisions Made without Human Intervention

Article 112.

When personal data is used in decision-making without human intervention, the data controller must so inform the data subject.

In addition, the data subject may exercise his right of access in order to discover the personal data used as part of the decision-making process, and as the case may be, his right to rectification, when he considers that some of the personal data used are incorrect or incomplete so that, in accordance with the mechanisms implemented by the data controller for this purpose, he can request a reconsideration of the decision made.

Chapter VIII
Procedure for Protection of Rights

Initiation

Article 113.

A request to begin proceedings for the protection of rights must be submitted by the data subject or his representative; either by a document in no particular format, on the forms set by the Institute, or through the system established by the latter, within the period contemplated by Article 45 of the Law.

Both the form and the system must be made available by the Institute on its website and in every one of the authorized offices as determined by it.

When filing a request for the protection of rights, the data subject or his representative must prove his identity or legal status, respectively, pursuant to Article 89 of these Regulations. In the case of the data subject, the latter may also prove his identity by electronic means or by other methods, as provided by applicable law.

The Institute may consider the identity of the data subject or the legal status of the representative as having been proven when the same has already been proven to the data controller upon exercising his ARCO rights.

Methods for Submitting a Request for the Protection of Rights

Article 114.

A request for the protection of rights must be filed at the address of the Institute, in its authorized offices, by certified mail with acknowledgment of receipt, or in the system referred to in the previous Article, in the latter case, provided that the person has the certification of electronic identification referred to in Article 69-C of the Federal Law of Administrative Procedures. In any case, the applicant shall be given an acknowledgment of receipt showing in a legally acceptable manner, the date of filing of the request.

When the applicant files his request by electronic means through the system established by the Institute, it will be understood that he accepts that notices will be made to him through the same system or by other electronic media generated by this, unless he indicates a different means for notifications.

When the request is submitted by the data subject or his representative in an office authorized by the Institute, the latter shall certify the proof of identity or, as the case may be, the legal status of the representative, and may send or register by electronic means, both the request and the attached documents. In this case, the request will be taken as having been received, for purposes of the period to which Article 47 of the Law refers, when the Institute, using this same media, generates proof of receipt.

The foregoing is without prejudice to the authorized office sending to the Institute by certified mail, proof of the identity of the data subject or the document proving the legal status of the representative, as well as the request and attached documents, to be included in the file of the matter.

If the data subject sends the request and its attachments by certified mail, the period to which Article 47 of the Law refers shall be calculated from the date stated on the date or receipt stamp of the Institute.

Admissibility

Article 115.

Proceedings for the protection of rights may be pursued when the data subject is not satisfied with actions or omissions of the data controller with respect to the exercise of ARCO rights when:

I. The data subject has not received a response from the data controller;

II. The data controller does not give access to the personal data requested or does so in a form that is not understandable;
III. The data controller refuses to make rectifications or corrections to personal data;
IV. The data subject disagrees with the information delivered because he considers that it is incomplete or does not correspond to what was requested or with the cost or type of reproduction;
V. The data controller refuses to cancel the personal data;
VI. The data controller persists in processing in spite of a proper request for objection, or refuses to deal with the request for objection, and
VII. For other reasons that in the opinion of the Institute are admissible under the Law or these Regulations.

Requirements of the Request for Protection of Rights

Article 116.

The applicant must attach to his request for protection of rights, pursuant to Article 46 of the Law, the following information and documents:
I. A copy of the request for the exercise of rights in question, as well as a copy of the documents attached for each of the parties, if applicable;
II. The document proving that he acts on his own behalf or in representation of the data subject;
III. The document showing the response of the data controller, if applicable;
IV. If he challenges the failure by the data controller to respond, a copy of the acknowledgement or proof of receipt, by the data controller, of the request for the exercise of rights;
V. The documentary evidence offered to prove his claim;
VI. The document in which he indicates the other evidence offered by him, pursuant to Article 119 of these Regulations, and
VII. Any other document he considers ought to be submitted to the judgment of the Institute.

If the data subject cannot prove that he attended the data controller, either because the latter had refused to receive the request to exercise his ARCO rights or to issue a receipt, he shall bring this to the attention of the Institute by filing a document with it and this shall be given to the data controller for his response, in order to guarantee for the data subject the exercise of his ARCO rights.

Admission Order

Article 117.

The Institute shall decide upon the admissibility of the request for protection of rights within a period of no more than ten days after its receipt.

After agreeing upon the admission, the Institute shall communicate this to the applicant, providing a copy to the data controller within a period no more than ten days, attaching all documents filed by the data subject, in order to allow the data controller to provide such response as it considers appropriate within a period of fifteen days from notification, with the obligation to offer the evidence it deems relevant.

Admission or Rejection of Evidence

Article 118.

The Institute shall issue a decision to admit or reject the evidence, and if necessary, the evidence will be examined at a hearing, the place or media, date and time of which the parties shall be notified.

Submission of evidence

Article 119.

The following may be produced as evidence:

I. Public documents;

II. Private documents;

III. Inspection, provided it is conducted through a competent authority;

IV. Legal presumptions, in its double aspect, legal and human;

V. Experts;

VI. Witness testimony, and

VII. Photographs, websites, documents, and other items provided by science and technology.

In the case of expert evidence or witness testimony, it shall be necessary to specify the facts they will deal with and indicate the name and address of the expert or the witnesses, producing the list of questions or the interrogatories, respectively, to prepare the same. Without these, the evidence will be deemed as not offered.

Conciliation

Article 120.

After the request is admitted and without prejudice to the provisions of Article 54 of the Law, the Institute shall order conciliation between the parties according to the following procedure:

I. In the order admitting the request for protection of rights, the Institute shall require the parties to declare, by any means, their willingness to reconcile, within a period of ten days, calculated

from the date of notification of the order. The order shall contain a summary of the request for protection of personal data and the response of the data controller, if any, indicating the common elements and the points in dispute. The conciliation may be held in person, by remote or local electronic communication means, or by any other means as determined by the Institute. In any case, the conciliation shall be recorded using means that prove it took place. The conciliation stage is waived when the data subject is a minor and any of the rights contemplated in the Law for the Protection of the Rights of Children and Adolescents, related to the Law and these Regulations, were violated, unless the minor has duly accredited legal representation.

II. If the parties accept the possibility of reconciling, the Institute shall indicate the place or means, day and time for the conciliation hearing which shall take place within twenty days after the Institute receives the declaration of the willingness of the parties to reconcile, attempting to reconcile the interests of the data subject and the data controller. The conciliator may, at any time during the conciliation, require the parties to produce within a maximum period of five days, the evidence that they consider necessary for the conciliation. The conciliator may suspend the conciliation hearing when he deems it appropriate or at the request of both parties, up to two times. If the hearing is suspended, the conciliator shall state the day and time for its resumption. A record shall be made of any conciliation hearing, showing its result. If the data controller or the data subject or their respective representatives do not sign the record, this will not affect its validity, it being necessary to state the refusal.

III. If a party does not attend the conciliation hearing and justifies the absence within a period of five days, a second conciliation hearing will be called. If the party does not attend the latter hearing, the proceedings for the protection of rights will continue. If a party fails to attend a conciliation hearing without justification, the proceedings shall continue.

IV. In the absence of agreement in the conciliation hearing, the proceedings for the protection of rights will continue;

V. If reconciliation is achieved at the hearing, the agreement shall be put in writing and will be binding and shall state, if applicable, the period for it to be complied with, and

VI. Compliance with the agreement shall terminate the proceedings for the protection of rights; if not complied with, the Institute shall resume the proceedings.

The period referred to in Article 47 of the Law will be suspended during the period for compliance with the conciliation agreement.

The procedure established in this Article does not prevent the Institute, pursuant to Article 54 of the Law, from seeking conciliation at any time during the procedure for the protection of rights.

Hearing

Article 121.

For the purposes of the penultimate paragraph of Article 45 of the Law, the Institute shall determine, if applicable, the place or means, date and time for the hearing, which may be postponed only for justified cause. At the hearing, evidence which by its nature so requires, shall be submitted and a record of this made.

Presentation of Arguments

Article 122.

Once an order had been made recording that all evidence had been submitted, the file will be made available to the parties in order for them to formulate arguments, if they wish to do so, within a period of five days, calculated from the notification of the order referred to in this Article. At the end of this period, the proceedings shall be closed and the Institute shall issue its decision within the period established in Article 47 of the Law.

Interested Third Party

Article 123.

If no interested third party has been indicated, a third party may appear in the proceedings by filing a document proving his legal standing to intervene in the matter and may do so up to the closing of the proceedings. Such party must attach to his document the document proving his identity when he does not act in his own name and the documentary evidence offered by him.

Lack of Response

Article 124.

If the proceedings begin due to a failure of the data controller to respond to a request for the exercise of ARCO rights, the Institute shall send a copy to the data controller so that it may prove, as applicable, that it did respond the request, or in the absence thereof, issue a response and communicate this to the data subject with a copy to the Institute within a period of ten days from the notification.

If the data controller proves that it did respond the request for exercise of rights on time and in the proper form and had so notified the data subject or his representative, the proceedings for the protection of rights shall be dismissed for want of subject matter, in accordance with the provisions of Article 53 (IV) of the Law.

When the data controller proves that it did respond the request for exercise of rights on time and in the proper form and the request for the procedure for the protection of rights was not

filed by the data subject within the period established by Law and these Regulations, the proceedings for the protection of rights shall be dismissed for being filed out-of-time, in accordance with the provisions of Article 53 (III) of the Law, as related to Article 52 (V) of the Law.

If the response was issued by the data controller during the proceedings for the protection of rights or was issued outside the period established in Article 32 of the Law, the data controller shall notify the Institute and the data subject of the response so that within a period of fifteen days from notification, the latter may take the appropriate steps to continue the course of the proceedings. If the data subject declares his satisfaction with the response, the proceedings shall be discontinued for want of subject matter.

When the data controller does not comply with the requirement referred to in the first paragraph of this Article, the facts declared by the applicant shall be deemed true and a decision made based on the items found in the file. Decisions Article 125. The decisions of the Institute must be complied with within the time period and in the terms stated in them and may be used as the basis for other proceedings contemplated in the Law.

Challenging a Decision

Article 126.

Against a decision in the proceedings for the protection of rights, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Renewal of Proceedings

Article 127.

If the request for the protection of rights does not contain any of the causes for admissibility provided in Article 115 of these Regulations, but refers to the inspection proceedings contained in Chapter IX of these Regulations, the proceedings shall be referred to the competent department or agency, within a period of no more than ten days, calculated from the day on which the request was received.

Chapter IX

Inspections

Initiation

Article 128.

The Institute, in order to prove compliance with the provisions of the Law or the regulations arising from it, may begin an inspection proceeding, requiring the data controller to provide the necessary documentation or visiting the establishment where the databases are located.

Basis for Admissibility

Article 129.

Inspections may be initiated ex officio or at the request of a party, upon the instructions of the Plenum of the Institute.

Any person may file a complaint with the Institute about alleged violations of the provisions of the Law and other applicable laws and regulations, provided that they do not fall within the scope of the admissibility of a proceeding for the protection of rights. In this case, the Plenum will determine, upon proper grounds, the admissibility of beginning an inspection proceeding.

Certification

Article 130.

While carrying out an inspection, the personnel of the Institute shall have official authority to certify the accuracy of facts related to the transactions they are carrying out.

Requirements of the Complaint

Article 131.

The complaint must indicate the following:

I. Name and address of the complainant, or if applicable, the means of receiving notifications;

II. List of the facts on which the complaint is based, and if applicable, the evidence to prove the allegations, and

III. Name and address of the complainant, or if applicable, information on the complainant's location.

The complaint may be filed by the same means as is established for proceedings for the protection of rights.

When the complainant files his complaint by electronic means through the system established by the Institute, it will be understood that he accepts that notifications will be made to him by the same system or through other electronic means generated by this, unless he indicates a different means for notifications.

When the proceedings are carried out as a consequence of a complaint, the Institute shall acknowledge receipt of the complaint and may request the documentation it deems appropriate to carry out the proceedings.

Carrying Out the Inspection

Article 132.

The inspection proceedings will have a maximum duration of one hundred and eighty days, calculated from the day the Plenum issues the decision to begin and shall conclude with a decision. The Plenum of the Institute may extend this term once for up to an equal period.

The Institute may carry out various inspections to gather the necessary evidence which inspections shall not take longer than a maximum of ten days for each one. Notice of this period must be given to the data controller or data processor, and if applicable, to the complainant.

Inspections

Article 133.

The personnel of the Institute who carry out the inspections must have a legally proper written order bearing the handwritten signature of the competent official of the Institute, specifying the location of the establishment of the data controller or the location of the databases that are the subject of the inspection, the purpose and scope of the visit, and the provisions of the law upon which it is based.

Identification of Personnel

Article 134.

When starting the visit, the inspector must show a valid credential with photograph, issued by the Institute, which accredits him to carry out such function, as well as the legally proper written order referred to in the previous Article, a copy of which must be left with the person visited.

Minutes of Inspection

Article 135.

The inspection will conclude with the drawing up of the minutes of the inspection which shall indicate the steps taken during the inspection(s).

The minutes will be drawn up in the presence of two witnesses proposed by the person with whom the proceedings took place or by the inspector, if the former refuses to propose them. The minutes issued in duplicate shall be signed by the inspector and by the data controller, data

processor, or the person with whom the inspection took place, who may take such steps as are considered appropriate.

If the party inspected refuses to sign the minutes, this circumstance shall be expressly noted therein. The refusal shall not affect the validity of the proceedings or the minutes themselves. The signature of the party inspected will not be considered as agreement with the minutes, only as the receipt thereof.

The party inspected will be given one of the originals of the inspection minutes and the other will be incorporated in the file.

Contents of Minutes of Inspections

Article 136.

The inspection minutes shall state:

I. Name of the party inspected;

II. Time, day, month and year when the inspection began and ended;

III. Information clearly identifying the address, such as street, number, area [colonia], municipality or district [delegación], postal code, and state where the visit took place, as well as the telephone number or other form of communication available for the party inspected;

IV. Number and date of the order authorizing the inspection;

V. Name and title of the person with whom the inspection was conducted; VI. Name and address of the people who acted as witnesses;

VII. Information concerning the proceedings;

VIII. Declaration of the party inspected, if he wishes to give it, and

IX. Name and signature of those taking part in the inspection, including those of the inspectors. If the party inspected or his legal representative refuses to sign, this will not affect the validity of the minutes, although the inspector shall make a note thereof.

The parties inspected for whom the minutes of the inspection were drawn up may make observations in the minutes and take such steps with respect to the contents of the minutes as they consider legally appropriate or may do so in writing within a period of five days after the date of the minutes.

Decision

Article 137.

The inspection proceedings shall conclude with a decision issued by the Plenum of the Institute, establishing, if applicable, the measures to be adopted by the data controller within the period established therein.

The decision of the Plenum may begin the commencement of sanction proceedings or establish a period for them to begin, something which will be carried out pursuant to the provisions of the Law and these Regulations.

Notice of the decision of the Plenum shall be given to the party inspected and to the complainant, if any.

Challenging a Decision

Article 138.

Against the decision issued in the inspection proceedings, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Redirection of Proceedings

Article 139.

If the complaint filed does not refer to the proceedings mentioned in this Chapter, but instead to one of the bases for admissibility of proceedings for the protection of rights contained in Article 115 of these Regulations, the matter will be redirected to the appropriate administrative office, within a period not to exceed ten days, calculated from the day on which the request was received.

Chapter X
Procedure for Imposing Sanctions

Beginning

Article 140.

For the purposes of Article 61 of the Law, the Institute shall begin proceedings for imposing sanctions when, from proceedings for the protection of rights or from an inspection, presumed violations of the Law capable of being sanctioned under Article 64 of the Law have been seen. Once the proceedings for doing so have been completed, the appropriate decision will be issued.

The proceedings will begin by notification to the presumed violator at the address recorded with the Institute in the proceedings for the protection of rights or inspection.

The notification will be accompanied by a report describing the facts constituting the presumed violation, summoning the presumed violator to provide a response within a period of fifteen days, calculated from the day on which the notification takes effect, and offer the evidence it considers appropriate.

Offer and Submission of Evidence

Article 141.

The presumed violator shall make concrete statements in its response concerning each of the facts expressly imputed to him, affirming them, denying them, indicating that he has no knowledge of them because they are not his own or explaining how they occurred, as the case may be; and will submit arguments to deny the violation of which he is charged and the evidence thereof.

If expert or witness testimony evidence is offered, the facts to be dealt with must be specified and the names and addresses of the expert or witnesses must be stated, attaching the list of questions or interrogatories, respectively, needed to prepare the same. Without these indications, the evidence shall be deemed as not offered.

Admission and Rejection of Evidence

Article 142.

Concerning the offer of evidence by the presumed violator, a decision must be made admitting or rejecting the same, and evidence will then be submitted.

If necessary, the place, date and time will be established for the submission of evidence, which by its nature, requires this. A record of the hearing and submission of evidence shall be prepared.

Closing of the Proceedings and Decision

Article 143.

After the submission of evidence, if applicable, the presumed violator shall be notified that he has five days to submit arguments, calculated from the day on which the notification takes effect. At the end of this period, the proceedings will be closed and the decision of the Institute shall be issued within a period not exceeding fifty days from the beginning of the proceedings.

In justified cases, the Plenum of the Institute may extend once, for up to a period equal to the period of fifty days referred to in the previous paragraph.

Challenging a Decision

Article 144.

Against the decision in the proceedings for imposing sanctions, a nullity action may be filed with the Federal Tax and Administrative Justice Tribunal.

Transitional Provisions

First.

These Regulations enter into force the day after their publication in the Federal Official Gazette.

Second.

Any processing governed by the Law and these Regulations carried out after the date of the Law enters into force must be in compliance with the provisions of the same, regardless of the fact that the personal data may have been obtained or the database may have been made or created before the entry into force of the Law. It shall not be necessary to obtain the consent of the data subjects for personal data obtained prior to the entry into force of the Law, provided that it complies with the following paragraph.

Data controllers that have collected personal data before the entry of the Law into force and that continue processing the same shall make a privacy notice available to the data subjects or, as the case may be, use any of the compensatory measures, as required, in accordance with the provisions of Article 18 of the Law and Articles 32, 33, 34, and 35 of these Regulations.

A data subject may exercise his ARCO rights with respect to the processing of which he is informed in the privacy notice or the corresponding compensatory measure.

Third.

The general guidelines for the use of compensatory measures to which Article 32 of these Regulations refer shall be published by the Institute no later than three months after the date these Regulations enter into force.

Fourth.

Data controllers shall comply with the provisions of Chapter III of these Regulations no later than eighteen months after the same enters into force.

Fifth.

The Ministry, in cooperation with the Institute, shall issue the parameters to which Articles 82, 83, 84, 85, and 86 of these Regulations refer within six months of their entry into force.

Given at the Office of the President, Mexico City, Federal District, on the 19th day of December, 2011. Filipe de Jesus Calderon Hinojasa. Initials. The Secretary of the Economy, Bruno Francisco Ferrari Garcia de Alba. Initials

ภาคผนวก ฉ
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเกาหลีใต้ (Act on the Development of Cloud Computing and Protection of its users)

ACT ON THE DEVELOPMENT OF CLOUD COMPUTING AND PROTECTION OF ITS USERS

Act No. 13234, Mar. 27, 2015

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to contribute to improvement of citizens' live and the development of the national economy by promoting the development and use of cloud computing and by creating an environment for safe use of cloud computing services.

Article 2 (Definitions)

The terms used in this Act shall be defined as follows:

1. The term "cloud computing" means an information processing system that makes it possible to flexibly use integrated and shared resources for information and communications (hereinafter referred to as "resources for information and communications"), such as devices for information and communications, information and communications systems, and software, through information and communications networks in accordance with changes in users' requirements or demands;
2. The term "cloud computing technologies" means information and communications technologies specified by Presidential Decree as those for the establishment and use of cloud computing, including technologies for virtualization and distributed processing;
3. The term "cloud computing services" means the services specified by Presidential Decree as commercial services of providing resources for information and communications to others by utilizing cloud computing;
4. The term "user information" means the information (referring to the information prescribed in subparagraph 1 of Article 3 of the Framework Act on National Informatization) stored by a user of cloud computing services (hereinafter referred to as "user") in the resources for information and communications of the person who provides the cloud computing services through a cloud computing system (hereinafter referred to as "cloud computing service provider") and owned or managed by the user.

Article 3 (Responsibilities of State, etc.)

(1) The State and local governments shall formulate policies necessary for promoting the development and use of cloud computing and for creating an environment for safe use of cloud computing services.

(2) Cloud computing service providers shall endeavor to protect user information and provide reliable cloud computing services.

(3) Users shall not engage in any activity compromising the safety of cloud computing services.

Article 4 (Relationship to Other Acts)

This Act shall take precedence over other Acts with regard to promoting development and use of cloud computing and the protection of users: Provided, That, with regard to the protection of personal information, the provisions of the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and other relevant Acts shall apply.

CHAPTER II CREATION OF BASIS FOR DEVELOPMENT OF CLOUD COMPUTING

Article 5 (Formulation of Master Plans and Implementation Plans)

(1) The Minister of Science, ICT and Future Planning shall collect plans, policies, etc. formulated by central administrative agencies related to the promotion of development and use of cloud computing and the protection of users (hereinafter referred to "relevant central administrative agencies"), formulate a master plan every three years (hereinafter referred to as "master plan"), and finalize the plan after deliberation by the Information Communications Strategy Committee under Article 7 of the Special Act on the Promotion of Information and Communications, the Invigoration of Convergence, etc.

(2) Each master plan shall contain the following matters:

1. The basic direction-setting for policies for the promotion of development and use of cloud computing and the protection of users;
2. Matters concerning the creation of a basis for promoting the cloud computing industry and the use of cloud computing;
3. Matters concerning the introduction of cloud computing and the promotion of use;
4. Matters concerning the facilitation of research and development of cloud computing technologies;
5. Matters concerning the training of human resources specializing in cloud computing;
6. Matters concerning promoting the international cooperation and the development of overseas markets for cloud computing;
7. Matters concerning protecting information of users of cloud computing services;
8. Matters concerning improving the statutes and systems related to cloud computing;
9. Matters concerning the facilitation of convergence of technologies and industries related to cloud computing;
10. Other necessary matters concerning the development of cloud computing technologies and cloud computing services.

(3) The head of the relevant central administrative agency shall formulate and execute an implementation plan for the affairs under his/her jurisdiction (hereinafter referred to as "implementation plan") in accordance with the master plan.

(4) The head of the relevant central administrative agency shall submit an implementation plan for next year and a report on the results of execution of the implementation plan for the preceding year to the Minister of Science, ICT and Future Planning, as prescribed by Presidential Decree, and the Minister of Science, ICT and Future Planning shall evaluate the results of execution of the implementation plan for each year.

(5) Except as otherwise expressly provided for in paragraphs (1) through (4), matters necessary for the formulation and execution of master plans and implementation plans and the submission and evaluation of reports on the results of execution shall be prescribed by Presidential Decree.

Article 6 (Cooperation from Relevant Agencies)

(1) The Minister of Science, ICT and Future Planning or the head of the relevant central administrative agency may request the head of a State agency, local government, or public agency defined by subparagraph 3 of Article 2 of the Electronic Government Act (hereinafter referred to as "State agency or other public authority") to cooperate with him/her as necessary for the formulation and implementation of master plans or implementation plans.

(2) Each person in receipt of the request under paragraph (1) shall comply with the request, in the absence of good cause to the contrary.

Article 7 (Fact-Finding Survey)

(1) The Minister of Science, ICT and Future Planning may conduct fact-finding surveys in order to secure information and statistics about the current situation of industries as necessary for the effective formulation and implementation of policies on cloud computing.

(2) Where the Minister of Science, ICT and Future Planning deems it necessary for the fact-finding surveys under paragraph (1), he/she may request a cloud computing service provider or any other related institution or organization to submit data or express opinions.

(3) Upon receipt of a request from the head of the relevant central administrative agency, the Minister of Science, ICT and Future Planning shall notify him/her of the results of fact-finding surveys.

(4) Necessary matters concerning the fact-finding surveys under paragraphs (1) through (3) shall be prescribed by Presidential Decree.

Article 8 (Research and Development)

(1) The head of the relevant central administrative agency may implement a research and development project for cloud computing technologies and cloud computing services.

(2) The head of the relevant central administrative agency may outsource an enterprise or research institute to perform a research and development project under paragraph (1) and may fully or partially subsidize it for expenses incurred in the performance of the project.

Article 9 (Pilot Projects)

(1) The head of the relevant central administrative agency may implement a pilot project to promote the use and diffusion of cloud computing technologies and cloud computing services and may request local governments to cooperate with him/her in implementing the pilot project.

(2) The head of the relevant central administrative agency may provide financial assistance to the persons who participate in a pilot project under paragraph (1).

Article 10 (Assistance by Taxation)

The State and local governments may take necessary measures, such as full or partial exemption of taxes, as provided for in the Restriction of Special Taxation Act, the Restriction of Special Local Taxation Act, and other Tax-related Acts, in order to promote the development and use of cloud computing technologies and cloud computing services.

Article 11 (Assistance to Small and Medium Enterprises)

(1) The Government may provide assistance to small and medium enterprises (referring to the small and medium enterprises defined in Article 2 of the Framework Act on Small and Medium Enterprises; hereinafter the same shall apply) engaging in cloud computing as follows in order to promote the development and use of cloud computing and to protect users:

1. Provision of information about cloud computing services and consulting thereon;

2. Provision of technologies and subsidization of expenses as necessary for protecting user information;

3. Training of human resources specializing in cloud computing;

4. Assistance in other matters necessary for fostering small and medium enterprises engaging in cloud computing.

(2) Where the head of a relevant central administrative agency implements a research and development project under Article 8, he/she shall prepare measures to promote participation by small and medium enterprises engaging in cloud computing.

(3) Necessary matters concerning the entities eligible for assistance, the method for providing assistance, etc. under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Article 12 (Facilitation of Introduction of Cloud Computing to State Agencies and Other Public Authorities)

(1) The State agencies and other public authorities shall endeavor to introduce cloud computing.

(2) Where the Government formulates a budget necessary for the implementation of a policy or project for national informatization under the Framework Act on National Informatization, it shall give preference to the introduction of cloud computing.

Article 13 (Forecast on Demand for Cloud Computing Projects)

(1) The head of each State agency or other public authority shall submit a forecast on the demand for cloud computing projects from affiliated agencies to the Minister of Science, ICT and Future Planning, at least annually.

(2) The Minister of Science, ICT and Future Planning shall disclose the forecasts received on the demand for cloud computing under paragraph (1) to cloud computing service providers, at least annually.

(3) Necessary matters concerning the frequency, timing, method, procedure, etc. for the submission and disclosure of forecasts under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Article 14 (Training of Specialized Human Resources)

(1) The Minister of Science, ICT and Future Planning may formulate and implement policies necessary for training human resources specializing in cloud computing.

(2) The Minister of Science, ICT and Future Planning may designate the institutions that meet the requirements prescribed by Presidential Decree, from among educational institutions that conduct educational and training courses related to cloud computing, and may fully or partially subsidize such institutions for expenses incurred in engaging in such courses.

(3) In any of the following cases, the Minister of Science, ICT and Future Planning may revoke the designation of an educational institution designated under paragraph (2): Provided, That the designation shall be revoked in cases of subparagraph 1:

1. Where an educational institution has obtained the designation by fraud or other wrongful means;

2. Where an educational institution ceases to meet any of the requirements for designation under paragraph (2);

3. Where an educational institution has no record of providing education for at least one year from the date of designation of the educational institution.

(4) Necessary matters concerning the formulation of policies, the requirements for designating educational institutions, the procedure for designation and revocation of designation, the scope of assistance, etc. shall be prescribed by Presidential Decree.

Article 15 (Facilitation of International Cooperation and Development of Overseas Markets)

In order to facilitate international cooperation in cloud computing and the development of overseas markets for cloud computing technologies and cloud computing services, the Government may conduct the following activities:

1. International exchange of information, technologies, and human resources in relation to cloud computing;

2. Advertising and overseas marketing, including exhibitions related to cloud computing;

3. Joint research and development of cloud computing with other countries;

4. Collection, analysis, and provision of information for the development of overseas markets for cloud computing;

5. Mutual assistance with other countries to ensure effective international cooperation in cloud computing;

6. Other activities necessary to facilitate international cooperation in cloud computing and the development of overseas markets.

Article 16 (Assistance in Establishment of Integrated Information and Communications Facilities Based on Cloud Computing Technologies)

(1) In order to promote the development and use of cloud computing, the State and local governments may provide administrative, financial, technical assistance to persons who intend to establish information and communications facilities integrated by using cloud computing technologies.

(2) Necessary matters concerning the persons eligible for the assistance under paragraph (1), the method and procedure for such assistance, etc. shall be prescribed by Presidential Decree.

Article 17 (Creation of Industrial Complexes)

(1) The State and local governments may create industrial complexes to promote the cloud computing industry and facilitate the utilization of cloud computing through research and development of technologies for the cloud computing industry and training of specialized human resources.

(2) The industrial complexes shall be created in accordance with the procedure for the designation and development of national industrial complexes, general industrial complexes, and urban hi-tech industrial complexes under the Industrial Sites and Development Act.

(3) Where the Minister of Science, ICT and Future Planning deems it necessary for facilitating the creation of industrial complexes, he/she may request the Minister of Land, Infrastructure and Transport to designate them as industrial complexes.

Article 18 (Creation of Environment for Fair Competition, etc.)

(1) The Government shall create an environment for fair competition between large enterprises (referring to enterprises that do not fall into the category of either small and medium enterprises under Article 2 of the Framework Act on Small and Medium Enterprises or middle-standing enterprises under subparagraph 1 of Article 2 of the Special Act on the Promotion of Growth and the Strengthening of Competitiveness of Middle-Standing Enterprises) that provide cloud computing services and small and medium enterprises that also provide cloud computing services.

(2) No large enterprise that provides cloud computing services shall compel a small or medium enterprise that also provides cloud computing services to sign an unfair contract nor shall obtain unjust benefits, without any reasonable cause, taking advantage of its position.

(3) In order to create an environment for fair competition in the cloud computing industry, the Government may analyze and evaluate the current conditions of the environment for competitions in the cloud computing industry and may implement other programs necessary for creating an environment for fair distribution.

Article 19 (Designation of Exclusively Responsible Institution, etc.)

(1) Where the Minister of Science, ICT and Future Planning deems it necessary for promoting the cloud computing industry and facilitating the use of cloud computing, he/she may designate an exclusively responsible institution.

(2) The Minister of Science, ICT and Future Planning may fully or partially subsidize an exclusively responsible institution for expenses incurred in performing its business activities.

(3) Necessary matters concerning the designation, operation, etc, of an exclusively responsible institution shall be prescribed by Presidential Decree.

CHAPTER III FACILITATING USE OF CLOUD COMPUTING SERVICES

Article 20 (Facilitating Public Institutions' Use of Cloud Computing Services)

The Government shall endeavor to encourage public institutions to use cloud computing services provided by cloud computing service providers for their work process.

Article 21 (Required Electronic Computer Systems, etc.)

Where electronic computer systems, equipment, facilities, etc. (hereinafter referred to as "electronic computer systems") are expressly provided for in any other statute as requirements for authorization, permission, registration, designation, or any similar action, relevant electronic computer systems shall be deemed to include cloud computing services: Provided, That the foregoing shall not apply to any of the following cases:

1. Where the relevant statute expressly prohibits the use of cloud computing services;

2. Where the relevant statute requires the building of physical partitions between lines or facilities and actually restrict the use of cloud computing services;

3. Where cloud computing services are used but do not meet the requirements for electronic computer systems required by the relevant statute.

Article 22 (Securing of Interoperability)

Where the Minister of Science, ICT and Future Planning deems it necessary for securing the interoperability of cloud computing services, he/she may recommend cloud computing service providers to establish a cooperation system.

CHAPTER IV ENHANCEMENT OF RELIABILITY OF CLOUD COMPUTING SERVICES AND PROTECTION OF USERS

Article 23 (Enhancement of Reliability)

(1) Cloud computing service providers shall endeavor to enhance the quality and performance of cloud computing services and the level of protection of information.

(2) The Minister of Science, ICT and Future Planning shall determine and publicly notify the standards for the quality and performance of cloud computing services and the standards for the protection of information (including managerial, physical, technical measures for protection) and may recommend cloud computing service providers to observe the standards.

(3) Where the Minister of Science, ICT and Future Planning intends to publicly notify the standards for the quality and performance of cloud computing services under paragraph (2), he/she shall seek opinions from the Korea Communications Commission thereon.

Article 24 (Standard Agreement Forms)

(1) In order to protect users and establish public order for fair transactions, the Minister of Science, ICT and Future Planning may formulate or amend standard agreement forms related to cloud computing services, subject to consultation with the Fair Trade Commission, and may recommend that cloud computing service providers use such forms. In such cases, the Minister of Science, ICT and Future Planning may seek opinions of cloud computing service providers, users, and others.

(2) Where the Minister of Science, ICT and Future Planning intends to formulate or amend standard agreement forms pursuant to paragraph (1), he/she shall seek the opinion of the Korea Communications Commission thereon.

Article 25 (Notification, etc. of Intrusions, etc.)

(1) In any of the following cases, the cloud computing service provider shall notify the relevant user of the fact promptly:

1. Where an intrusion defined by subparagraph 7 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as "intrusion") occurs;

2. Where the relevant user information is leaked;

3. Where services are interrupted for a period at least the period specified by Presidential Decree (referring to the period stipulated by an agreement between the parties, if such agreement has been made) without prior notice.

(2) In case falling under paragraph (1) 2, the cloud computing service provider shall notify the Minister of Science, ICT and Future Planning of the fact immediately.

(3) Where the Minister of Science, ICT and Future Planning receives the notice under paragraph (2) or becomes aware of such fact, he/she may take measures necessary for preventing worsening of damage, preventing reoccurrence, and restoring damaged systems,

(4) Necessary matters concerning the notification and measures under paragraphs (1) through (3) shall be prescribed by Presidential Decree.

Article 26 (Disclosure of Information for Protection of Users, etc.)

(1) Any user may request a cloud computing service provider to inform him/her of the name of the country where the relevant user information is stored.

(2) Any person who uses information and communications services (referring to the information and communications services defined by subparagraph 2 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.; hereinafter the same shall apply in paragraph (3)) may request an information and communications service provider (referring to the information and communications service provider defined by subparagraph 3 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.; hereinafter the same shall apply in paragraph (3)) to inform him/her as to whether it uses cloud computing services and the name of the country where the relevant user information is stored.

(3) Where the Minister of Science, ICT and Future Planning deems it necessary for protecting users or the users of information and communications services, he/she may recommend that cloud computing service providers or information and communications service providers disclose the information referred to in paragraph (1) or (2).

(4) Where the Minister of Science, ICT and Future Planning intends to recommend the disclosure of information pursuant to paragraph (3), he/she shall seek opinions from the Korea Communications Commission thereon.

Article 27 (Protection of User Information)

(1) No cloud computing service provider shall provide user any information to a third party or use user information for any purpose other than for the purpose of providing services, without the relevant user's consent, unless it is required by a court order to submit or a warrant issued by a judge. The foregoing shall also apply to a third party to whom a cloud computing service provider has provided user information.

(2) Where a cloud computing service provider intends to provide any user information to a third party or to use the user information for any purpose other than for the purpose of providing services, it shall notify the user of the following matters and shall obtain consent thereto. The same shall apply where a change occurs to any of the following matters:

1. The person to whom the user information is to be provided;

2. The purpose of use of the user information (referring to the purpose of use of the person to whom the information is provided, if it is provided);

3. A list of user information used or provided;

4. The period of holding and use of user information (referring to the period of possession and user information by the person to whom user information is provided, where such information is provided);

5. A statement that the user has a right to refuse to give consent and the details of disadvantages in such cases, if disadvantages are given against refusal to give consent.

(3) Where the contract made with a user terminates, the cloud computing service provider shall return the user information to the user and destroy the user information possessed by the cloud computing service provider: Provided, That the user information shall be destroyed, if it is actually impossible to return the user information, because the user does not accept the return of the user information or does not want to have the user information returned.

(4) Where a cloud computing service provider intends to close its business, it shall notify each user of the closure of business, return the user information before the date of closure of business, and destroy the user information possessed by the cloud computing service provider: Provided, That the user information shall be destroyed, if it is actually impossible to return the user information, because the user does not accept the return of the user information or does not wish to have the user information returned.

(5) Notwithstanding paragraphs (3) and (4), if a cloud computing service provider has expressly agreed on different conditions with users, such conditions shall apply.

(6) Matters concerning the methods and timing for the return and destruction of user information and the methods of notifying the termination of a contract or the closure of business shall be prescribed by Presidential Decree.

Article 28 (Deposit of User Information)

(1) A cloud computing service provider and users may deposit user information in an institution equipped with professional personnel and facilities (hereinafter referred to as "depository") under an agreement entered into with the depository.

(2) Where an event specified in the agreement made under paragraph (1) occurs, a user may request the depository to provide user information.

Article 29 (Liability for Damages)

Where a user sustains an injury or loss caused by a cloud computing service provider's violation of any provision of this Act, he/she may claim damages for such injury or loss against the cloud computing service provider. In such cases, the cloud computing service provider shall not be

exempted from liability, unless it proves that such injury or loss has not been caused by its intentional conduct or negligence.

CHAPTER V SUPPLEMENTARY PROVISIONS

Article 30 (Fact-Finding Investigation and Corrective Measures)

(1) Where the Minister of Science, ICT and Future Planning has a reasonable ground to suspect that a cloud computing service provider has violated any provision of this Act, he/she may instruct public officials of the Ministry to conduct investigations as necessary to ascertain the violation.

(2) Where the Minister of Science, ICT and Future Planning deems it necessary for the investigation under paragraph (1), he/she may authorize public officials of the Ministry to enter the office or place of business of a cloud computing service provider to inspect books of accounts, documents, and other materials or articles.

(3) Where the Minister of Science, ICT and Future Planning intends to conduct an investigation under paragraph (1), he/she shall notify the relevant cloud computing service provider of the plan for investigation, including the period and scope of investigation, the grounds for the investigation, etc., by not later than seven days before the scheduled date of investigation: Provided, That the foregoing shall not apply to an emergency case or where it is deemed impossible to achieve the objectives of investigation if prior notice is given, because of destruction of evidence, etc.

(4) Any person who enters the office or place of business of a cloud computing service provider to conduct an investigation shall show a certificate of authority to persons involved and shall have the persons in the office or place of business attend at the scene of the investigation.

(5) The Minister of Science, ICT and Future Planning may order a cloud computing service provider who violates Article 25 (1) or 27 to cease the violation or to take corrective measures.

Article 31 (Delegation and Entrustment)

(1) The authority of the Minister of Science, ICT and Future Planning or the head of the relevant central administrative agency under this Act may be partially delegated to the heads of affiliated agencies, as prescribed by Presidential Decree.

(2) The affairs assigned to the Minister of Science, ICT and Future Planning or the head of the relevant central administrative agency under this Act may be partially entrusted to a specialized institution, as prescribed by Presidential Decree.

Article 32 (Duty of Confidentiality)

Any person who currently or formerly engaged in an affair entrusted under this Act shall not divulge a cloud computing service provider's confidential information on business which becomes known to him/her in the course of executing the affair.

Article 33 (Legal Fiction of Deeming Public Officials for Application of Penalty Provisions)

Executive officers and employees of a specialized institution engaging in the affairs entrusted pursuant to Article 31 (2) shall be deemed public officials for the purpose of applying penalty provisions of Articles 129 through 132 of the Criminal Act to them.

CHAPTER VI PENALTY PROVISIONS

Article 34 (Penalty Provisions)

Any person who uses user information or provides user information to a third party, without the relevant user's consent, or any person who obtains user information for profit or for any wrongful purpose, knowing that the relevant user has not consented thereto, in violation of Article 27 (1), shall be punished by imprisonment for not more than five years or by a fine not exceeding 50 million won.

Article 35 (Penalty Provisions)

Any person who divulges confidential information which becomes known to him/her in the course of executing an affair entrusted, in violation of Article 32, shall be punished by imprisonment for not more than three years or by a fine not exceeding 30 million won.

Article 36 (Joint Penalty Provisions)

Where the representative of a corporation or an agent, employee, or servant who works for a corporation or for an individual commits an offense in violation of Article 34 or 35 in connection with the business of the corporation or individual, not only shall such offender be punished accordingly, but the corporation or individual also shall be punished by the fine prescribed in the relevant Article: Provided, That the foregoing shall not apply where the corporation or individual has not neglected due care and supervision over the relevant business to prevent such offense.

Article 37 (Administrative Fines)

Any of the following persons shall be punished by an administrative fine not exceeding ten million won:

1. A person who fails to notify users of an intrusion, the leakage of user information, or the interruption of service, in violation of Article 25 (1);

2. A person who fails to notify the Minister of Science, ICT and Future Planning of the leakage of user information, in violation of Article 25 (2);

3. A person who fails to return or destroy user information, in violation of Article 27 (3) or (4);

4. A person who fails to comply with an order issued under Article 30 (5) to cease a violation or to take corrective measures.

(2) The administrative fines under paragraph (1) shall be imposed and collected by the Minister of Science, ICT and Future Planning, as prescribed by Presidential Decree.

ADDENDUM

This Act shall enter into force six months after the date of its promulgation.

ภาคผนวก ช

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ฉบับคณะรัฐมนตรีอนุมัติหลักการ)

บันทึกหลักการและเหตุผล
ประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ....

หลักการ

ให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เหตุผล

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือนร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป ดังนั้น จึงสมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

ร่าง

พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ....

.....

.....

.....

.....

.....

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา 26 ประกอบกับมาตรา 32 มาตรา 33 และมาตรา 37 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิเสรีภาพของบุคคลตามพระราชบัญญัตินี้เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

.....

.....

มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่บทบัญญัติในหมวด 1 บทบัญญัติในหมวด 4 และมาตรา 77 มาตรา 78 มาตรา 79 มาตรา 80 มาตรา 81 มาตรา 82 และมาตรา 83 ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใดกิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลและบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(2) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลแต่ไม่เพียงพอเท่ากับอำนาจของ

คณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคล ผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาพผู้แทนราษฎร วุฒิสภาพ รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(5) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

มาตรา 5 พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าผู้นั้นจะอยู่ในหรือนอกราชอาณาจักรก็ตาม

การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่กระทำนอกราชอาณาจักรแม้แต่ส่วนหนึ่งส่วนใดของการกระทำได้กระทำในราชอาณาจักร หรือกระทำนอกราชอาณาจักรที่ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักรหรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นนั้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักร ให้ถือว่าเป็นการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้กระทำในราชอาณาจักร

มาตรา 6 ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าของข้อมูลส่วนบุคคล” ให้หมายความรวมถึง

(1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ

(3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

“บุคคล” หมายความว่า บุคคลธรรมดา

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“เลขาธิการ” หมายความว่า เลขาธิการสำนักงานคณะกรรมการการคุ้มครองข้อมูลส่วนบุคคล

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา 7 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้ใช้บังคับได้

หมวด 1
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 8 ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(1) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ

(3) กรรมการโดยตำแหน่ง จำนวนแปดคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา อัยการสูงสุด เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้แทนสภาหอการค้าแห่งประเทศไทย ผู้แทนสภาอุตสาหกรรมแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

(4) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา 10 ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

มาตรา 9 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(1) มีสัญชาติไทย

(2) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(3) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(4) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา 10 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา 11 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 10 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 9

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระให้รองประธานกรรมการทำหน้าที่เป็นประธานกรรมการเป็นการชั่วคราว

มาตรา 12 การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้รองประธานกรรมการทำหน้าที่เป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด

มาตรา 13 กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณา ให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา 14 คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้

(1) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติตามนโยบายและแผนระดับชาติดังกล่าว

(2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมการแผนยุทธศาสตร์ตาม (1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าวเพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

(3) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(4) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

(6) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ

(7) พิจารณากำหนดค่าปรับทางปกครองตามมาตรา 69 มาตรา 70 มาตรา 71 มาตรา 72 มาตรา 73 มาตรา 74 และมาตรา 75 รวมทั้งฟ้องคดีต่อศาลปกครอง ทั้งนี้ ในกรณีที่มีการบังคับทางปกครองเพื่อชำระค่าปรับทางปกครอง ให้คณะกรรมการเป็นผู้มีอำนาจออกคำสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินในการบังคับทางปกครองและให้ประธานกรรมการเป็นผู้ลงนามแทนในคำสั่งดังกล่าว

(8) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(9) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้

(10) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(11) ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัตินี้

(12) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(13) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(14) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ

มาตรา 15 ให้กรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

อนุกรรมการและกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา 16 คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการให้นำความในมาตรา 12 มาใช้บังคับโดยอนุโลม

หมวด 2
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 1
บททั่วไป

มาตรา 17 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

มาตรา 18 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ส่วนที่ 2
การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา 19 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 20 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้

(1) วัตถุประสงค์ของการเก็บรวบรวม

(2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ

(5) สิทธิของเจ้าของข้อมูลตามมาตรา 26 มาตรา 27 และมาตรา 28

กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

มาตรา 21 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(5) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

(6) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล

(7) เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

(8) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา 22 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตาม มาตรา 24

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

มาตรา 23 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) ได้รับยกเว้นตามมาตรา 21 (2) หรือ (7)

(2) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ส่วนที่ 3

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 21 หรือมาตรา 23 หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา 22(3) แล้วแต่กรณี

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่งจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา 31

มาตรา 25 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 14 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(5) กรณีอื่นตามที่กำหนดในกฎกระทรวง

หมวด 3

สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา 26 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้

(1) เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล

(2) มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย

(3) การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น

(4) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 31

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ทั้งนี้ คณะกรรมการจะประกาศกำหนดระยะเวลาในการดำเนินการตามคำขอให้เร็วขึ้นหรือขยายระยะเวลาดังกล่าวหรือกำหนดหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

มาตรา 27 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา 28 ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามวรรคหนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามวรรคหนึ่งไว้ในรายการตามมาตรา 31

มาตรา 29 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ

(2) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(4) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 27 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(5) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

มาตรา 30 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด

มาตรา 31 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้และการเปิดเผยตามมาตรา 24 วรรคสาม

(7) การปฏิเสธคำขอตามมาตรา 26 วรรคสาม และมาตรา 28 วรรคสอง

หมวด 4
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 32 ให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

สำนักงานเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยแรงงานรัฐวิสาหกิจสัมพันธ์ กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

ให้สำนักงานเป็นหน่วยงานของรัฐตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่

มาตรา 33 นอกจากดำเนินการให้เป็นไปตามวัตถุประสงค์ตามมาตรา 32 วรรคหนึ่ง ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

(1) จัดทำร่างแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการ

(2) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(3) วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(4) สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคลและแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการ

(5) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(6) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(7) เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานภาครัฐ หน่วยงานเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

(8) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(9) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามอำนาจหน้าที่ของสานักงาน

(10) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(11) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

มาตรา 34 ในการดำเนินงานของสำนักงาน นอกจากอำนาจหน้าที่ตามที่บัญญัติในมาตรา 33 แล้ว ให้สำนักงานมีอำนาจหน้าที่ทั่วไป ดังต่อไปนี้ด้วย

(1) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิต่าง ๆ

(2) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน

(3) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน

(4) ถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นในกิจการที่เกี่ยวกับวัตถุประสงค์ของสำนักงาน

(5) กู้ยืมเงินเพื่อประโยชน์ในการดำเนินการตามวัตถุประสงค์ของสำนักงาน

(6) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(7) ดำเนินการอื่นใดที่จำเป็นหรือต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของสำนักงาน

(8) ปฏิบัติการใด ๆ ให้เป็นไปตามพระราชบัญญัตินี้ หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือคณะกรรมการมอบหมาย

การถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นตาม (4) และการกู้ยืมเงินตาม (5) ให้เป็นไปตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา 35 ทุนและทรัพย์สินในการดำเนินงานของสำนักงานประกอบด้วย

(1) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา 80

(2) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(3) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้จากการดำเนินงาน

(4) เงินอุดหนุนจากภาคเอกชนหรือองค์กรอื่น รวมทั้งจากต่างประเทศหรือองค์การระหว่างประเทศ และเงินหรือทรัพย์สินที่มีผู้อุทิศให้

(5) ดอกผลและผลประโยชน์หรือรายได้อื่นใดที่เกิดจากการดำเนินงานของสำนักงาน

ทรัพย์สินของสำนักงานไม่อยู่ในความรับผิดแห่งการบังคับคดีและมาตรการบังคับทางปกครอง

เงินและทรัพย์สินของสำนักงานไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน ยกเว้นดอกผล และผลประโยชน์หรือรายได้อื่นตามวรรคหนึ่ง (5) เมื่อใช้จ่ายตามอำนาจหน้าที่ของสำนักงานแล้ว ที่เหลือให้นำส่งคลังเป็นรายได้แผ่นดิน

มาตรา 36 ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ประธานกรรมการซึ่งรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติเป็นกรรมการ และกรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งจำนวนหกคน

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานเป็นผู้ช่วยเลขานุการได้ตามความจำเป็นแต่ไม่เกินสองคน

กรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งตามวรรคหนึ่ง ต้องมีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยสามคน และด้านอื่นที่เกี่ยวข้องอันเป็นประโยชน์ต่อการดำเนินงานของสำนักงาน

ให้นำบทบัญญัติมาตรา 9 และมาตรา 11 มาใช้บังคับกับประธานกรรมการและกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา 37 ให้ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวาระการดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง ให้ดำเนินการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ภายในหกสิบวัน ในระหว่างที่ยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา 38 ในกรณีที่ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ พ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนและในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้ดำเนินการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิแทนตำแหน่งที่ว่างภายในหกสิบวันนับแต่วันที่ตำแหน่งว่างลง และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน เว้นแต่วาระของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิเหลือไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

มาตรา 39 การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

ในการวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้ามีคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

กรรมการที่มีส่วนได้เสียในเรื่องที่มีการพิจารณาจะเข้าร่วมประชุมมิได้

การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจกระทำโดยวิธีการทางอิเล็กทรอนิกส์ตามที่คณะกรรมการกำหนดก็ได้

มาตรา 40 คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีอำนาจและหน้าที่ดังต่อไปนี้

(1) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(2) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

(3) อนุมัติแผนการดำเนินงาน แผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(4) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(5) แต่งตั้งคณะกรรมการสรรหาเลขาธิการ

(6) วินิจฉัยอุทธรณ์คำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(7) ประเมินผลการดำเนินการของสำนักงาน และการปฏิบัติงานของเลขาธิการ

(8) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการกำกับสำนักงานคุ้มครองข้อมูลส่วนหรือตามที่คณะรัฐมนตรีมอบหมาย

ข้อบังคับตาม (2) ถ้ามีการจำกัดอำนาจเลขาธิการในการทำนิติกรรมกับบุคคลภายนอกให้ประกาศในราชกิจจานุเบกษา

มาตรา 41 คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจแต่งตั้งคณะอนุกรรมการ เพื่อปฏิบัติหน้าที่หรือกระทำการอย่างหนึ่งอย่างใดตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมอบหมายได้

คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจแต่งตั้งบุคคลซึ่งมีความเชี่ยวชาญหรือประสบการณ์ที่จะเป็นประโยชน์ในการปฏิบัติหน้าที่ของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้

การปฏิบัติหน้าที่และจำนวนของคณะอนุกรรมการตามวรรคหนึ่งหรือบุคคลตามวรรคสอง ให้เป็นไปตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ให้นำมาตรา 39 มาใช้บังคับแก่คณะอนุกรรมการโดยอนุโลม

มาตรา 42 ให้ประธานกรรมการและกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประธานอนุกรรมการและ

อนุกรรมการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง ได้รับเบี้ยประชุมหรือค่าตอบแทนตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา 43 ให้สำนักงานมีเลขาธิการคนหนึ่งซึ่งคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง มีหน้าที่บริหารกิจการของสำนักงาน

การแต่งตั้งเลขาธิการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์และวิธีการสรรหาตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 44 ผู้ที่จะได้รับการแต่งตั้งเป็นเลขาธิการต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(1) มีสัญชาติไทย

(2) อายุไม่เกินห้าสิบห้าปีบริบูรณ์

(3) สามารถทำงานให้แก่สำนักงานได้เต็มเวลา

(4) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงาน และการบริหารจัดการ

(5) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(6) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(7) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(8) ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจ หรือจากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(9) ไม่เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(10) ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่พรรคการเมือง

(11) ไม่เป็นผู้มีส่วนได้เสียในกิจการที่เกี่ยวข้องกับสำนักงานไม่ว่าโดยทางตรงหรือทางอ้อม

มาตรา 45 เลขาธิการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระติดต่อกันไม่ได้

ก่อนครบกำหนดตามวาระการดำรงตำแหน่งของเลขาธิการเป็นเวลาไม่น้อยกว่าสามสิบวันแต่ไม่เกินหกสิบวัน หรือภายในสามสิบวันนับแต่วันที่เลขาธิการพ้นจากตำแหน่งก่อนครบวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งคณะกรรมการเพื่อสรรหาเลขาธิการคนใหม่ ทั้งนี้ ให้คณะกรรมการสรรหาเสนอรายชื่อบุคคลที่เหมาะสมไม่เกินสามคนต่อคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 46 ในแต่ละปีให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 47 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 45 เลขาธิการพ้นจากตำแหน่ง เมื่อ

(1) ตาย

(2) ลาออก

(3) อายุครบหกสิบปีบริบูรณ์

(4) คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน มีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(6) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 44

มาตรา 48 ให้เลขาธิการมีอำนาจหน้าที่ ดังต่อไปนี้

(1) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนระดับชาติ แผนยุทธศาสตร์ นโยบายของคณะรัฐมนตรี คณะกรรมการ และคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และระเบียบข้อบังคับหรือมติของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2) วางระเบียบเกี่ยวกับการดำเนินงานของสำนักงานโดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศที่คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(3) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามระเบียบหรือข้อบังคับของสำนักงาน

(4) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(5) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงาน และลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามระเบียบหรือข้อบังคับที่คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(6) ปฏิบัติการอื่นใดตามระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการรับผิดชอบในการบริหารงานของสำนักงานขึ้นตรงต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 49 ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการ เป็นผู้แทนของสำนักงาน เพื่อการนี้ เลขาธิการจะมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทน ก็ได้ แต่ต้องเป็นไปตามข้อบังคับที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 50 ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้กำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา 51 เพื่อประโยชน์ในการบริหารงานของสำนักงาน เลขาธิการอาจขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐมาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราวได้ ทั้งนี้ เมื่อได้รับอนุมัติจากผู้บังคับบัญชาหรือนายจ้างของผู้นั้น และมีข้อตกลงที่ทำไว้ในการอนุมัติ และในกรณีที่เจ้าหน้าที่ของรัฐได้รับอนุมัติให้มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราว ให้ถือว่าเป็นการได้รับอนุญาตให้ออกจากราชการหรือออกจากงานไปปฏิบัติงานใด ๆ

เมื่อสิ้นสุดระยะเวลาที่ได้รับอนุมัติให้มาปฏิบัติงานในสำนักงาน ให้เจ้าหน้าที่ของรัฐตามวรรคหนึ่ง มีสิทธิได้รับการบรรจุและแต่งตั้งให้ดำรงตำแหน่งและรับเงินเดือนในส่วนราชการหรือหน่วยงานเดิมไม่ต่ำกว่าตำแหน่งและเงินเดือนเดิมตามข้อตกลงที่ทำไว้ในการอนุมัติ

ในกรณีที่เจ้าหน้าที่ของรัฐผู้นั้นกลับมาบรรจุและได้รับแต่งตั้งในส่วนราชการหรือหน่วยงานเดิมตามวรรคสองแล้ว ให้นับระยะเวลาของเจ้าหน้าที่ของรัฐผู้นั้นระหว่างที่มาปฏิบัติงานในสำนักงานสำหรับการคำนวณบำเหน็จบำนาญหรือประโยชน์ตอบแทนอื่นทำนองเดียวกันเสมือนอยู่ปฏิบัติราชการหรือปฏิบัติงานเต็มเวลาดังกล่าว แล้วแต่กรณี

มาตรา 52 ข้าราชการหรือเจ้าหน้าที่ของรัฐซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากส่วนราชการหรือหน่วยงานของรัฐ ที่ได้ย้ายมาปฏิบัติหน้าที่ที่สำนักงานโดยได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัด ให้ถือเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในสำนักงานเป็นระยะเวลาในการชดใช้ทุน

ในกรณีที่หน่วยงานของรัฐแห่งใดประสงค์จะขอให้พนักงานของสำนักงานซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากสำนักงานไปเป็นข้าราชการหรือเจ้าหน้าที่ของรัฐในหน่วยงานของรัฐแห่งนั้น ต้องได้รับความเห็นชอบจากเลขาธิการก่อน และให้ถือว่าการไปปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นระยะเวลาในการชดใช้ทุน

มาตรา 53 การบัญชีของสำนักงานให้จัดทำตามหลักสากล ตามแบบและหลักเกณฑ์ที่คณะกรรมการกากับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา 54 ให้สำนักงานจัดทางบดุล งบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในหนึ่งร้อยยี่สิบวันนับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อคณะกรรมการเพื่อรับรอง

มาตรา 55 ให้สำนักงานจัดทำรายงานการดำเนินงานประจำปีเสนอคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นชอบ

มาตรา 56 ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามอำนาจหน้าที่และตามกฎหมาย นโยบายของรัฐบาล แผนยุทธศาสตร์ และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่ออำนาจหน้าที่ของสำนักงาน นโยบายของรัฐบาล แผนยุทธศาสตร์ หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้

ในกรณีที่เลขาธิการฝ่าฝืนหรือไม่กระทำการตามคำสั่งของรัฐมนตรีตามวรรคหนึ่ง ให้รัฐมนตรีส่งเรื่องให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาดำเนินการตามอำนาจหน้าที่ต่อไป

หมวด 6
การร้องเรียน

มาตรา 57 ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร

คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่งและการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา 58 คณะกรรมการผู้เชี่ยวชาญมีอำนาจและหน้าที่ ดังต่อไปนี้

(1) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้

(2) ตรวจสอบการกระทำใดๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(3) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(4) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ

มาตรา 59 เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียน ให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

มาตรา 60 ในกรณีที่ผู้ร้องเรียนตามมาตรา 59 ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา 59 วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นไม่ได้กำหนดให้ไม่ให้รับไว้พิจารณาให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา

เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา 59(1) หรือตรวจสอบการกระทำใดๆ ตามมาตรา 59(2) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง

ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้

(1) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด

(2) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (1) หรือ (2) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น

การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสองหรือวรรคสาม (1) หรือ (2) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน

มาตรา 61 คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา 60 วรรคหนึ่งหรือยุติเรื่องตามมาตรา 60 วรรคสอง หรือคำสั่งตามมาตรา 60 วรรคสาม (1) หรือ (2) ให้เป็นที่สุด

มาตรา 62 ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะเรียกให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้

มาตรา 63 ในการปฏิบัติตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ดังต่อไปนี้

(1) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้

(2) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำความผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

ในการดำเนินการตาม (2) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร

หมวด 6
ความรับผิดทางแพ่ง

มาตรา 64 ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(3) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 14(6)

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

หมวด 7
บทกำหนดโทษ

ส่วนที่ 1
โทษอาญา

มาตรา 65 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 เพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น หรือโดยประการที่น่าจะทำให้ผู้อื่นนั้นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 66 ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 67 ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆ ด้วย

มาตรา 68 บรรดาความผิดตามพระราชบัญญัตินี้ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้

เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ส่วนที่ 2
โทษทางปกครอง

มาตรา 69 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 20 มาตรา 26 วรรคสี่ มาตรา 31 หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 17 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 17 วรรคห้า ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งแสนบาท

มาตรา 70 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ต้องระวางโทษปรับทางปกครองไม่เกินสามแสนบาท

มาตรา 71 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 หรือฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท

มาตรา 72 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 30 โดยไม่มีเหตุอันควร ต้องระวางโทษปรับทางปกครองไม่เกินสามแสนบาท

มาตรา 73 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 62 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 63 วรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งแสนบาท

มาตรา 74 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนทบาท

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

มาตรา 75 ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด

ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

บทเฉพาะกาล

มาตรา 76 ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา 8 (2) (3) และกรรมการตามวรรคสอง เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ และให้รอบประธานกรรมการทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา 8(1) และกรรมการผู้ทรงคุณวุฒิตามมาตรา 8(4) ภายในเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 77 ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 78 ในวาระเริ่มแรกที่ยังไม่มีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ให้รัฐมนตรีแต่งตั้งผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือบุคคลใดตามที่รัฐมนตรีเห็นสมควร ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 79 ในวาระเริ่มแรก เมื่อได้จัดตั้งสำนักงานแล้วแต่ยังไม่มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ และผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลที่รัฐมนตรีแต่งตั้ง จำนวนสี่คน เป็นกรรมการ และให้ผู้ปฏิบัติหน้าที่เลขาธิการตามมาตรา 78 เป็นเลขานุการของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยให้ปฏิบัติหน้าที่เป็นการชั่วคราวไปจนกว่าจะมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ

มาตรา 80 ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

มาตรา 81 ในวาระเริ่มแรก ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานเป็นพนักงานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนดได้

มาตรา 82 ในระหว่างที่ยังมิได้มีการออกประกาศ ระเบียบ หรือข้อบังคับในส่วนที่เกี่ยวข้องกับสำนักงานตามพระราชบัญญัตินี้ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถกำหนดให้นำประกาศ ระเบียบ หรือข้อบังคับของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือของหน่วยงานของรัฐอื่นซึ่งอยู่ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ใช้บังคับอยู่ในวันก่อนวันที่บทบัญญัติใน

หมวด 1 และหมวด 4 มีผลใช้บังคับ มาใช้บังคับโดยอนุโลมกับสำนักงานได้ ทั้งนี้ เท่าที่ไม่ขัดหรือแย้งกับพระราชบัญญัตินี้

มาตรา 83 ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมที่ ทั้งนี้ ผู้ควบคุมข้อมูลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกค วามยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

มาตรา 84 การดำเนินการออกกฎกระทรวง ประกาศ ระเบียบและข้อบังคับตามพระราชบัญญัตินี้ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

ผู้สนองพระบรมราชโองการ

.....

นายกรัฐมนตรี

ภาคผนวก ซ

ตารางเปรียบเทียบความแตกต่างระหว่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับความมั่นคงดิจิทัล ฉบับรับฟังความคิดเห็น และฉบับคณะรัฐมนตรีอนุมัติหลักการ

ความแตกต่างของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ฉบับความมั่นคงดิจิทัล ฉบับรับฟังความคิดเห็น และฉบับคณะรัฐมนตรีอนุมัติหลักการ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
เหตุผล เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือนร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้	**เหตุผล** ไม่เปลี่ยนแปลง	**เหตุผล** ไม่เปลี่ยนแปลง
มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”	**มาตรา 1** ไม่เปลี่ยนแปลง	**มาตรา 1** ไม่เปลี่ยนแปลง
มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป	**มาตรา 2** พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่บทบัญญัติในหมวดหนึ่งและหมวดห้าให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป	**มาตรา 2** คล้ายกับร่างฉบับรับฟังความคิดเห็นแต่แก้ไขให้บทบัญญัติในหมวด 1 หมวด 4 และมาตรา 77 มาตรา 78 มาตรา 79

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		มาตรา 80 มาตรา 81 มาตรา 82 และมาตรา 83 มีผลใช้บังคับในวันถัดจากวันที่ประกาศในราชกิจการนุเบกษา
มาตรา 3 ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่ (1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม (2) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ในกรณีดังต่อไปนี้ (ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน (ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลแต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าว	**มาตรา 3** ไม่เปลี่ยนแปลง	**มาตรา 3** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคล ผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี		
<u>มาตรา 4</u> พระราชบัญญัตินี้ไม่ใช้บังคับแก่ (1) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น (2) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น (3) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี (4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา (5) การดำเนินกิจการทางศาสนาขององค์การทางศาสนา (6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต	**<u>มาตรา 4</u>** ไม่เปลี่ยนแปลง	**<u>มาตรา 4</u>** ตัดการดำเนินกิจการทางศาสนาขององค์การทางศาสนาออก

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา		
		<u>มาตรา 5</u> เพิ่มขอบเขตการใช้บังคับของพระราชบัญญัติโดยให้รวมถึงกรณีดังต่อไปนี้ (1) การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรโดยผู้ควบคุมข้อมูลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าผู้นั้นจะอยู่ในหรือนอกราชอาณาจักร (2) การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่กระทำนอกราชอาณาจักรแม้แต่ส่วนหนึ่งส่วนใดของการกระทำได้กระทำในราชอาณาจักร หรือกระทำนอกราชอาณาจักรที่ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้ควบคุม

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		ข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักรหรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นนั้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักร ให้ถือว่าเป็นการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้กระทำในราชอาณาจักร
มาตรา 5 ในพระราชบัญญัตินี้ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	**มาตรา 5** ในพระราชบัญญัตินี้ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้คำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล	มาตรา 6 แก้ไขบทนิยามของผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้ “ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า ให้หมายความรวมถึง (1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ (2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ (3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ “บุคคล” หมายความว่า บุคคลธรรมดา “คณะกรรมการ”หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ “สำนักงาน” หมายความว่า สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ “เลขาธิการ” หมายความว่า เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ “รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้	“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า ให้หมายความรวมถึง (1) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ (2) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ (3) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ “บุคคล” หมายความว่า บุคคลธรรมดา “คณะกรรมการ”หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ “สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “เลขาธิการ” หมายความว่า เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้	
มาตรา 6	**มาตรา 6** ไม่เปลี่ยนแปลง	**มาตรา 7** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้ กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้ใช้บังคับได้		
มาตรา 7 ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย (1) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล (2) กรรมการโดยตำแหน่ง จำนวนเจ็ดคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ผู้แทนสภาหอการค้าแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย	**มาตรา 7** ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย (1) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล (2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ (3) กรรมการโดยตำแหน่ง จำนวนสามคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ (4) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วน	**มาตรา 8** เพิ่มกรรมการโดยตำแหน่งอีก 5 คน ได้แก่ เลขาธิการคณะกรรมการกฤษฎีกา อัยการสูงสุด ผู้แทนสภาหอการค้าแห่งประเทศไทย ผู้แทนสภาอุตสาหกรรมแห่งประเทศไทย และผู้แทนสมาคาธนาคารไทย

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(3) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา 10 ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด	บุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา 10 ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด	
<u>มาตรา 8</u> ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้ (1) มีสัญชาติไทย (2) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต (3) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ	**<u>มาตรา 8</u>** ไม่เปลี่ยนแปลง	**<u>มาตรา 9</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(4) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ		
มาตรา 9 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระดำรงตำแหน่งคราวละสามปี เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้	**มาตรา 9** ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระดำรงตำแหน่งคราวละสี่ปี เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้	**มาตรา 10** ไม่เปลี่ยนแปลง
มาตรา 10 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 9 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ (1) ตาย (2) ลาออก (3) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ (4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 8	**มาตรา 10** นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 9 ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ (1) ตาย (2) ลาออก (3) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ (4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 8	**มาตรา 11** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้ ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระให้กรรมการที่เหลือเลือกกรรมการคนหนึ่งทำหน้าที่ประธานกรรมการเป็นการชั่วคราว	ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้ ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระให้รองประธานกรรมการทำหน้าที่เป็นประธานกรรมการเป็นการชั่วคราว	
มาตรา 11 การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด	**มาตรา 11** การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้รองประธานกรรมการทำหน้าที่เป็นประธานในที่ประชุม การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด	**มาตรา 12** เพิ่มข้อความในวรรคสอง ดังนี้ “ในกรณีที่ประธานกรรมการและรองประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม”

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด	การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด	
มาตรา 12 กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณาให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว	**มาตรา 12** ไม่เปลี่ยนแปลง	**มาตรา 13** ไม่เปลี่ยนแปลง
มาตรา 13 คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้ (1) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติตามนโยบายและแผนระดับชาติดังกล่าว (2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมการแผนยุทธศาสตร์ตาม (1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าวเพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (3) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้ (4) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้	**มาตรา 13** คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้ (1) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติตามนโยบายและแผนระดับชาติดังกล่าว (2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมการแผนยุทธศาสตร์ตาม (1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าวเพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (3) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้ (4) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้	**มาตรา 14** เพิ่มอำนาจหน้าที่ของคณะกรรมการ โดยแทรกเป็น (6) และ (7) ดังนี้ (6) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ (7) พิจารณากำหนดค่าปรับทางปกครองตามมาตรา 69 มาตรา 70 มาตรา 71 มาตรา 72 มาตรา 73 มาตรา 74 และมาตรา 75 รวมทั้งฟ้องคดีต่อศาลปกครอง ทั้งนี้ ในกรณีที่มีการบังคับทางปกครองเพื่อชำระค่าปรับทางปกครอง ให้คณะกรรมการเป็นผู้มีอำนาจออกคำสั่งยึด

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ (6) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (7) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้ (8) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้ (9) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน (10) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (11) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ	(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ (6) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (7) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้ (8) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้ (9) ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัตินี้ (10) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน (11) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (12) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ	อายัด หรือขายทอดตลาดทรัพย์สินในการบังคับทางปกครองและให้ประธานกรรมการเป็นผู้ลงนามแทนในคำสั่งดังกล่าว
มาตรา 14 ให้กรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด	**มาตรา 14** ไม่เปลี่ยนแปลง	**มาตรา 15** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
อนุกรรมการและกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด		
มาตรา 15 คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้ การประชุมคณะอนุกรรมการให้นำความในมาตรา 11 มาใช้บังคับโดยอนุโลม	**มาตรา 15** ไม่เปลี่ยนแปลง	**มาตรา 16** ไม่เปลี่ยนแปลง
มาตรา 16 ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ดังต่อไปนี้ (1) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (2) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ (3) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้างหรือประชาชนทั่วไป (4) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้		

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(5) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของสำนักงาน		
มาตรา 17 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้ การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล	**มาตรา 16** ไม่เปลี่ยนแปลง	**มาตรา 17** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น		
มาตรา 18 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่ (1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว (2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้	**มาตรา 17** ไม่เปลี่ยนแปลง	**มาตรา 18** ไม่เปลี่ยนแปลง
มาตรา 19 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล	**มาตรา 18** ไม่เปลี่ยนแปลง	**มาตรา 19** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
มาตรา 20 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ (1) วัตถุประสงค์ของการเก็บรวบรวม (2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม (3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ (5) สิทธิของเจ้าของข้อมูลตามมาตรา 26 มาตรา 27 และมาตรา 28 กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า	**มาตรา 19** ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ (1) วัตถุประสงค์ของการเก็บรวบรวม (2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม (3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ (5) สิทธิของเจ้าของข้อมูลตามมาตรา 25 มาตรา 26 และมาตรา 27 กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า	**มาตรา 20** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ
มาตรา 21 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ	**มาตรา 20** ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล	**มาตรา 21** ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล (4) เป็นการปฏิบัติตามกฎหมาย (5) กรณีอื่นตามที่กำหนดในกฎกระทรวง	(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล (4) เป็นการจำเป็นสำหรับการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือในการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวด้อยกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล (5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายสำหรับผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลที่สาม เว้นแต่ประโยชน์ดังกล่าวด้อยกว่าประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นเด็ก กรณีข้อนี้ไม่ใช้บังคับกับการดำเนินการข้อมูลส่วนบุคคลในการปฏิบัติหน้าที่ของหน่วยงานของรัฐ (6) เป็นการปฏิบัติตามกฎหมาย (7) กรณีอื่นตามที่กำหนดในกฎกระทรวง	(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล (4) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (5) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้การดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูล (6) เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล (7) กรณีอื่นตามที่กำหนดในกฎกระทรวง
มาตรา 22 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตาม มาตรา 24	**มาตรา 21** ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตามมาตรา 23 (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ	**มาตรา 22** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ		
มาตรา 23 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) ได้รับยกเว้นตามมาตรา 21 (2) หรือ (4) (2) กรณีอื่นตามที่กำหนดในกฎกระทรวง	**มาตรา 22** ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) ได้รับยกเว้นตามมาตรา 20 (2) หรือ (6) (2) กรณีอื่นตามที่กำหนดในกฎกระทรวง	**มาตรา 23** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ
มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 21 หรือมาตรา 23 หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา 22(3) แล้วแต่กรณี บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่งจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น	**มาตรา 23** ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 20 หรือมาตรา 22 หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา 21(3) แล้วแต่กรณี บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่งจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น	**มาตรา 24** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา 30	ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา 30	
มาตรา 25 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 13 (5) เว้นแต่ (1) เป็นการปฏิบัติตามกฎหมาย (2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (3) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล (4) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้ (5) เป็นการโอนไปยังผู้ซึ่งได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 32 หรือมาตรา 34 (6) กรณีอื่นตามที่กำหนดในกฎกระทรวง	**มาตรา 24** ไม่เปลี่ยนแปลง	**มาตรา 25** เพิ่มว่า “ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ”
มาตรา 26 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม	**มาตรา 25** ไม่เปลี่ยนแปลง	**มาตรา 26** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้ (1) เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล (2) มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย (3) การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น (4) กรณีอื่นตามที่กำหนดในกฎกระทรวง ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 30 เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ทั้งนี้ คณะกรรมการจะประกาศกำหนดระยะเวลาในการดำเนินการตามคำขอให้เร็วขึ้นหรือขยายระยะเวลาดังกล่าวหรือกำหนดหลักเกณฑ์อื่นตามความเหมาะสมก็ได้		
<u>มาตรา 27</u> ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล	**<u>มาตรา 26</u>** ไม่เปลี่ยนแปลง	**<u>มาตรา 27</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ดำเนินการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้		
<u>มาตรา 28</u> ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามวรรคหนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามวรรคหนึ่งไว้ในรายการตามมาตรา 30	**<u>มาตรา 27</u>** ไม่เปลี่ยนแปลง	**<u>มาตรา 28</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
มาตรา 29 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้ (1) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (3) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 27 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม (4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนดให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด	**มาตรา 28** ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้ (1) ประเมินผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นประจำอย่างสม่ำเสมอ (2) จัดให้มีมาตรการรักษาความมั่งคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (3) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (4) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา 26 วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม (5) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด	**มาตรา 29** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**มาตรา 29** ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้ (1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ (2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ (3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามที่คณะกรรมการประกาศกำหนด	**มาตรา 30** ไม่เปลี่ยนแปลง
มาตรา 30 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น	**มาตรา 30** ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น (6) การใช้และการเปิดเผยตามมาตรา 23 วรรคสาม	**มาตรา 31** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(6) การใช้และการเปิดเผยตามมาตรา 24 วรรคสาม (7) การปฏิเสธคำขอตามมาตรา 26 วรรคสาม และมาตรา 28 วรรคสอง	(7) การปฏิเสธคำขอตามมาตรา 25 วรรคสาม และมาตรา 27 วรรคสอง	
มาตรา 31 ให้คณะกรรมการประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติ	**มาตรา 31** ให้คณะกรรมการประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ	ตัดทิ้ง
มาตรา 32 ให้มีเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงานมีสิทธิใช้หรือแสดงเครื่องหมายดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลที่ประสงค์จะมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ให้ยื่นคำขอรับใบรับรองต่อสำนักงานตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด ในการพิจารณาคำขอตามวรรคสอง ให้สำนักงานประเมินผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 31 ให้สำนักงานออกใบรับรองแก่ผู้ควบคุมข้อมูลส่วนบุคคลนั้น	**มาตรา 32** ไม่เปลี่ยนแปลง	ตัดทิ้ง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ลักษณะและรายละเอียดของเครื่องหมายรับรองมาตรฐาน การใช้หรือการแสดงเครื่องหมาย วิธีการประเมินผล การตรวจติดตามผล อัตราค่าธรรมเนียมการประเมินผลหรือการตรวจติดตามผล และการเพิกถอนใบรับรองให้เป็นไปตามที่คณะกรรมการประกาศกำหนด ในกรณีที่สำนักงานเพิกถอนใบรับรองของผู้ควบคุมข้อมูลส่วนบุคคลใด ให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นคืนใบรับรองให้แก่สำนักงานภายในสิบห้าวันนับแต่วันที่ได้รับแจ้งการเพิกถอน คณะกรรมการจะประกาศกำหนดให้หน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนทั้งในประเทศและต่างประเทศเป็นผู้ประเมินผลและตรวจติดตามผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อขอรับใบรับรองจากสำนักงานตามวรรคสามด้วยก็ได้ ห้ามมิให้ผู้ใดใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเว้นแต่เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงาน		
<u>มาตรา 33</u> มาตรฐานของผู้ประเมินผลและตรวจติดตามผล การตรวจสอบมาตรฐานและอัตราค่าธรรมเนียมการตรวจสอบมาตรฐานสำหรับหน่วยงานของเอกชน รวมทั้งการเพิกถอนรายชื่อจากประกาศตามมาตรา 32 วรรคหก ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด	**<u>มาตรา 33</u>** ไม่เปลี่ยนแปลง	ตัดทิ้ง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
มาตรา 34 คณะกรรมการจะประกาศยอมรับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานต่างประเทศหรือองค์การระหว่างประเทศก็ได้ หากปรากฏว่า การคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามที่คณะกรรมการประกาศกำหนดตามมาตรา 31	**มาตรา 34** ไม่เปลี่ยนแปลง	ตัดทิ้ง
-	**มาตรา 35** ให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ สำนักงานเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยแรงงานรัฐวิสาหกิจสัมพันธ์ กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน	**มาตรา 32** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	ให้สำนักงานเป็นหน่วยงานของรัฐตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่	
-	**มาตรา 36** นอกจากดำเนินการให้เป็นไปตามวัตถุประสงค์ตามมาตรา 35 วรรคหนึ่ง ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ดังต่อไปนี้ (1) จัดทำร่างแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการ (2) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล	**มาตรา 33** ปรับเลขมาตราเพียงเล็กน้อยซึ่งไม่กระทบสาระสำคัญ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(3) วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (4) สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล และแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการ (5) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (6) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ (7) เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานภาครัฐ หน่วยงานเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล (8) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป (9) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามอำนาจหน้าที่ของสำนักงาน (10) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้	

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(11) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด	
-	**มาตรา 37** ในการดำเนินงานของสำนักงาน นอกจากอำนาจหน้าที่ตามที่บัญญัติในมาตรา 36 แล้ว ให้สำนักงานมีอำนาจหน้าที่ทั่วไป ดังต่อไปนี้ด้วย (1) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิ ต่าง ๆ (2) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน (3) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน (4) ถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นในกิจการที่เกี่ยวกับวัตถุประสงค์ของสำนักงาน (5) กู้ยืมเงินเพื่อประโยชน์ในการดำเนินการตามวัตถุประสงค์ของสำนักงาน (6) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (7) ดำเนินการอื่นใดที่จำเป็นหรือต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของสำนักงาน	**มาตรา 34** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(8) ปฏิบัติการใด ๆ ให้เป็นไปตามพระราชบัญญัตินี้ หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือคณะกรรมการมอบหมาย การถือหุ้น เข้าเป็นหุ้นส่วน หรือเข้าร่วมทุนกับนิติบุคคลอื่นตาม (4) และการกู้ยืมเงินตาม (5) ให้เป็นไปตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด	
-	**มาตรา 38** ทุนและทรัพย์สินในการดำเนินงานของสำนักงานประกอบด้วย (1) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา 78 (2) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี (3) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้จากการดำเนินงาน (4) เงินอุดหนุนจากภาคเอกชนหรือองค์กรอื่น รวมทั้งจากต่างประเทศหรือองค์การระหว่างประเทศ และเงินหรือทรัพย์สินที่มีผู้อุทิศให้ (5) ดอกผลและผลประโยชน์หรือรายได้อื่นใดที่เกิดจากการดำเนินงานของสำนักงาน ทรัพย์สินของสำนักงานไม่อยู่ในความรับผิดแห่งการบังคับคดีและมาตรการบังคับทางปกครอง เงินและทรัพย์สินของสำนักงานไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน ยกเว้นดอกผล และผลประโยชน์หรือรายได้อื่นตามวรรคหนึ่ง (5) เมื่อใช้จ่ายตามอำนาจหน้าที่ของสำนักงานแล้ว ที่เหลือให้นำส่งคลังเป็นรายได้แผ่นดิน	**มาตรา 35** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**มาตรา 39** ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ประธานกรรมการซึ่งรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งจำนวนหกคน ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานเป็นผู้ช่วยเลขานุการได้ตามความจำเป็นแต่ไม่เกินสองคน กรรมการผู้ทรงคุณวุฒิซึ่งรัฐมนตรีแต่งตั้งตามวรรคหนึ่ง ต้องมีความรู้ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยสามคน และด้านอื่นที่เกี่ยวข้องอันเป็นประโยชน์ต่อการดำเนินงานของสำนักงาน ให้นำบทบัญญัติมาตรา 8 และมาตรา 10 มาใช้บังคับกับประธานกรรมการและกรรมการผู้ทรงคุณวุฒิโดยอนุโลม	**มาตรา 36** เพิ่มให้ “เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เป็นกรรมการ”
-	**มาตรา 40** ให้ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวาระการดำรงตำแหน่งคราวละสี่ปี	**มาตรา 37** ให้ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีวาระการดำรงตำแหน่งคราวละสี่ปี

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		เมื่อครบกำหนดตามวาระในวรรคหนึ่ง ให้ดำเนินการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ภายในหกสิบวัน ในระหว่างที่ยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้
-	**มาตรา 41** เมื่อประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา 39 พ้นจากตำแหน่งตามวาระ ให้ดำเนินการแต่งตั้งใหม่ภายในหกสิบวัน ในระหว่างที่ยังมิได้มีการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้น อยู่ใน	**มาตรา 38** ในกรณีที่ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ พ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วยกรรมการทั้งหมด

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	ตำแหน่งเพื่อปฏิบัติหน้าที่ต่อไปจนกว่าประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่ ในกรณีที่ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการประกอบด้วยกรรมการเท่าที่เหลืออยู่และให้ดำเนินการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิแทนตำแหน่งที่ว่างภายในหกสิบวันนับแต่วันที่ตำแหน่งว่างลง เว้นแต่วาระของกรรมการเหลือไม่ถึงเก้าสิบวัน และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน	เท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทน และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่ประธานกรรมการเป็นการชั่วคราว ให้ดำเนินการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิแทนตำแหน่งที่ว่างภายในหกสิบวันนับแต่วันที่ตำแหน่งว่างลง และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน เว้นแต่วาระของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิเหลือไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**มาตรา 42** การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ จึงจะเป็นองค์ประชุม ให้ประธานกรรมการเป็นประธานในที่ประชุม ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้ที่ประชุมเลือกกรรมการคนหนึ่งเพื่อทำหน้าที่ประธานในที่ประชุม ในการวินิจฉัยชี้ขาดให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้ามีคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด กรรมการที่มีส่วนได้เสียในเรื่องที่มีการพิจารณาจะเข้าร่วมประชุมมิได้ การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจกระทำโดยวิธีการทางอิเล็กทรอนิกส์ตามที่คณะกรรมการกำหนดก็ได้	**มาตรา 39** ไม่เปลี่ยนแปลง
-	**มาตรา 43** ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีอำนาจหน้าที่ ดังต่อไปนี้ (1) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน	**มาตรา 40** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(2) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน (3) อนุมัติแผนการดำเนินงาน แผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน (4) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง (5) แต่งตั้งคณะกรรมการสรรหาเลขาธิการ (6) วินิจฉัยอุทธรณ์คำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน (7) ประเมินผลการดำเนินการของสำนักงาน และการปฏิบัติงานของเลขาธิการ (8) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการกำกับสำนักงานคุ้มครองข้อมูลส่วนหรือตามที่คณะรัฐมนตรีมอบหมาย ข้อบังคับตาม (2) ถ้ามีการจำกัดอำนาจเลขาธิการในการทำนิติกรรมกับบุคคลภายนอกให้ประกาศในราชกิจจานุเบกษา	
-	**<u>มาตรา 44</u>** ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจแต่งตั้งคณะอนุกรรมการ เพื่อปฏิบัติหน้าที่หรือกระทำการอย่างหนึ่ง	**<u>มาตรา 41</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	อย่างใดตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมอบหมายได้ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจแต่งตั้งบุคคลซึ่งมีความเชี่ยวชาญหรือประสบการณ์ที่จะเป็นประโยชน์ในการปฏิบัติหน้าที่ของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ การปฏิบัติหน้าที่และจำนวนของคณะอนุกรรมการตามวรรคหนึ่งหรือบุคคลตามวรรคสอง ให้เป็นไปตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด ให้นำมาตรา 42 มาใช้บังคับแก่คณะอนุกรรมการโดยอนุโลม	
-	**<u>มาตรา 45</u>** ให้ประธานกรรมการและกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประธานอนุกรรมการและอนุกรรมการภายใต้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้รับเบี้ยประชุมหรือค่าตอบแทนตามหลักเกณฑ์ที่คณะกรรมการกำหนด	**<u>มาตรา 42</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**มาตรา 46** ให้สำนักงานมีเลขาธิการคนหนึ่งซึ่งคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง มีหน้าที่บริหารกิจการของสำนักงาน	**มาตรา 43** ไม่เปลี่ยนแปลง
-	**มาตรา 47** ผู้ที่จะได้รับการแต่งตั้งเป็นเลขาธิการต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้ (1) มีสัญชาติไทย (2) อายุไม่เกินห้าสิบห้าปีบริบูรณ์ (3) สามารถทำงานให้แก่สำนักงานได้เต็มเวลา (4) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงาน และการบริหารจัดการ (5) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต (6) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ (7) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ (8) ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจ หรือจากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง (9) ไม่เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย	**มาตรา 44** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(10) ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่พรรคการเมือง (11) ไม่เป็นผู้มีส่วนได้เสียในกิจการที่เกี่ยวข้องกับสำนักงานไม่ว่าโดยทางตรงหรือทางอ้อม	
-	**มาตรา 48** เลขาธิการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระติดต่อกันไม่ได้ ก่อนครบกำหนดตามวาระการดำรงตำแหน่งของเลขาธิการเป็นเวลาไม่น้อยกว่าสามสิบวันแต่ไม่เกินหกสิบวัน หรือภายในสามสิบวันนับแต่วันที่เลขาธิการพ้นจากตำแหน่งก่อนครบวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งคณะกรรมการเพื่อสรรหาเลขาธิการคนใหม่ ทั้งนี้ ให้คณะกรรมการสรรหาเสนอรายชื่อบุคคลที่เหมาะสมไม่เกินสามคนต่อคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	**มาตรา 45** ไม่เปลี่ยนแปลง
-	**มาตรา 49** ในแต่ละปีให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด	**มาตรา 46** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**<u>มาตรา 50</u>** นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 48 เลขาธิการพ้นจากตำแหน่ง เมื่อ (1) ตาย (2) ลาออก (3) อายุครบหกสิบปีบริบูรณ์ (4) คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน มีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ (5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก (6) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 47 ยกเว้นกรณีมาตรา 47 (2)	**<u>มาตรา 47</u>** ปรับมาตราเล็กน้อย ไม่กระทบสาระสำคัญ
-	**<u>มาตรา 51</u>** ให้เลขาธิการมีอำนาจหน้าที่ ดังต่อไปนี้ (1) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนระดับชาติ แผนยุทธศาสตร์ นโยบายของคณะรัฐมนตรี คณะกรรมการ และคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และระเบียบข้อบังคับหรือมติของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	**<u>มาตรา 48</u>** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	(2) วางระเบียบเกี่ยวกับการดำเนินงานของสำนักงานโดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศที่คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด (3) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามระเบียบหรือข้อบังคับของสำนักงาน (4) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย (5) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงาน และลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามระเบียบหรือข้อบังคับที่คณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด (6) ปฏิบัติการอื่นใดตามระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ให้เลขาธิการรับผิดชอบในการบริหารงานของสำนักงานขึ้นตรงต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
-	**มาตรา 52** ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการ เป็นผู้แทนของสำนักงาน เพื่อการนี้ เลขาธิการจะมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทน ก็ได้ แต่ต้องเป็นไปตามข้อบังคับที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด	**มาตรา 49** ไม่เปลี่ยนแปลง
-	**มาตรา 53** ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้กำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด	**มาตรา 50** ไม่เปลี่ยนแปลง
-	**มาตรา 54** เพื่อประโยชน์ในการบริหารงานของสำนักงาน เลขาธิการอาจขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐ มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราวได้ ทั้งนี้ เมื่อได้รับอนุมัติจากผู้บังคับบัญชาหรือนายจ้างของผู้นั้น และมีข้อตกลงที่ทำไว้ในการอนุมัติ และในกรณีที่เจ้าหน้าที่ของรัฐได้รับอนุมัติให้มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราว ให้ถือว่าเป็นการได้รับอนุญาตให้ออกจากราชการหรือออกจากงานไปปฏิบัติงานใด ๆ	**มาตรา 51** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	เมื่อสิ้นสุดระยะเวลาที่ได้รับอนุมัติให้มาปฏิบัติงานในสำนักงาน ให้เจ้าหน้าที่ของรัฐตามวรรคหนึ่ง มีสิทธิได้รับการบรรจุและแต่งตั้งให้ดำรงตำแหน่งและรับเงินเดือนในส่วนราชการหรือหน่วยงานเดิมไม่ต่ำกว่าตำแหน่งและเงินเดือนเดิมตามข้อตกลงที่ทำไว้ในการอนุมัติ ในกรณีที่เจ้าหน้าที่ของรัฐผู้นั้นกลับมาบรรจุและได้รับแต่งตั้งในส่วนราชการหรือหน่วยงานเดิมตามวรรคสองแล้ว ให้นับระยะเวลาของเจ้าหน้าที่ของรัฐผู้นั้นระหว่างที่มาปฏิบัติงานในสำนักงานสำหรับการคำนวณบำเหน็จบำนาญหรือประโยชน์ตอบแทนอื่นทำนองเดียวกันเสมือนอยู่ปฏิบัติราชการหรือปฏิบัติงานเต็มเวลาดังกล่าว แล้วแต่กรณี	
-	**มาตรา 55** ข้าราชการหรือเจ้าหน้าที่ของรัฐซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากส่วนราชการหรือหน่วยงานของรัฐ ที่ได้ย้ายมาปฏิบัติหน้าที่ที่สำนักงานโดยได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัด ให้ถือเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในสำนักงานเป็นระยะเวลาในการชดใช้ทุน ในกรณีที่หน่วยงานของรัฐแห่งใดประสงค์จะขอให้พนักงานของสำนักงานซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากสำนักงานไปเป็นข้าราชการหรือเจ้าหน้าที่ของรัฐในหน่วยงานของรัฐแห่งนั้น ต้องได้รับความเห็นชอบจากเลขาธิการก่อน และให้ถือว่าการไปปฏิบัติงานในหน่วยงานของรัฐแห่ง	**มาตรา 52** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	นั้นเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นระยะเวลาในการชดใช้ทุน	
-	**มาตรา 56** การบัญชีของสำนักงานให้จัดทำตามหลักสากล ตามแบบและหลักเกณฑ์ที่คณะกรรมการกากับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด	**มาตรา 53** ไม่เปลี่ยนแปลง
-	**มาตรา 57** ให้สำนักงานจัดทางบดุล งบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในหนึ่งร้อยยี่สิบวันนับแต่วันสิ้นปีบัญชี ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงานและประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อคณะกรรมการเพื่อรับรอง	**มาตรา 54** ไม่เปลี่ยนแปลง
-	**มาตรา 58** ให้สำนักงานจัดทำรายงานการดำเนินงานประจำปีเสนอคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน รายงานการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว	**มาตรา 55** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นชอบ	
-	**มาตรา 59** ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามอำนาจหน้าที่และตามกฎหมาย นโยบายของรัฐบาล แผนยุทธศาสตร์และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่ออำนาจหน้าที่ของสำนักงาน นโยบายของรัฐบาล แผนยุทธศาสตร์ หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้ ในกรณีที่เลขาธิการฝ่าฝืนหรือไม่กระทำการตามคำสั่งของรัฐมนตรีตามวรรคหนึ่ง ให้รัฐมนตรีส่งเรื่องให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาดำเนินการตามอำนาจหน้าที่ต่อไป	**มาตรา 56** ไม่เปลี่ยนแปลง
มาตรา 35 ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร	**มาตรา 60** ไม่เปลี่ยนแปลง	**มาตรา 57** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่งและการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด		
มาตรา 36 คณะกรรมการผู้เชี่ยวชาญมีอำนาจหน้าที่ ดังต่อไปนี้ (1) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้ (2) ตรวจสอบการกระทำใดๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล (3) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล (4) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ	**มาตรา 61** ไม่เปลี่ยนแปลง	**มาตรา 58** ไม่เปลี่ยนแปลง
มาตรา 37 เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ การยื่น การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียนให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด	**มาตรา 62** ไม่เปลี่ยนแปลง	**มาตรา 59** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
มาตรา 38 ในกรณีที่ผู้ร้องเรียนตามมาตรา 37 ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา 37 วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นไม่ได้กำหนดให้ไม่ให้รับไว้พิจารณาให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา 36 (1) หรือตรวจสอบการกระทำใดๆ ตามมาตรา 36(2) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้ หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้ (1) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด (2) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด	**มาตรา 63** ในกรณีที่ผู้ร้องเรียนตามมาตรา 62 ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา 62 วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นไม่ได้กำหนดให้ไม่ให้รับไว้พิจารณาให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา 61 (1) หรือตรวจสอบการกระทำใดๆ ตามมาตรา 61 (2) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้ หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้ (1) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด (2) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด	**มาตรา 60** ปรับเลขมาตราเล็กน้อย ไม่กระทบสาระสำคัญ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (1) หรือ (2) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสองหรือวรรคสาม (1) หรือ (2) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน	ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (1) หรือ (2) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสองหรือวรรคสาม (1) หรือ (2) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน	
มาตรา 39 คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา 38 วรรคหนึ่งหรือยุติเรื่องตามมาตรา 38 วรรคสอง หรือคำสั่งตามมาตรา 38 วรรคสาม (1) หรือ (2) ให้เป็นที่สุด	**มาตรา 64** คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา 63 วรรคหนึ่งหรือยุติเรื่องตามมาตรา 63 วรรคสอง หรือคำสั่งตามมาตรา 63 วรรคสาม (1) หรือ (2) ให้เป็นที่สุด	**มาตรา 61** ปรับเลขมาตราเล็กน้อย ไม่กระทบสาระสำคัญ
มาตรา 40 ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการ	**มาตรา 65** ไม่เปลี่ยนแปลง	**มาตรา 62** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
คุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะเรียกให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้		
มาตรา 41 ในการปฏิบัติตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ดังต่อไปนี้ (1) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลส่วนบุคคลหรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้ (2) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำความผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ ในการดำเนินการตาม (2) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด	**มาตรา 66** ในการปฏิบัติตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ดังต่อไปนี้ (1) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลส่วนบุคคลหรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้ (2) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำความผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ ในการดำเนินการตาม (2) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด	**มาตรา 63** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร	ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร	
มาตรา 42 ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า (1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย (3) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา 31 ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย	**มาตรา 67** ไม่เปลี่ยนแปลง	**มาตรา 64** ไม่เปลี่ยนแปลง
		มาตรา 65 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 เพื่อแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น หรือโดยประการที่น่าจะทำให้ผู้อื่นนั้นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ
		มาตรา 66 ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ
		มาตรา 67 ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆ ด้วย
		มาตรา 68 บรรดาความผิดตามพระราชบัญญัตินี้ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้ เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา
มาตรา 43 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 20 มาตรา 26 วรรคสี่ มาตรา 30 หรือมาตรา 32 วรรคห้า หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 17 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 17 วรรคห้า ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท	**มาตรา 68** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 19 มาตรา 25 วรรคสี่ มาตรา 30 หรือมาตรา 32 วรรคห้า หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 16 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 16 วรรคห้า ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท	**มาตรา 69** ปรับเป็นโทษปรับทางปกครอง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
มาตรา 44 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์หรือผู้ใดฝ่าฝืนมาตรา 32 วรรคเจ็ด ต้องระวางโทษปรับไม่เกินสามแสนบาท การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือเพื่อให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ	**มาตรา 69** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 17 มาตรา 18 มาตรา 20 มาตรา 21 มาตรา 23 วรรคหนึ่งหรือวรรคสอง มาตรา 24 หรือมาตรา 28 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์หรือผู้ใดฝ่าฝืนมาตรา 32 วรรคเจ็ด ต้องระวางโทษปรับไม่เกินสามแสนบาท การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือเพื่อให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษปรับไม่เกินห้าแสนบาท	**มาตรา 70** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 18 มาตรา 19 มาตรา 21 มาตรา 22 มาตรา 24 วรรคหนึ่งหรือวรรคสอง มาตรา 25 หรือมาตรา 29 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ต้องระวางโทษปรับทางปกครองไม่เกินสามแสนบาท
		มาตรา 71 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 หรือฝ่าฝืนมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท
	มาตรา 70 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 29 ต้องระวางโทษปรับไม่เกินสามแสนบาท	**มาตรา 72** ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 30 โดยไม่มีเหตุอันควร ต้องระวางโทษปรับทางปกครองไม่เกินสามแสนบาท

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษปรับไม่เกินห้าแสนบาท	
		มาตรา 73 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 62 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 63 วรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งแสนบาท
มาตรา 45 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 23 ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ การฝ่าฝืนตามมาตรา 24 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 25 เกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 23 ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาทหรือทั้งจำทั้งปรับ	**มาตรา 71** ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 22 ต้องระวางโทษปรับไม่เกินห้าแสนบาท การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่น ได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษปรับไม่เกินสองล้านบาท การฝ่าฝืนตามมาตรา 23 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 24 เกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 22 ต้องระวางโทษปรับไม่เกินห้าแสนบาท	

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
การฝ่าฝืนวรรคสาม หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ	การฝ่าฝืนตามวรรคสาม หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษปรับไม่เกินสองล้านบาท	
มาตรา 46 ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 40 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 41 วรรคสาม ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท	**มาตรา 72** ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 65 หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 66 วรรคสาม ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท	**มาตรา 73** เพิ่มโทษปรับทางปกครองและปรับรายละเอียด
มาตรา 47 ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติตามหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ	**มาตรา 73** ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติตามหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษปรับไม่เกินสองหมื่นบาท	**มาตรา 66** เพิ่มโทษจำคุกไม่เกินหนึ่งปี
มาตรา 48 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนทบาท หรือทั้งจำทั้งปรับ ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้ (1) การเปิดเผยตามหน้าที่ (2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี (3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย	**มาตรา 74** ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับไม่เกินห้าแสนบาท ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้ (1) การเปิดเผยตามหน้าที่ (2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี (3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย	**มาตรา 74** ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนทบาท ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้ (1) การเปิดเผยตามหน้าที่

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล (5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ	(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล (5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ	(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี (3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย (4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล (5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ
		มาตรา 75 ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		ราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้
มาตรา 49 บรรดาความผิดตามพระราชบัญญัตินี้ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้ เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา	**มาตรา 75** ไม่เปลี่ยนแปลง	**มาตรา 68** กำหนดไว้ในมาตรา 68
มาตรา 50 ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา 7(2) และกรรมการตามวรรคสองเพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่	**มาตรา 76**	**มาตรา 76** ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา 8 (2)

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ไม่เกินเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และให้กรรมการดังกล่าวเลือกกรรมการหนึ่งคนทำหน้าที่ประธานกรรมการเป็นการชั่วคราว ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา 7(1) และกรรมการผู้ทรงคุณวุฒิตามมาตรา 7(3) ภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ	ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา 7 (1) (2) และวรรคสอง เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวดหนึ่งและหมวดห้ามีผลใช้บังคับ	(3) และกรรมการตามวรรคสอง เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ และให้รองประธานกรรมการทำหน้าที่ประธานกรรมการเป็นการชั่วคราว ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา 8(1) และกรรมการผู้ทรงคุณวุฒิตามมาตรา 8(4) ภายในเก้าสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ
มาตรา 51 ในวาระเริ่มแรกที่ยังไม่มีเลขาธิการตามพระราชบัญญัตินี้ ให้ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีเลขาธิการตามพระราชบัญญัตินี้ ในกรณีที่ยังไม่มีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคหนึ่ง ให้ผู้ดำรงตำแหน่งผู้อำนายการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนา	**มาตรา 77** ในวาระเริ่มแรก ที่ยังไม่มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ และผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมายด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลที่รัฐมนตรีแต่งตั้ง จำนวนสี่คน เป็นกรรมการ และให้ผู้ปฏิบัติ	**มาตรา 77** ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่า

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
ธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 ปฏิบัติหน้าที่ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และเลขาธิการตามพระราชบัญญัตินี้ เป็นการชั่วคราวจนกว่าจะมีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์หรือเลขาธิการตามพระราชบัญญัตินี้ แล้วแต่กรณี	หน้าที่เลขาธิการตามวรรคสองเป็นเลขานุการของคณะกรรมการกำกับสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยให้ปฏิบัติหน้าที่เป็นการชั่วคราวไปจนกว่าจะมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวดหนึ่งและหมวดห้ามีผลใช้บังคับ ในระหว่างที่ยังไม่มีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งผู้ที่เห็นสมควรให้ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราว จนกว่าจะมีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวดหนึ่งและหมวดห้ามีผลใช้บังคับ	จะมีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ
		<u>มาตรา 78</u> ในวาระเริ่มแรกที่ยังไม่มีการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ให้รัฐมนตรีแต่งตั้งผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือบุคคลใดตามที่รัฐมนตรีเห็นสมควร ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีการแต่งตั้งเลขาธิการ

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		ตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ
		มาตรา 79 ในวาระเริ่มแรก เมื่อได้จัดตั้งสำนักงานแล้วแต่ยังไม่มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ และผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคลที่รัฐมนตรีแต่งตั้ง จำนวนสี่คน เป็น

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		กรรมการ และให้ผู้ปฏิบัติหน้าที่เลขาธิการตามมาตรา 78 เป็นเลขานุการของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยให้ปฏิบัติหน้าที่เป็นการชั่วคราวไปจนกว่าจะมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินหนึ่งร้อยแปดสิบวันนับแต่วันที่บทบัญญัติในหมวด 1 และหมวด 4 มีผลใช้บังคับ
มาตรา 52 ในวาระเริ่มแรกที่ยังไม่มีสำนักงานตามพระราชบัญญัตินี้ ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีสำนักงานตามพระราชบัญญัตินี้		
	มาตรา 78 ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น	**มาตรา 80** ไม่เปลี่ยนแปลง

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
	มาตรา 79 ในวาระเริ่มแรก ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานเป็นพนักงานของสานักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นการชั่วคราว ภายในระยะเวลาที่คณะรัฐมนตรีกาหนดได้	**มาตรา 81** ไม่เปลี่ยนแปลง
	มาตรา 80 ในระหว่างที่ยังมิได้มีการออกประกาศ ระเบียบ หรือข้อบังคับในส่วนที่เกี่ยวข้องกับสำนักงานตามพระราชบัญญัตินี้ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถกำหนดให้นำประกาศ ระเบียบ หรือข้อบังคับขององค์การมหาชนอื่นซึ่งอยู่ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับมาใช้บังคับโดยอนุโลมกับสำนักงานได้ ทั้งนี้ เท่าที่ไม่ขัดหรือแย้งกับพระราชบัญญัตินี้	**มาตรา 82** ในระหว่างที่ยังมิได้มีการออกประกาศ ระเบียบ หรือข้อบังคับในส่วนที่เกี่ยวข้องกับสำนักงานตามพระราชบัญญัตินี้ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถกำหนดให้นำประกาศ ระเบียบ หรือข้อบังคับของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554 หรือของหน่วยงานของรัฐอื่นซึ่งอยู่ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ใช้บังคับอยู่ในวันก่อนวันที่บทบัญญัติใน

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		หมวด 1 และหมวด 4 มีผลใช้บังคับ มาใช้บังคับโดยอนุโลมกับสำนักงานได้ ทั้งนี้ เท่าที่ไม่ขัดหรือแย้งกับพระราชบัญญัตินี้
มาตรา 53 ผู้ใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้อยู่ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ เว้นแต่การปฏิบัติตามมาตรา 29(1) ให้ปฏิบัติตามบทบัญญัติดังกล่าวภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ	**มาตรา 81** ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมที่ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคล และต้องดำเนินการขอ ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวให้เป็นไปตามพระราชบัญญัตินี้ ตามหลักเกณฑ์และระยะเวลาที่กำหนดในกฎกระทรวง ทั้งนี้ ระยะเวลาที่กำหนดไว้ในกฎกระทรวงต้องไม่เกินสามปีนับแต่วันที่พระราชบัญญัตินี้มีผลใช้บังคับ	**มาตรา 83** ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้มีผลใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมที่ ทั้งนี้ ผู้ควบคุมข้อมูลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

ฉบับความมั่นคงดิจิทัล	ฉบับรับฟังความคิดเห็น	ฉบับคณะรัฐมนตรีอนุมัติหลักการ
		มาตรา 84 การดำเนินการออกกฎกระทรวง ประกาศ ระเบียบและข้อบังคับตามพระราชบัญญัตินี้ ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

ประวัติผู้เขียน

ชื่อ	นางสาวเบญญาภา ช่างประดิษฐ์
วันเดือนปีเกิด	24 พฤศจิกายน 2535
วุฒิการศึกษา	ปีการศึกษา 2557: นิติศาสตรบัณฑิต เกียรตินิยมอันดับสอง มหาวิทยาลัยธรรมศาสตร์
ตำแหน่ง	นิติกร ส่วนงานภาษีอากร บริษัท กฎหมายเอสซีจี จำกัด

ผลงานทางวิชาการ

เบญญาภา ช่างประดิษฐ์. “ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต (กฎหมายการค้าระหว่างประเทศ) มหาวิทยาลัยธรรมศาสตร์, 2560

ประสบการณ์ทำงาน	พ.ศ. 2559 – 2560: Tax Consultant บริษัท ที่ปรึกษากฎหมายและภาษีอากร ไพร้ซวอเตอร์เฮาส์คูเปอร์ส จำกัด
	พ.ศ. 2560 – ปัจจุบัน: นิติกร ส่วนงานภาษีอากร บริษัท กฎหมายเอสซีจี จำกัด