ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหว ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในธุรกิจประกันภัย

โดย

ปรารถนา สุวรรณศักดิ์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขาการค้าระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2564

ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

Ref. code: 25646301033624ADV

PROBLEMS OF SENSITIVE PERSONAL DATA PROCESSING REGARDING PERSONAL DATA PROTECTION ACT B.E. 2562 IN INSURANCE BUSINESS

BY

PRATTANA SUWANNASAK

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS

INTERNATIONAL TRADE REGULATIONS

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2021

COPYRIGHT OF THAMMASAT UNIVERSITY

Ref. code: 25646301033624ADV

มหาวิทยาลัยธรรมศาสตร์

คณะนิติศาสตร์

การค้นคว้าอิสระ

ของ

ปรารถนา สุวรรณศักดิ์

เรื่อง

ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหว
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2562 ในธุรกิจประกันภัย

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เมื่อ วันที่ 5 สิงหาคม พ.ศ. 2565

ประธานกรรมการสอบการค้นคว้าอิสระ _____

(อาจารย์อดิศร พิพัฒน์วรพงศ์)

กรรมการและอาจารย์ที่ปรึกษาการค้นคว้าอิสระ _____

(ศาสตราจารย์ ดร. กำชัย จงจักรพันธ์)

คณบดี _____

(รองศาสตรจารย์ ดร. ปกป้อง ศรีสนิท)

หัวข้อการค้นคว้าอิสระ	ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในธุรกิจประกันภัย
ชื่อผู้เขียน	ปรารถนา สุวรรณศักดิ์
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	กฎหมายการค้าระหว่างประเทศ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ	ศาสตราจารย์ ดร. กำชัย จงจักรพันธ์
ปีการศึกษา	2564

บทคัดย่อ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 เป็นกฎหมายที่มีประเด็นปัญหาในการปฏิบัติตามของภาคเอกชนอยู่มาก โดยเฉพาะในภาคธุรกิจที่มีข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ธุรกิจประกันภัย ธุรกิจโรงพยาบาลหรือสถานพยาบาล เป็นต้น ในธุรกิจประกันภัย คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยก็ได้ประกาศแนวปฏิบัติให้ผู้ประกอบธุรกิจประกันชีวิต ผู้ประกอบธุรกิจประกันวินาศภัย รวมถึงตัวแทนประกันภัย และนายหน้าประกันภัย ได้ปฏิบัติตาม

อย่างไรก็ตาม แนวปฏิบัติของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยดังกล่าวมีประเด็นปัญหาในเรื่องปัญหาการตีความที่เป็นที่สงสัยว่าอาจไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกำหนดให้ผู้ประกอบธุรกิจประกันภัย ตัวแทนประกันภัย และนายหน้าประกันภัยสามารถเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อวัตถุประสงค์ในการพิจารณารับประกันภัย พิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทนโดยไม่ต้องขอความยินยอม เพราะถือว่าเป็นการเก็บรวบรวม ใช้ และเปิดเผยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (จ) กล่าวคือ เพื่อการจำเป็นในการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์อันเกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญอันถือได้ว่ายังเป็นการตีความที่อาจไม่ชัดเจนเพียงพอ ถึงแม้ว่าหลักการดังกล่าวจะช่วยให้ผู้รับประกันภัย ผู้เอาประกันภัย และบุคคลที่เกี่ยวข้องในสัญญา

Ref. code: 25646301033624ADV

ประกันภัยมีความสะดวกในการเข้าทำสัญญา ควบคุมต้นทุนของการเกิดสัญญา และบรรลุวัตถุประสงค์ของสัญญาประกันภัยก็ตาม

รายงานฉบับนี้ จึงขอนำเสนอแนวทางการแก้ไขกฎหมายเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

คำสำคัญ: ข้อมูลส่วนบุคคลที่มีความอ่อนไหว, ข้อมูลสุขภาพ, การประกันภัย, การประกันชีวิต, การประกันสุขภาพ, ข้อมูลส่วนบุคคล

Ref. code: 25646301033624ADV

Dissertation Title	PROBLEMS OF SENSITIVE PERSONAL DATA PROCESSING REGARDING PERSONAL DATA PROTECTION ACT B.E. 2562 IN INSURANCE BUSINESS
Author	Prattana Suwannasak
Degree	Master of Laws
Major Field/Faculty/University	International Trade Regulations Law Thammasat University
Dissertation Advisor	Professor Dr. Kumchai Jongjakapun
Academic Year	2021

ABSTRACT

Thailand's Personal Data Protection Act B.E. 2562 came into effect on June 1st, 2022. This law encounters many compliance issues in the private sector, especially the sector using sensitive personal data, such as insurance and hospital businesses. For the insurance business, the Office of Insurance Commission has announced a guideline to comply with the Personal Data Protection Act B.E. 2562 for all insurers, insurance agents and insurance brokers.

However, there are still legal interpretation problems with the Office of Insurance Commission guidelines. Such guidelines determine that the insurers, insurance agents and insurance brokers can collect, use and disclose sensitive personal data for insurance underwriting, reinsurance underwriting, calculating insurance premiums, denial of insurance, and insurance claims without personal data consent. Because it deems to collect, use and disclose under the Personal Data Protection Act B.E. 2562, Section 26 (5) (e), that is, for the necessity of law enforcement to achieve the objectives involving public interests. Nonetheless, it remains unclear to be one of the public interests, even though this helps the insurer and all related parties of

Ref. code: 25646301033624ADV

the insurance contract make an insurance contract easier, control the contract formation cost and accomplish its objectives of the insurance contract.

This report will suggest the guidelines for amending the law to be in line with the Personal Data Protection Act B.E. 2562.

Keywords: Sensitive Data, Insurance, Life Insurance, Health Insurance, Personal Data, GDPR

Ref. code: 25646301033624ADV

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงลงได้ด้วยความกรุณาจากบุคคลผู้มีพระคุณหลายท่านที่ให้ความช่วยเหลือ ให้คำปรึกษา และความคิดเห็นทางวิชาการอันเป็นประโยชน์อย่างยิ่ง ผู้เขียนต้องขอขอบพระคุณทุกท่านมา ณ ที่นี้

ผู้เขียนขอขอบพระคุณ ศาสตราจารย์ ดร. กำชัย จงจักรพันธ์ กรรมการและอาจารย์ที่ปรึกษาการค้นคว้าอิสระฉบับนี้ ที่ได้สละเวลาอันมีค่ารับเป็นอาจารย์ที่ปรึกษาตลอดจนให้คำชี้แนะทั้งความเห็นทางวิชาการ และการปรับปรุงการเขียนรายงานการค้นคว้าอิสระฉบับนี้ และขอขอบพระคุณอาจารย์อดิศร พิพัฒน์วรพงศ์ กรรมการสอบการค้นคว้าอิสระเป็นอย่างสูงที่สละเวลาอันมีค่ากรุณามาเป็นกรรมการสอบการค้นคว้าอิสระและให้ข้อชี้แนะอันเป็นประโยชน์ต่อความสมบูรณ์ของการค้นคว้าอิสระนี้

สุดท้ายนี้ ผู้เขียนขอขอบพระคุณทุกท่านที่ให้ความช่วยเหลือสำหรับการค้นคว้าอิสระครั้งนี้ของผู้เขียน โดยเฉพาะบุคลากรในภาคธุรกิจประกันภัย ผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ให้สัมภาษณ์ ที่ให้ความคิดเห็น มุมมอง ตลอดจนตรวจสอบความถูกต้องสมบูรณ์ของการค้นคว้าอิสระในครั้งนี้ หากการค้นคว้าอิสระในครั้งนี้ มีข้อบกพร่องประการใด ผู้เขียนต้องกราบขออภัยมา ณ ทีนี้ และขอน้อมรับข้อบกพร่องทั้งหลายไว้แต่เพียงผู้เดียว

ปรารถนา สุวรรณศักดิ์

Ref. code: 25646301033624ADV

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	(1)
บทคัดย่อภาษาอังกฤษ	(3)
กิตติกรรมประกาศ	(5)
สารบัญตาราง	(12)
สารบัญภาพ	(11)
รายการสัญลักษณ์และคำย่อ	(13)
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ในการศึกษา	5
1.3 สมมติฐานในการศึกษา	6
1.4 ขอบเขตของการศึกษา	6
1.5 วิธีการศึกษา	7
1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา	7
บทที่ 2 ข้อมูลที่เกี่ยวข้องและปัญหาการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในธุรกิจประกันภัย	8
2.1 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)	8
2.1.1 เชื้อชาติหรือเผ่าพันธุ์ (racial or ethnic origin)	10
2.1.2 ความคิดเห็นทางการเมือง (political opinions)	12

Ref. code: 25646301033624ADV

2.1.3 ความเชื่อในลัทธิ ศาสนา หรือปรัชญา (religious or philosophical beliefs) 13
2.1.4 พฤติกรรมทางเพศ (person's sex life or sexual orientation) 15
2.1.5 ประวัติอาชญากรรม (criminal records) 16
2.1.6 ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต (Data concerning Health) 18
2.1.7 ข้อมูลสหภาพแรงงาน (trade union membership) 19
2.1.8 ข้อมูลพันธุกรรม (genetic data) 20
2.1.9 ข้อมูลชีวภาพ (biometric data) 20
2.1.10 ข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด 21
2.2 แนวทางการจัดการกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 21
2.3 ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัย 27
2.3.1 การขอความยินยอมในการเปิดเผยข้อมูลสุขภาพก่อนการทำสัญญาประกันชีวิตหรือประกันสุขภาพ 29
2.3.2 การให้ข้อมูลสุขภาพ ประวัติการรักษาพยาบาล เพื่อเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัย 29
2.3.3 การดำเนินการทำประกันภัยที่ต้องเปิดเผยข้อมูลสุขภาพของเจ้าของข้อมูลส่วนบุคคลผ่านนายหน้าประกันภัย 31
2.3.4 การทำประกันชีวิตและประกันสุขภาพ ประเภทการทำประกันภัยแบบกลุ่ม 32
2.3.5 ปัญหาการให้ความยินยอมที่มากเกินความจำเป็น 32

บทที่ 3 วิเคราะห์กฎหมาย แนวทางการกำกับดูแล และแนวปฏิบัติในประเทศไทย 34

3.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2561 34
3.2 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 36

Ref. code: 25646301033624ADV

3.3 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 44
3.4 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guideline 3.0) 50
3.5 แนวปฏิบัติของภาคธุรกิจประกันภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 54
3.5.1 แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติ\คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 54
3.5.2 แนวปฏิบัติของภาคธุรกิจประกันชีวิตตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 55
3.6 ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. 55
3.7 ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. 58

บทที่ 4 วิเคราะห์และอภิปรายกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างประเทศ 60

4.1 GENERAL DATA PROTECTION REGULATION (GDPR) and Recital 60
4.1.1 GENERAL DATA PROECTION REGULATION (GDPR) 60
4.1.2 ความแตกต่างของ GDPR ข้อ 9 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 62
4.1.3 GDPR recitals and articles 63
4.1.4 ตัวอย่างแนวทางจัดการข้อมูลสุขภาพในสหภาพยุโรป 65
4.2 Data Protection Act 2018 68
4.3 Personal Data Protection Act 2012 70
4.4 กรณีศึกษาการใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัย 72

Ref. code: 25646301033624ADV

4.4.1 กรณีการเก็บ ใช้ เปิดเผยข้อมูลสุขภาพสำหรับการเรียกร้องค่าสินไหมทดแทน 72

4.4.2 กรณีการเก็บข้อมูลเกินเวลาที่กำหนดไว้ และการบันทึกเสียงสำหรับโทรศัพท์โดยไม่แจ้งสิทธิ 73

บทที่ 5 บทสรุปและข้อเสนอแนะ 75

5.1 บทสรุป 75

5.2 ข้อเสนอแนะ 77

Ref. code: 25646301033624ADV

บรรณานุกรม 82

ภาคผนวก

ภาคผนวก ก GDPR recitals and articles 91
ภาคผนวก ข Data Protection Act 2018 190
ภาคผนวก ค PERSONAL DATA PROTECTION ACT 2012 399
ภาคผนวก ง บันทึกการสัมภาษณ์ คุณสุวรรณโชติ ศิริมหาศาล 486
ภาคผนวก จ บันทึกการสัมภาษณ์ คุณรุ่งเรือง สัมฤทธิ์ทรัพย์ 489
ภาคผนวก ฉ ผลสำรวจการตอบแบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 491

ประวัติผู้เขียน 496

Ref. code: 25646301033624ADV

สารบัญตาราง

ตารางที่ หน้า

2.1 ตารางเปรียบเทียบความยินยอมโดยทั่วไป และความยินยอมโดยชัดแจ้ง 25

Ref. code: 25646301033624ADV

สารบัญภาพ

ภาพที่ หน้า

3.1 ส่วนที่ 6 ของใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม ชนิดมีคำถามสุขภาพอย่างสั้น 44

3.2 ใบคำขอเอาประกันภัย กรมธรรม์ประกันภัยสุขภาพเฉพาะโรค แบบส่วนบุคคล หน้าที่ 1 46

3.3 ใบคำขอเอาประกันภัย กรมธรรม์ประกันภัยสุขภาพเฉพาะโรค แบบส่วนบุคคล หน้าที่ 2 47

Ref. code: 25646301033624ADV

รายการสัญลักษณ์และคำย่อ

สัญลักษณ์/คำย่อ	คำเต็ม/คำจำกัดความ
GDPR	GENERAL DATA PROTECTION REGULATION
BDSG	Bundesdatenshutzgesetz

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 ราชกิจจานุเบกษาได้ประกาศพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ .ศ. 2562 อันมีวัตถุประสงค์เพื่อควบคุมการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลสำหรับกิจการต่าง ๆ ทั้งในภาครัฐและภาคเอกชน และกำหนดให้ภาครัฐและภาคเอกชนที่มีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลต้องมีมาตรการป้องกันและเยียวยาเจ้าของข้อมูลส่วนบุคคลที่ถูกทำละเมิดอย่างเหมาะสม โดยพระราชบัญญัติดังกล่าวกำหนดให้มีผลบังคับใช้ครบทุกมาตราเมื่อพ้นกำหนดหนึ่งปีนับแต่วันที่ประกาศในราชกิจจานุเบกษา[1] อย่างไรก็ตาม เมื่อล่วงพ้นระยะเวลาจนใกล้ครบกำหนดดังกล่าว ราชกิจจานุเบกษาได้ประกาศพระราชกฤษฎีกาเลื่อนการบังคับใช้พระราชบัญญัติออกไป และกำหนดให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ. 2564 แทน[2] หลังจากนั้น วันที่ 8 พฤษภาคม พ.ศ. 2564 ราชกิจจานุเบกษาได้มีประกาศพระราชกฤษฎีกาอีกหนึ่งฉบับเพื่อขยายเวลาการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกไปอีกครั้ง โดยให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ. 2565 เป็นต้นไป[3] เนื่องจากกลุ่มสมาคมและภาคธุรกิจต่างๆ ได้ยื่นข้อร้องเรียนไปยังนายกรัฐมนตรีว่า ภาคธุรกิจต่างๆ ในประเทศไทยยังขาดความพร้อมในการดำเนินการตามกฎหมายตามระยะเวลาที่ควรจะเป็น เพราะได้รับผลกระทบจากวิกฤติการแพร่ระบาดของไวรัสโควิด-19[4] จึงขอให้มีการเลื่อนการบังคับใช้กฎหมายออกไป

สำหรับภาครัฐนั้น การคุ้มครองข้อมูลส่วนบุคคลเริ่มปรากฏอยู่ในกฎหมายตั้งแต่ปี พ.ศ. 2540 คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อันมีผลบังคับใช้ตั้งแต่เดือนธันวาคม 2540 เป็นต้นมา แต่สำหรับภาคเอกชนที่ประกอบธุรกิจในประเทศไทยไม่เคยมีกฎหมายใด

---

[1] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

[2] พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563.

[3] พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564.

[4] ‘เลื่อนบังคับใช้ พ.ร.บ.ข้อมูลส่วนบุคคล’ ไทยรัฐฉบับพิมพ์ (20 พฤษภาคม 2563) <https://www.thairath.co.th/business/economics/1848624> สืบค้นเมื่อวันที่ 15 ธันวาคม 2564.

Ref. code: 25646301033624ADV

กำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า พนักงาน หรือผู้ที่มาติดต่อมาก่อน เว้นแต่ภาคธุรกิจที่มีหน่วยงานกำกับดูแลเป็นการเฉพาะ ซึ่งมีประกาศเพื่อกำกับดูแลภายในภาคธุรกิจเท่านั้น เช่น ในภาคธุรกิจสถาบันการเงิน และผู้ประกอบธุรกิจที่มิใช่สถาบันการเงินซึ่งอยู่ภายใต้การกำกับของธนาคารแห่งประเทศไทย มีการกำหนดแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ในประกาศธนาคารแห่งประเทศไทย เรื่อง การบริการจัดการด้านการให้บริการลูกค้าอย่างเป็นธรรม (Market Conduct)[5] และในภาคธุรกิจประกันภัย คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย มีประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง กำหนดหลักเกณฑ์วิธีการออก การเสนอขายกรมธรรม์ประกันภัยและการปฏิบัติหน้าที่ของตัวแทนประกันชีวิต นายหน้าประกันชีวิต และธนาคาร พ.ศ. 2551[6] เป็นต้น

นอกจากนี้ การคุ้มครองข้อมูลส่วนบุคคลยังเป็นประเด็นสำคัญในเรื่องความสัมพันธ์ระหว่างประเทศ เนื่องจากสหภาพยุโรปไม่อนุญาตให้มีการส่งข้อมูลข่าวสารไปยังประเทศที่ไม่มีกฎหมาย หรือมาตรการคุ้มครองข้อมูลส่วนบุคคลในมาตรฐานที่ยอมรับได้ ตามข้อบังคับว่าด้วยการถ่ายทอดข้อมูล ซึ่งก็มิได้มีเพียงประเทศในสหภาพยุโรปเท่านั้นที่มีนโยบายเช่นนี้[7] นานาประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างก็มีข้อบังคับหรือกฎหมายเป็นอย่างเดียวกัน แม้ว่าประเทศไทยและนานาประเทศจะมี General Data Protection Regulation หรือ GDPR เป็นกฎหมายแม่แบบเพื่อประโยชน์ในการได้รับการถ่ายทอดข้อมูลต่างๆ จากสหภาพยุโรปก็ตาม ก็มิได้หมายความว่าไม่มีประเทศใดที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างจากข้อบังคับดังกล่าว แต่ยังคงยึดหลักเดียวกันคือการคุ้มครองข้อมูลส่วนบุคคลของบุคคลธรรมดา ยกตัวอย่างเช่น กฎหมายคุ้มครอง

---

[5] ประกาศธนาคารแห่งประเทศไทย ที่ สกส2. 4/2563 เรื่อง การบริหารจัดการด้านการให้บริการลูกค้าอย่างเป็นธรรม (Market Conduct) เอกสารแนบ 6 มาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลลูกค้า (Data Privacy).

[6] ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง กำหนดหลักเกณฑ์วิธีการออก การเสนอขายกรมธรรม์ประกันภัยและการปฏิบัติหน้าที่ของตัวแทนประกันชีวิต นายหน้าประกันชีวิต และธนาคาร พ.ศ. 2551 ข้อ 11.2 ข้อ11.3 และ ข้อ 12.2 (4).

[7] นคร เสรีรักษ์, *ความเป็นส่วนตัว* (พิมพ์ครั้งที่ 2, บริษัท พี.เพรส จำกัด 2563) 21-23.

Ref. code: 25646301033624ADV

ข้อมูลส่วนบุคคลในประเทศมาเลเซีย[8] และกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์[9] เป็นต้น ทั้งนี้ การปรับตัวของภาคธุรกิจในประเทศไทยให้เป็นไปตามทิศทางใหม่ของโลกเรื่องการคุ้มครองข้อมูลส่วนบุคคลมีต้นทุนที่ค่อนข้างสูง เพราะขาดความชัดเจนในแนวปฏิบัติจากภาครัฐ และขาดบุคลากรผู้มีความรู้เฉพาะทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ภาคเอกชนจึงต้องจ้างที่ปรึกษาภายนอกที่มีความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลมาช่วยจัดการให้มีการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งภาคธุรกิจประกันภัยทั้งบริษัทรับประกันภัย นายหน้าประกันภัย และผู้ประกอบธุรกิจที่เกี่ยวข้องที่ต้องดำเนินการตามกฎหมายในฐานะผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลเพื่อการประกันภัยนั้น นอกจากปัญหาหรือผลกระทบเชิงลบแล้ว บุคลากรในภาคธุรกิจประกันภัยยังมีความเห็นว่าการที่ภาคธุรกิจปรับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น จะทำให้ภาคธุรกิจเพิ่มขีดความสามารถในการแข่งขันกับตลาดโลก และขยายฐานลูกค้าครอบคลุมไปถึงลูกค้าในต่างประเทศได้ โดยเฉพาะอย่างยิ่งในกลุ่มประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานสูง เช่น สหภาพยุโรป หรือ สิงคโปร์ จึงอาจกล่าวได้ว่าการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนั้น มีผลกระทบทั้งในเชิงบวกและเชิงลบต่อภาพรวมธุรกิจ[10]

ผู้เขียนเล็งเห็นถึงปัญหาการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับภาคธุรกิจประกันภัย และจากการศึกษาข้อมูลพบว่าในธุรกิจประกันภัย มีปัญหาการจัดเก็บ การทำซ้ำ การประมวลผลและการเปิดเผยข้อมูลส่วนบุคคล ทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหวอยู่หลายประเด็น ซึ่งบริษัทประกันภัย คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) สมาคมประกันชีวิตไทยและสมาคมประกันวินาศภัยไทย เล็งเห็นถึงปัญหาการปฏิบัติตามกฎหมายฉบับนี้ จึงมีการออกประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับ

---

[8] Noriswadi Ismal, *Understanding Personal Data Protection Law* (Percetakan Jiwabaru Sdn Bhd).

[9] Robert Walters and others, *Data Protection Law, A Comparative Analysis of Asia-Pacific and European Approaches* (Markono Print Media Pte Ltd, 2019) 84-85.

[10] สุวเพ็ญ ค้ำจุน. 'ผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีต่ออุตสาหกรรมประกันภัยในประเทศไทย' (การค้นคว้าอิสระ บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2563) 80.

Ref. code: 25646301033624ADV

ธุรกิจประกันวินาศภัย พ.ศ. 2564 ที่มีเนื้อหาเป็นแนวทางการตีความพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับภาคธุรกิจประกันภัย ตั้งแต่วันที่ 28 ธันวาคม พ.ศ. 2564 เพื่อเป็นประโยชน์ต่อบริษัทประกันภัย ตัวแทนประกันภัย และนายหน้าประกันภัยในการปฏิบัติตามกฎหมายดังกล่าว แต่ประกาศดังกล่าวมีเนื้อหาที่นอกเหนือขอบเขตของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเมื่อพิจารณาแล้ว มีข้อสงสัยว่าเป็นการยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แก่ภาคธุรกิจประกันภัยในข้อใดข้อหนึ่งหรือไม่ นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ยังมิได้มีการประกาศกฎหมายลำดับรองที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือการจัดการที่เกี่ยวข้อง ปัจจุบัน (วันที่ 22 กรกฎาคม 2565) มีเพียงร่างกฎหมายลำดับรองที่เกี่ยวข้องคือ ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. .... และร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. .... เท่านั้น ซึ่งพระราชบัญญัติดังกล่าวมิได้ให้อำนาจหน่วยงานกำกับดูแลอื่นประกาศแนวปฏิบัติที่มีความแตกต่างจากกฎหมายบางส่วนหรือทั้งหมดโดยที่มิได้ตราเป็นพระราชกฤษฎีกา[11] อย่างไรก็ตาม ผู้เขียนมีความเห็นว่าสัญญาประกันภัยนั้นเป็นไปเพื่อบริหารความเสี่ยง และบรรเทาความเสียหายของผู้เอาประกันภัยเมื่อเกิดภัยขึ้น การก่อให้เกิดสัญญาดังกล่าวจึงควรมีลักษณะเป็นสัญญาที่เกิดขึ้นได้โดยง่าย และมีข้อมูลที่จำเป็น ถูกต้องครบถ้วนตามหลักสุจริตอย่างยิ่งในการทำสัญญาประกันภัย[12] และไม่สร้างต้นทุนที่สูงเกินไปจนทำให้ผู้เอาประกันภัยต้องจ่ายเบี้ยประกันภัยที่แพงจนเกินไป แต่ด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลสุขภาพซึ่งเป็นปัจจัยสำคัญของการประกอบธุรกิจประกันภัย และเป็นประโยชน์ต่อการปฏิบัติตามสัญญาประกันภัยนั้น ต้องขอความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง[13] อันรวมถึงการจัดให้มีกระบวนการในการบริหารจัดการการขอความยินยอมนั้นด้วย เป็นการก่อให้เกิดปัญหาในการดำเนินงานแก่ธุรกิจประกันภัย ทั้งด้านการบริหารจัดการที่ปราศจากความจำเป็น การสร้างต้นทุนเพิ่มเติมที่อาจกระทบต่อเบี้ยประกันภัย การขอความยินยอมที่ไม่สมเหตุสมผล เนื่องจากบริษัทที่รับประกันภัยย่อมไม่สามารถพิจารณารับประกันภัยได้โดยมิได้รู้ถึง

---

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 วรรคสอง.

[12] 'UTMOST GOOD FAITH' (เว็บไซต์คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย) <https://www.oic.or.th/th/node/27334> สืบค้นเมื่อวันที่ 18 ธันวาคม 2564.

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26.

Ref. code: 25646301033624ADV

ความเสี่ยงของผู้เอาประกันภัย และหากไม่มีข้อมูลดังกล่าวก็ไม่อาจก่อเกิดสัญญาประกันภัยหรือปฏิบัติตามสัญญาประกันภัยได้[14] และประการสำคัญอีกข้อหนึ่งคือการดำเนินการขอความยินยอมและเปิดโอกาสให้มีการถอนความยินยอมนั้นอาจเป็นอุปสรรคสำคัญในการเกิดสัญญาประกันภัยอีกด้วย

1.2 วัตถุประสงค์ในการศึกษา

เพื่อศึกษาปัญหาการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ของผู้ประกอบธุรกิจที่เกี่ยวข้องกับการรับประกันภัยที่ได้รับอนุญาตอย่างถูกต้องจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ได้แก่ ผู้ประกอบธุรกิจรับประกันภัย ตัวแทนประกันภัย นายหน้าประกันภัย ผู้ประเมินวินาศภัย หรือผู้ที่ทำหน้าที่สนับสนุนงานให้แก่บริษัทประกันภัยซึ่งได้รับอนุญาตจากเลขาธิการคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เช่น การชดใช้ค่าสินไหมทดแทนในนามบริษัทสำหรับการประกันอุบัติเหตุ การประกันสุขภาพ หรือการประกันภัยการเดินทางในต่างประเทศ โดยมีการให้ความเห็นเบื้องต้น[15] เป็นต้น นอกจากนี้ ยังพิจารณาไปถึงปัญหาการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ถูกหยิบยกขึ้นมาปรึกษาในสมาคมที่เกี่ยวข้องกับการประกันภัย รวมถึง หลักเกณฑ์ต่างๆ ของหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคล และหน่วยงานกำกับดูแลธุรกิจประกันภัย โดยศึกษาถึงเจตนารมณ์ของกฎหมาย ศึกษาเปรียบเทียบกับกฎหมายแม่แบบของต่างประเทศ กฎหมาย

---

[14] กิตติศักดิ์ จันเส, 'มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต' <http://www.research.rmutt.ac.th/wp-content/uploads/2012/05/%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%83%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5.pdf> สืบค้นเมื่อวันที่ 8 พฤษภาคม 2565.

[15] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวทางปฏิบัติในการใช้บริหารจากบุคคลภายนอก (Outsourcing) ขิงบริษัทประกันภัย ข้อ 3.

Ref. code: 25646301033624ADV

ที่ใกล้เคียง และวิธีปฏิบัติของต่างประเทศในเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับการประกันภัย เพื่อใช้เป็นแนวทางลดปัญหาการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันภัยได้

1.3 สมมติฐานในการศึกษา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขาดความชัดเจนและก่อให้เกิดอุปสรรคในการปฏิบัติตามกฎหมายของภาคเอกชน โดยเฉพาะอย่างยิ่งในกลุ่มผู้ประกอบธุรกิจเกี่ยวกับการประกันภัย จึงมีความจำเป็นต้องศึกษาประเด็นทางกฎหมาย เพื่อปรับปรุง แก้ไข ปัญหาการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันภัยก่อนการบังคับใช้จริง รวมถึงการออกกฎหมายหรือแนวทางการกำกับดูแลเพิ่มเติม เพื่อให้เกิดการปฏิบัติตามกฎหมายได้จริง ส่งผลให้เกิดประโยชน์สูงสุดตามวัตถุประสงค์ของกฎหมาย และเป็นไปตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เป็นสากล

1.4 ขอบเขตของการศึกษา

รายงานฉบับนี้มุ่งศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ที่เกี่ยวข้องของหน่วยงานกำกับดูแล โดยเฉพาะกฎเกณฑ์ของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย รวมถึง กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ แนวปฏิบัติและเอกสารที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย แนวปฏิบัติของต่างประเทศในการใช้ข้อมูลส่วนบุคคลในธุรกิจประกันภัย ซึ่งกฎหมายที่จะดำเนินการศึกษา ได้แก่

1.4.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และร่างกฎหมายลำดับรองที่เกี่ยวข้อง

1.4.2 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันวินาศภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564

1.4.3 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันวินาศภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

1.4.4 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 3.0 และแนวปฏิบัติของสมาคมที่เกี่ยวข้อง

Ref. code: 25646301033624ADV

1.4.5 General Data Protection Regulation (GDPR)

1.4.6 Data Protection Act 2018

1.4.7 Personal Data Protection Act 2012

อย่างไรก็ตาม การศึกษาในหัวข้อรายงานฉบับนี้ จำกัดการศึกษาเพียงกฎหมายที่เกี่ยวข้องทั้งภายในและภายนอกประเทศ ประกอบกับแนวทางการแก้ปัญหา หรือแนวปฏิบัติของต่างประเทศในภาคธุรกิจประกันภัย เพื่อหาแนวทางการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 อย่างมีประสิทธิภาพ ไม่ก่อภาระในการทำธุรกรรมหรือการทำสัญญาประกันภัยแก่ผู้บริโภคและภาคธุรกิจโดยไม่จำเป็น และเป็นไปตามมาตรฐานสากล

1.5 วิธีการศึกษา

การศึกษาใช้วิธีการค้นคว้าและรวบรวมข้อมูลแบบศึกษาโดยเอกสาร (Documentary Research) โดยผู้เขียนมุ่งเน้นการศึกษา วิเคราะห์ และรวบรวมข้อมูลจากปัญหาที่เกิดขึ้นจริงในการปฏิบัติงานในภาคธุรกิจประกันภัย และวิเคราะห์ถึงวัตถุประสงค์ในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล เปรียบเทียบกับความจำเป็นในการใช้ข้อมูลส่วนบุคคลเพื่อประกอบธุรกิจ รวมถึงแนวปฏิบัติและความเห็นของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) การศึกษานี้ไม่จำกัดเพียงตัวบทกฎหมาย แต่รวมถึง บทความ ข้อมูลบนเว็บไซต์และสื่ออิเล็กทรอนิกส์ต่าง ๆ ข้อมูลจากผู้ประกอบการ และข่าวสารที่เป็นข้อมูลที่เกี่ยวข้องทั้งหมด

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

การศึกษาจะเป็นประโยชน์ต่อบุคคลและองค์กรที่เกี่ยวข้อง ให้สามารถศึกษาและทำความเข้าใจ เพื่อเตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้นจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทั้งในแง่ของภาระในการประกอบธุรกิจ และผลกระทบหากปฏิบัติไม่ครบถ้วนถูกต้องหรือละเว้นการปฏิบัติ อีกทั้งเป็นข้อมูลให้หน่วยงานกำกับดูแลได้ทราบถึงผลกระทบ และปัญหาในการปฏิบัติตามกฎหมายที่ไม่ก่อประโยชน์ให้ทั้งผู้ประกอบธุรกิจ ผู้ประกอบอาชีพที่เกี่ยวข้องและผู้บริโภค นอกจากนี้ การศึกษาในครั้งนี้อาจเป็นแนวทางสำหรับการแก้ไขปรับปรุงกฎหมายออกแนวปฏิบัติ หรือคำอธิบายกฎหมายให้เหมาะสมครอบคลุมกับบริบทที่อาจเกิดปัญหา สอดคล้องกับสภาพปัญหา และก่อให้เกิดประโยชน์สูงสุดแก่การประกอบธุรกิจที่สอดคล้องกับกฎหมายอย่างมีประสิทธิภาพและประสิทธิผล

Ref. code: 25646301033624ADV

บทที่ 2
ข้อมูลที่เกี่ยวข้องและปัญหาการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในธุรกิจประกันภัย

เนื่องจากการศึกษาในหัวข้อนี้ เน้นศึกษาการบริหารจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นหลัก ก่อนจะชี้ให้เห็นถึงประเด็นปัญหาที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เขียนขอเริ่มด้วยการอภิปรายถึงความหมายของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) และความแตกต่างระหว่างข้อมูลส่วนบุคคลที่มีความอ่อนไหวและข้อมูลส่วนบุคคลทั่วไป ดังต่อไปนี้

2.1 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)

ข้อมูลส่วนบุคคล หมายความว่าข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[1] ข้อมูลที่ระบุถึงตัวบุคคลได้ทางตรงคือข้อมูลส่วนบุคคลที่สามารถระบุถึงตัวบุคคลได้โดยไม่จำเป็นต้องอาศัยข้อมูลอื่นๆ เช่น ชื่อ-นามสกุล ลายนิ้วมือ หรือเลขบัตรประจำตัวประชาชน เป็นต้น ส่วนข้อมูลส่วนบุคคลที่ระบุถึงตัวบุคคลได้ทางอ้อม คือข้อมูลที่อาจระบุถึงตัวบุคคลได้เมื่อประกอบกับข้อมูลอื่น และข้อมูลส่วนบุคคลนั้นถูกระบุในสภาพแวดล้อมที่มีวงจำกัดเพียงพอที่จะคาดหมายได้ว่าผู้ใดเป็นเจ้าของข้อมูลส่วนบุคคล เช่น การใช้รหัสไปรษณีย์และวันเกิดประกอบกันเพื่อระบุตัวบุคคลในบัญชีผู้มีสิทธิเลือกตั้ง[2] เป็นต้น ข้อมูลส่วนบุคคลนั้น ถือเป็นสิทธิอย่างหนึ่งซึ่งได้รับการพัฒนาจากสิทธิในชีวิต ร่างกาย ทรัพย์สินและเสรีภาพ โดยขอบเขตในสิทธิข้อมูลส่วนบุคคลนั้น ครอบคลุมไปถึงความคิด ทัศนคติ ความเชื่อถือของบุคคล ซึ่งในเชิงองค์ประกอบนั้น ข้อมูลส่วนบุคคลแบ่งออกเป็น 2 ประเภท ได้แก่ ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ ที่อยู่ สถานที่ทำงาน วันเดือนปีเกิด เป็นต้น และข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น เชื้อชาติ ศาสนา ความเชื่อ พฤติกรรมทางเพศ ความคิดเห็นทาง

---

[1] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6.

[2] ปิยะบุตร บุญอร่ามเรือง และคณะ, ‘แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 3.0)’ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) 40 <https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf> สืบค้นเมื่อวันที่ 2 มิถุนายน 2565.

Ref. code: 25646301033624ADV

การเมือง รวมถึงข้อมูลสุขภาพ ซึ่งข้อมูลเหล่านี้ หากถูกละเมิดหรือล่วงรู้อาจทำให้เจ้าของข้อมูลได้รับความเสื่อมเสีย เดือดร้อน หรือเป็นอันตรายต่อชีวิต ร่างกาย ทรัพย์สินหรือเสรีภาพ[3] ได้

ในประเทศไทยนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีข้อกำหนดอันเป็นคำนิยาม คำว่า “ข้อมูลส่วนบุคคล” ไว้ แต่มิได้ให้คำนิยามคำว่าข้อมูลส่วนบุคคลที่มีความอ่อนไหวไว้ อย่างไรก็ตาม มีการบัญญัติเรื่องการจัดการกับข้อมูลชนิดพิเศษ ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด[4] โดยบัญญัติให้มีความเข้มงวดในการบริหารจัดการเพื่อ เก็บ ใช้ และเปิดเผยมากกว่าข้อมูลส่วนบุคคลทั่วไป เช่น การเก็บ ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวไม่อาจอ้างฐานสัญญาได้ และการขอความยินยอมสำหรับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นต้องกระทำโดยชัดแจ้ง เป็นต้น ทั้งนี้ในรายละเอียดของมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เข้มงวดกว่านั้น ผู้เขียนจะได้อภิปรายในส่วนถัดไป ซึ่งการกำหนดมาตรการเช่นนี้ก็เป็นการกำหนดตามกฎหมายแม่แบบ กล่าวคือ GENERAL DATA PROTECTION REGULATION (GDPR) ข้อ 9 ของสหภาพยุโรป ซึ่งแม้กฎหมายทั้งสองฉบับจะไม่มีคำว่าข้อมูลส่วนบุคคลที่มีความอ่อนไหว หรือ Sensitive Data แต่หนังสือ แนวปฏิบัติ และคำแนะนำต่างๆ ในอินเทอร์เน็ตนั้น มักใช้คำดังกล่าวแทนข้อมูลชนิดพิเศษตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือคำว่า “special categories of personal data” ในข้อ 9 ของ GDPR[5]

ข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น หากพิจารณาจากตัวอย่างที่กฎหมายข้างต้นได้ยกมาแล้ว อาจกล่าวได้ว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือ ข้อมูลส่วนบุคคลที่มีความเสี่ยงในการถูกนำไปใช้เพื่อก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป

---

[3] นคร เสรีรักษ์, *ความเป็นส่วนตัว* (พิมพ์ครั้งที่ 2, บริษัท พี.เพรส จำกัด 2563) 98-101.

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26.

[5] Luke Irwin, ‘The GDPR: What is sensitive personal data?’ (it governance, 3 December 2020) <https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data> สืบค้นเมื่อวันที่ 2 มิถุนายน 2565.

Ref. code: 25646301033624ADV

โดยเฉพาะอย่างยิ่งการนำข้อมูลมาใช้เพื่อเลือกปฏิบัติต่อเจ้าของข้อมูลส่วนบุคคลจนทำให้เกิดความไม่เป็นธรรมขึ้น จึงทำให้ต้องใช้ความระมัดระวังในการเก็บ ใช้ และเปิดเผยเป็นพิเศษ[6]

นอกจากนี้ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถือเป็นข้อมูลส่วนตัวที่ปกติ มิได้มีการเปิดเผยให้กับบุคคลอื่นทราบ เพราะหากข้อมูลดังกล่าวถูกเปิดเผยอาจกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เช่น เสรีภาพทางความคิด ความเชื่อ และศาสนา เสรีภาพในการแสดงออกถึงความเป็นตัวตนของเจ้าของข้อมูล เสรีภาพในการรวมกลุ่มของผู้ที่มีความคิดเช่นเดียวกัน สิทธิในร่างกายของตนโดยแท้จริง สิทธิในเรื่องส่วนตัวโดยเฉพาะเรื่องชีวิตครอบครัว หรือสิทธิเท่าเทียมที่จะไม่ถูกเลือกปฏิบัติ เป็นต้น[7]

แม้ในกฎหมายไทยยังไม่มีการตีความอย่างเป็นทางการถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ในภาคการศึกษาและหน่วยงานภาคเอกชนได้มีการจัดทำแนวปฏิบัติ การจัดสัมมนาจำนวนมากที่กล่าวถึงการตีความข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอ้างอิงจากกฎหมาย GDPR ของสหภาพยุโรป ซึ่งผู้เขียนได้รวบรวมการตีความข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และนำมาอภิปรายได้ ดังนี้

2.1.1 เชื้อชาติหรือเผ่าพันธุ์ (racial or ethnic origin)

หมายความรวมถึง ชื่อที่มีลักษณะบ่งเฉพาะถึงเชื้อชาติหรือเผ่าพันธุ์ ภาษาท้องถิ่นที่ใช้ เชื้อสาย ชื่อของบิดามารดาที่มีลักษณะเฉพาะ และสถานที่เกิดซึ่งอาจนำไปสู่การตีความถึงเชื้อชาติหรือเผ่าพันธุ์ของเจ้าของข้อมูลส่วนบุคคลได้[8] ทั้งนี้ คำว่า เชื้อชาติหรือเผ่าพันธุ์นั้น เป็นคำที่ยังมีความหมายแตกต่างหลากหลายอยู่ในแต่ละประเทศ เช่น ในประเทศฝรั่งเศส คำว่า เชื้อชาติและเผ่าพันธุ์มีความหมายเหมือนกัน แต่ในประเทศอังกฤษมีการแยกคำศัพท์ทั้งสองคำนี้ออกจากกันโดยอ้างอิงจากข้อพิพาททางกฎหมายภายในของประเทศอังกฤษ นอกจากนี้ ส่วนอื่นๆ ของสหภาพยุโรป

---

[6] ปิยะบุตร บุญอร่ามเรือง และคณะ (เชิงอรรถ 2) 22.

[7] 'Why is this data special?' (Information Commissioner's Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

[8] Sanjay Sharma, *Data Privacy and GDPR Handbook* (United States of America 2020) 151.

Ref. code: 25646301033624ADV

นั้น คำศัพท์ทั้งสองยังถูกยกขึ้นมาถกเถียงกันทางวิชาการและทางกฎหมายโดยยังไม่มีข้อสรุปที่แน่นอน เนื่องจากหลายประเทศในสหภาพยุโรปมีปัญหาความหลากหลายของชนกลุ่มน้อยอยู่มาก โดยเฉพาะในประเทศโปแลนด์ และประเทศโรมาเนีย[9] ผู้เขียนจึงสรุปได้ว่าการกำหนดความหมายของคำดังกล่าวให้ชัดเจน อาจต้องพิจารณาถึงจารีตประเพณีและบริบทของประเทศนั้นๆ ซึ่งเมื่อพิจารณาถึงบริบทดังกล่าวในประเทศไทย ในปัจจุบันมิได้ระบุเชื้อชาติลงบนบัตรประชาชน รวมถึงประชาชนทั่วไปมักมีความเข้าใจว่าเชื้อชาติ และสัญชาติเป็นสิ่งเดียวกัน ปัญหาในเรื่องของการแบ่งเชื้อชาติหรือเลือกปฏิบัติเพราะเหตุความแตกต่างทางเชื้อชาติหรือเผ่าพันธุ์อาจมิได้มีความเด่นชัดเหมือนอย่างปัญหาการเลือกปฏิบัติต่อบุคคลที่มีเชื้อชาติแอฟริกา เชื้อชาติเอเชียในประเทศสหรัฐอเมริกา[10] หรือปัญหาเผ่าพันธุ์ต่างๆ ที่มีความหลากหลาย และปัญหาเรื่องผู้ลี้ภัยในสหภาพยุโรป[11] จึงอาจกล่าวได้ว่าในประเทศไทยไม่มีความจำเป็นต้องเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่เป็นเชื้อชาติหรือเผ่าพันธุ์ ยกเว้นเพื่อการบริหารจัดการกิจการใดๆ ของภาครัฐเท่านั้น ส่วนในภาคเอกชนซึ่งรวมถึงข้อมูลเพื่อรับประกันภัยหรือชดใช้ค่าสินไหมทดแทนนั้น ข้อมูลเชื้อชาติและเผ่าพันธุ์ไม่มีความจำเป็นต้องเก็บรวบรวม ใช้ และเปิดเผยแต่อย่างใด ส่วนความหมายของคำดังกล่าว ผู้เขียนขอสรุปว่าเชื้อชาติหรือเผ่าพันธุ์ มิใช่ข้อมูลชนิดเดียวกันกับสัญชาติ แต่มีลักษณะเป็นการระบุต้นกำเนิดของบุคคลผู้เป็นเจ้าของข้อมูลในลักษณะเชื้อชาติหรือเผ่าพันธุ์ ซึ่งการตีความคำดังกล่าวในแต่ละพื้นที่การบังคับใช้กฎหมายต้องพิจารณาตามจารีตประเพณีและบริบทของสังคมนั้นๆ ประกอบ

---

[9] Lilla Farkas, ‘The meaning of racial or ethnic origin in EU law: between stereotypes and identities’ (January 2017) 57 < https://op.europa.eu/en/publication-detail/-/publication/c1cf6b78-094c-11e7-8a35-01aa75ed71a1/language-en> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

[10] ‘US election 2020: Why racism is still a problem for the world's most powerful country’ BBC News (30 October 2020) <https://www.bbc.com/news/election-us-2020-54738922> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

[11] ‘Europe and the Refugee Crisis: A Challenge to Our Civilization’ United Nation <https://www.un.org/en/academic-impact/europe-and-refugee-crisis-challenge-our-civilization> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

Ref. code: 25646301033624ADV

2.1.2 ความคิดเห็นทางการเมือง (political opinions)

หมายความรวมถึง การรณรงค์ การระดมทุน การสำรวจความคิดเห็นทางการเมือง[12] หากพิจารณาถึงบริบทในสังคมไทยจะพบว่าการแสดงความคิดเห็นทางการเมืองมีความอ่อนไหวต่อสังคมอย่างชัดเจน เช่น กรณีการแสดงความคิดเห็นทางการเมืองของนางสาวปนัสยา สิทธิจิรวัฒกุล[13] และนายพริษฐ์ ชิวารักษ์[14] แกนนำแนวร่วมธรรมศาสตร์และการชุมนุมที่การแสดงความคิดเห็นทางการเมืองได้ทำให้ถูกวิจารณ์การแสดงออกทางการเมืองอย่างชัดเจน และเกิดผลกระทบทางกฎหมาย และทางสังคม อันเห็นเป็นตัวอย่างหนึ่งในเรื่องความอ่อนไหวในการแสดงความคิดเห็นทางการเมืองในบริบทของสังคมไทย นอกจากนี้ ในต่างประเทศก็ได้มีกรณีตัวอย่างเกี่ยวการนำข้อมูลส่วนบุคคลของผู้มีสิทธิเลือกตั้งที่เป็นผู้ใช้งานแพลตฟอร์มซึ่งได้แสดงความคิดเห็นต่างๆ รวมถึงความคิดเห็นที่เกี่ยวกับการเมืองลงบนแพลตฟอร์มหนึ่ง และถูกนำข้อมูลส่วนบุคคลเหล่านี้ไปประมวลผลจนทำให้เกิดผลกระทบเป็นวงกว้าง คือกรณีของ Facebook บริษัทสื่อสังคมออนไลน์ที่ใหญ่ที่สุดในโลกซึ่งถูกปรับจาก คณะกรรมาธิการการค้าของสหรัฐอเมริกา (Federal Trade Commission หรือ FTC) กว่า 4.9 พันล้านดอลลาร์ เนื่องจากกระทำการบกพร่องในการคุ้มครองความเป็นส่วนตัวของข้อมูลผู้ใช้งาน จนทำให้บริษัท Cambridge Analytica บริษัทวิจัยข้อมูลที่ประกอบธุรกิจโดยเน้นการวิจัยข้อมูลเพื่อกลยุทธ์ทางการเมือง และการหาเสียงเลือกตั้ง นำข้อมูลผู้ใช้งาน Facebook ไปประมวลผลนอกเหนือวัตถุประสงค์ที่ Facebook ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคล โดย Cambridge Analytica นำข้อมูลเหล่านั้นมาประมวลผลเพื่อ

---

[12] ปิยะบุตร บุญอร่ามเรือง และคณะ (เชิงอรรถ 2) 52.

[13] ธันยพร บัวทอง, ‘รุ้ง ปนัสยา ฟังพี่สาวเล่าเรื่องน้องคนเล็กผู้กลายเป็นแกนนำ : “ราษฎร” และผู้ต้องหาหมิ่นสถาบันฯ’ BBC NEWS (25 ธันวาคม 2563) <https://www.bbc.com/thai/thailand-55442292> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

[14] กุลธิดา สามะพุทธิ, ‘พริษฐ์ ชิวารักษ์: จดหมายจากเรือนจำ น้ำตาของแม่และการเดินทางไกลของหญิงวัย 51 ปี’ BBC NEWS (2 มีนาคม 2564) <https://www.bbc.com/thai/56182261> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

Ref. code: 25646301033624ADV

สนับสนุนการออกนโยบายทางการเมืองของ ดอนัลด์ จอห์น ทรัมป์[15] จนส่งผลให้ ดอนัลด์ จอห์น ทรัมป์ ชนะการเลือกตั้งเป็นประธานาธิบดีของประเทศสหรัฐอเมริกาในปี พ.ศ. 2559[16]

จึงอาจกล่าวโดยสรุปได้ว่า ความคิดเห็นทางการเมืองนั้น มีความหมายอย่างตรงตัวคือความคิดเห็นและการแสดงออกทางการเมือง และไม่ว่าจะเป็นบริบทในประเทศไทยหรือบริบทของต่างประเทศต่างก็มีผลกระทบอย่างชัดเจนต่อบุคคลที่เป็นเจ้าของข้อมูล และอาจส่งผลกระทบต่อสังคมได้ดังตัวอย่างเรื่องผลการเลือกตั้งในประเทศสหรัฐอเมริกา จึงเป็นข้อมูลที่ต้องได้รับการคุ้มครองเป็นพิเศษ

2.1.3 ความเชื่อในลัทธิ ศาสนา หรือปรัชญา (religious or philosophical beliefs)

จากการศึกษาความหมายตาม พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 พบว่า

ลัทธิ หมายความว่า คติความเชื่อถือ ความคิดเห็น และหลักการ ที่มีผู้นิยมนับถือและปฏิบัติตามสืบเนื่องกันมา เช่น ลัทธิสังคมนิยม ลัทธิชาตินิยม ลัทธิทุนนิยม

ศาสนา หมายความว่า ลัทธิความเชื่อถือของมนุษย์อันมีหลัก คือแสดงกำเนิดและความสิ้นสุดของโลก เป็นต้น อันเป็นไปในฝ่ายปรมัตถ์ประการหนึ่ง แสดงหลักธรรมเกี่ยวกับบุญบาปอันเป็นไปในฝ่ายศีลธรรมประการหนึ่ง พร้อมทั้งลัทธิพิธีที่กระทำตามความเห็นหรือตามคำสั่งสอนในความเชื่อถือนั้นๆ

ปรัชญา หมายความว่า วิชาว่าด้วยหลักแห่งความรู้และความจริง[17]

---

[15] ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ (2018) <https://www.theguardian.com/news/ 2018/mar /17/cambridge-analytica-facebook-influence-us-election> สืบค้นเมื่อวันที่ 3 มิถุนายน 2565.

[16] Graison Dangor, ‘Facebook Overpaid FTC Fine By Billions To Protect Zuckerberg, Lawsuits Say’ (2021) <https://www.forbes.com/sites/graisondangor /2021/09/21/facebook-overpaid-ftc-fine-by-billions-to-protect-zuckerberg-lawsuits-say/?sh=25169fe8352e> สืบค้นเมื่อวันที่ 27 มีนาคม 2565.

[17] พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 <https://dictionary.orst.go.th/> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

Ref. code: 25646301033624ADV

ตัวอย่างความอ่อนไหวของความเชื่อในลัทธิ ศาสนา หรือปรัชญานั้น เป็นเรื่องของการใช้ความเชื่อในลัทธิ ศาสนา และปรัชญาก่อให้เกิดความรุนแรงในประวัติศาสตร์ เช่น ความขัดแย้งระหว่างชาวพุทธยะไข่กับชาวมุสลิมโรฮิงญาในพม่า ความขัดแย้งของชาวฮินดูและชาวซิกข์ที่อยู่ในแคว้นปัญจาบแหล่งกำเนิดของศาสนาซิกข์ ประวัติศาสตร์ความขัดแย้งของชาวสิงหลที่นับถือพุทธศาสนาเถรวาทและพระสงฆ์เปลี่ยนแปลงมาเป็นอุดมการณ์กีดกันทางการเมืองและสร้างความเกลียดชังชาวทมิฬทั้งที่นับถือศาสนาฮินดูและอิสลาม[18] เป็นต้น ซึ่งในบริบทของสังคมไทย การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในหมวดนี้ที่เห็นชัดเจนที่สุดนั้น เป็นเรื่องของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลศาสนาบนบัตรประชาชน ซึ่งเมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาให้การเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลดังกล่าวต้องเป็นไปเพื่อวัตถุประสงค์ตามกฎหมายหรือได้รับความยินยอมเท่านั้น จึงก่อให้เกิดปัญหาในภาครัฐและภาคธุรกิจที่ต้องใช้สำเนาบัตรประชาชนในการทำธุรกรรมต่างๆ ผู้ที่เก็บรวบรวม ใช้ และเปิดเผยสำเนาบัตรประชาชนต้องแจ้งหรือกำหนดให้เจ้าของข้อมูลทำการปิดบังข้อมูลศาสนาบนหน้าบัตรประชาชนก่อนเก็บข้อมูลส่วนบุคคลดังกล่าว[19] อย่างไรก็ตาม ภาครัฐในประเทศไทยมีความพยายามที่จะแก้ไขปัญหานี้โดยการยกเว้นการเก็บสำเนาบัตรประชาชนในการทำธุรกรรมต่างๆ กับภาครัฐ เช่น การยกเลิกการเรียกสำเนาบัตรประจำตัวประชาชน และสำเนาทะเบียนบ้านสำหรับการติดต่อกรมการปกครอง[20] เป็นต้น ในส่วนของปัญหาดังกล่าวนั้น ไม่ปรากฏในประเทศสมาชิกในสหภาพยุโรปและประเทศอังกฤษ เนื่องจากกลุ่มประเทศเหล่านี้ไม่มีการระบุข้อมูลศาสนาลงในบัตรประจำตัวประชาชน ผู้เขียนได้ศึกษาต่อจนพบประเทศที่ระบุศาสนาในบัตรประจำตัวประชาชนและทะเบียนบ้าน คือ ประเทศตุรกี โดยมีการระบุข้อมูลศาสนาในบัตรประจำตัวประชาชนและทะเบียนบ้านมาตั้งแต่ ปี ค.ศ. 1972 และต่อมามีการกำหนดให้สามารถลบข้อมูลศาสนาออกจากทะเบียนบ้านได้โดยต้องส่งคำขอไปที่

---

[18] ปรีดี หงษ์สต้น และ อัมพร หมาดเด็น, *ศาสนากับความรุนแรง* (พิมพ์ครั้งที่ 1, สำนักพิมพ์ Illuminations Edition 2562).

[19] ‘นโยบายความเป็นส่วนตัวที่จอดรถ’ (บริษัท สยามฟิวเจอร์ดีเวลอปเมนท์ จำกัด (มหาชน)) <https://www.siamfuture.com/th/policy/privacy-policy-parking-lot> สืบค้นเมื่อวันที่ 27 มีนาคม พ.ศ.2565.

[20] ประกาศกรมการปกครอง เรื่อง ยกเลิกการเรียกสำเนาบัตรประจำตัวประชาชน และสำเนาทะเบียนบ้าน ข้อ1.

Ref. code: 25646301033624ADV

หน่วยงานรัฐอันเป็นประเด็นทางวิชาการของประเทศตุรกีเช่นเดียวกัน[21] อย่างไรก็ตาม ตั้งแต่เดือนมกราคม 2009 ประเทศตุรกีได้ยกเลิกการแสดงข้อมูลศาสนาบนหน้าบัตรประจำตัวประชาชนแล้ว นอกจากนี้หลายประเทศที่ประสบปัญหานี้ก็เริ่มทยอยดำเนินการยกเลิกการแสดงข้อมูลศาสนาบนหน้าบัตรประชาชนบ้างแล้ว เช่นกัน[22] แม้เรื่องดังกล่าวจะเป็นประเด็นข้อกังวลของงานวิชาการต่างๆ และเป็นปัญหาในการก่อกระบวนการที่ไม่จำเป็นเพิ่มเติมจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย แต่ก็ยังมิได้มีแนวทางการแก้ไขปัญหาจากประเทศเหล่านี้แต่อย่างใด มีเพียงความเคลื่อนไหวในการยกเลิกการแสดงข้อมูลศาสนาบนบัตรประจำตัวประชาชนเท่านั้น อย่างไรก็ตาม ผู้เขียนเห็นว่าผู้ประกอบการควรดำเนินการโดยการปกปิดข้อมูลศาสนาบนสำเนาบัตรประชาชนให้กับลูกค้าไปก่อนจนกว่าจะมีแนวปฏิบัติที่ชัดเจน

2.1.4 พฤติกรรมทางเพศ (person's sex life or sexual orientation)

คำว่าพฤติกรรมทางเพศ นั้น มิได้หมายความว่าการระบุเพศหญิงหรือเพศชาย แต่เป็นการระบุถึงพฤติกรรมทางเพศของเจ้าของข้อมูลส่วนบุคคล อันหมายความรวมถึงข้อมูลเกี่ยวกับชีวิตทางเพศ รสนิยมทางเพศ เช่น พื้นฐานของอารมณ์ ความใคร่ และ/หรือ ความสนใจทางเพศ[23] ซึ่งสังคมปัจจุบันมีความหลากหลายทางเพศ ความหลากหลายในความสนใจทางเพศ หรือรสนิยมทางเพศ และมีข้อกังวลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอันเกี่ยวกับลักษณะทางเพศ และพฤติกรรมทางเพศที่มีความหลากหลายนั้นด้วย เช่น ความกังวลในการเอาชีวิตส่วนตัวทางเพศหรือ

---

[21] Selin Esen and Levent Gonenç, 'Religious Information on Identity Cards: A Turkish Debate' (Cambridge University Press, 24 April 2015) <https://www.cambridge.org/core/journals/journal-of-law-and-religion/article/abs/religious-information-on-identity-cards-a-turkish-debate/A992BF6304C33E8922FB028F18075B5C> สืบค้นเมื่อวันที่ 5 มิถุนายน 2565.

[22] Paula Peñacoba, 'Identified by religion: Religion on national ID cards' (Underground Network) <https://underground.net/identified-by-religion-religion-on-national-id-cards/> สืบค้นเมื่อวันที่ 5 มิถุนายน 2565.

[23] กฤษฎ์ อุทัยรัตน์, *บทสรุป PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล หลักการ แนวคิด ข้อกฎหมาย กรณีศึกษาและแนวปฏิบัติ* (บริษัท ธรรมนิติ เพรส จำกัด 2563) 327-328.

Ref. code: 25646301033624ADV

ทางครอบครัวไปเปิดเผยต่อสาธารณชนของกลุ่ม LGBTQ+[24] เป็นต้น และหากพิจารณาจากบริบทในสังคมไทยกับวิถีทางเพศในปัจจุบัน พบว่าความหลากหลายทางเพศนั้น มีผลกระทบต่อการยอมรับของสังคมและชุมชนและสถานศึกษา แม้ว่าในปัจจุบันมีการยอมรับทางสังคมมากขึ้น แต่ก็ยังส่งผลต่อการเลือกปฏิบัติในสังคมอยู่จึงยังเป็นปัญหาที่มีความอ่อนไหวในสังคม[25] นอกจากนี้ ในปัจจุบันสังคมได้มีความเคลื่อนไหวจากกลุ่มผู้มีความหลากหลายทางเพศและผู้สนับสนุนให้มีกฎหมายที่เกี่ยวกับความหลากหลายทางเพศ ซึ่งประเด็นที่น่าสนใจที่ยืนยันได้ว่าพฤติกรรมทางเพศอาจส่งผลกระทบต่อชีวิต ร่างกาย หรือเสรีภาพของบุคคลได้ ได้แก่ มีการออกกฎหมายที่เกี่ยวกับความเกลียดชังผู้มีความหลากหลายทางเพศในหลากหลายประเทศเพื่อลดอาชญากรรมที่เกิดจาดความเกลียดชังผู้มีความหลากหลายทางเพศ แม้กฎหมายในลักษณะนี้จะยังไม่ปรากฏในประเทศไทย และไม่เคยมีการเก็บสถิติเรื่องการก่ออาชญากรรมต่อผู้มีความหลากหลายทางเพศ แต่ในช่วงหลังก็มีความตระหนักมากขึ้นในสังคมถึงเรื่องดังกล่าว[26] จากข้อมูลดังกล่าว จึงสนับสนุนได้ว่าข้อมูลพฤติกรรมทางเพศอาจนำไปสู่การเลือกปฏิบัติ หรือการมีผลต่อชีวิต ร่างกาย เสรีภาพของเจ้าของข้อมูลได้ อันเป็นข้อมูลที่ควรเก็บรวบรวม ใช้ และเปิดเผยอย่างระมัดระวังเป็นพิเศษ และในทางปฏิบัติหน่วยงานเอกชนโดยเฉพาะในภาคธุรกิจประกันภัยก็มิได้มีการเก็บข้อมูลดังกล่าวมาใช้แต่อย่างใด

2.1.5 ประวัติอาชญากรรม (criminal records)

ประวัติอาชญากรรมเป็นหนึ่งในข้อมูลชนิดพิเศษตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่มิใช่ข้อมูล “special categories”

---

[24] Chloe Flascher ‘LGBTQ+ and protecting your privacy in the UK’ (10 June 2020) Withersworldwide <https://www.withersworldwide.com/en-gb/insight/lgbtq-and-protecting-your-privacy-in-the-uk> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

[25] จรีลักษณ์ รัตนาพันธ์, ‘เพศวิถีศึกษา : ผลกระทบต่อสถาบันทางสังคม’ (2563) 2 วารสารอิเล็กทรอนิกส์การเรียนรู้ทางไกลเชิงนวัตกรรม 28-30 <https://so01.tci-thaijo.org/index.php/e-jodil/article/view/244879/165675> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

[26] เอมผกา เตชะอภัยคุณ, ‘สรุปสาระสำคัญจากเสวนาวิชาการหัวข้อ สถานการณ์กฎหมายเกี่ยวกับความหลากหลายทางเพศ’ (สรุปสาระสำคัญจากเสวนาวิชาการหัวข้อ “สถานการณ์กฎหมายเกี่ยวกับความหลากหลายทางเพศ”, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 26 มิถุนายน 2564) <https://www.law.tu.ac.th/seminar-summary-law-and-lgbtq/> สืบค้นเมื่อวันที่ 27 มีนาคม 2565.

Ref. code: 25646301033624ADV

ตาม GDPR ข้อ 9 โดย GDPR แยกประวัติอาชญากรรมมาเป็นข้อกำหนดอีกข้อหนึ่ง คือ GDPR ข้อ 10 ซึ่งกำหนดให้การประมวลผลข้อมูลอาชญากรรมนั้นกระทำได้แต่โดยหน่วยงานที่กฎหมายของสหภาพยุโรปและกฎหมายของประเทศสมาชิกอนุญาตให้ประมวลผลเท่านั้น แต่ในประเทศไทย ประวัติอาชญากรรมอาจถูกประมวลผลโดยหน่วยงานใดก็ตามที่ได้รับความยินยอมเป็นหนังสือหรือประมวลผลตามสิทธิตามกฎหมายข้ออื่นในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมีหนังสือมอบอำนาจจากเจ้าของข้อมูลส่วนบุคคลนั้น[27] โดยผู้ควบคุมข้อมูลที่ได้รับความยินยอมหรือมีสิทธิประมวลผลข้อมูลอาชญากรรม สามารถยื่นขอข้อมูลอาชญากรรมของบุคคลที่กองทะเบียนประวัติอาชญากร ฝ่ายทะเบียนประวัติอาชญากร 3

อย่างไรก็ตาม การประมวลผลประวัติอาชญากรรม อาจส่งผลกระทบต่อบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ เช่น กรณีที่บริษัทเอกชนหลายแห่ง โดยเฉพาะกลุ่มธนาคาร สถาบันการเงิน และบริษัทประกันภัยมีระเบียบการเข้าทำงานให้ตรวจประวัติอาชญากรรมของผู้สมัครงานที่ผ่านการคัดเลือกเป็นพนักงานเพื่อบริหารความเสี่ยงด้านทรัพยากรบุคคลของบริษัท จึงอาจส่งผลให้ผู้ที่มีประวัติอาชญากรรมไม่ผ่านการคัดเลือกเข้าทำงานในบริษัท ซึ่งถือเป็นประเด็นอ่อนไหวที่ทำให้เกิดผลกระทบต่อเจ้าของข้อมูลได้เช่นกัน แต่ก็มิได้หมายความว่าการมีกฎเกณฑ์หรือระเบียบเช่นนี้ของบริษัทต่างๆ จะขัดต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่บริษัทดังกล่าวจะมีการเก็บรวบรวม ใช้ และเปิดเผยโดยไม่มีความยินยอมของเจ้าของข้อมูล รวมถึงไม่มีฐานกฎหมายอื่นที่สามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้ อย่างไรก็ตาม บริษัทเหล่านี้ต้องมีกระบวนการในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลอาชญากรรมให้เป็นไปตามกฎหมาย ดังนั้น เมื่อบริษัทเอกชนไม่สามารถประมวลผลข้อมูลอาชญากรรมโดยอาศัยฐานตามมาตรา 26 (1) ถึง (5) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ บริษัทที่มีกฎเกณฑ์หรือระเบียบข้อบังคับดังกล่าว ต้องจัดให้มีการขอความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง[28] และควรต้องพิจารณาถึงประโยชน์ของบริษัทในการเก็บรวบรวม และใช้ข้อมูลดังกล่าวเปรียบเทียบกับผลกระทบและความเสียหายของเจ้าของข้อมูลประกอบด้วย หากบริษัทพิจารณาแล้วเห็นว่าการตรวจประวัติอาชญากรรมของพนักงานในบางตำแหน่งมีความจำเป็นอย่างยิ่ง เช่น พนักงานที่ต้องรับหรือจ่ายเงินสด พนักงานที่ต้องทำบัญชี เป็นต้น บริษัทอาจพิจารณาขอความยินยอมจากผู้สมัครงานที่ผ่านการคัดเลือกเป็นหนังสือเพื่อขอเก็บรวบรวม ใช้ ข้อมูลประวัติอาชญากรรมในการประเมินคุณสมบัติเข้าทำงานกับบริษัท โดยตัวอย่างการขอความยินยอมโดยชัดแจ้งนั้น ผู้เขียนจะได้อภิปรายในบทถัดไป

---

[27] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 24.

[28] ปิยะบุตร บุญอร่ามเรือง และคณะ (เชิงอรรถ 2) 350.

Ref. code: 25646301033624ADV

อย่างไรก็ตาม เพื่อลดการบริหารจัดการเรื่องการขอความยินยอมโดยชัดแจ้ง และการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่จำเป็นตามวัตถุประสงค์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การตรวจประวัติอาชญากรรมของพนักงานที่มิได้มีความเสี่ยงสูงด้านการกระทำอาชญากรรมต่อบริษัท เช่น พนักงานธุรการที่มิได้เกี่ยวข้องด้านการเงิน หรือช่างซ่อมบำรุงทั่วไป เป็นต้น บริษัทอาจพิจารณายกเว้นเกณฑ์การตรวจประวัติอาชญากรรมของพนักงานในตำแหน่งเหล่านี้ เพื่อลดความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลด้วย

2.1.6 ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต (Data concerning Health)

ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต หรือใน GDPR ใช้คำว่า data concerning health ซึ่งหากพิจารณาแล้ว คำว่าข้อมูลสุขภาพ หรือ data concerning health นั้น หมายความรวมถึงข้อมูลความพิการและข้อมูลสุขภาพจิตด้วย

สำหรับกฎหมายในประเทศไทยที่ให้ความคุ้มครองข้อมูลสุขภาพในปัจจุบัน นอกเหนือจากที่ระบุไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้แก่ มาตรการคุ้มครองทางแพ่งที่เกี่ยวข้องกับการทำละเมิดโดยใช้ข้อมูลสุขภาพ มาตรการคุ้มครองทางอาญาในเรื่องการไม่เปิดเผยความลับสำหรับผู้ประกอบวิชาชีพและผู้ศึกษาอบรม การคุ้มครองข้อมูลสุขภาพในฐานะเป็นข้อมูลข่าวสารราชการ และการคุ้มครองโดยกฎหมายว่าด้วยสุขภาพแห่งชาติ[29] ซึ่งในกฎหมายหลักเรื่องข้อมูลสุขภาพอันได้แก่ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 ได้กำหนดความหมายของคำว่าสุขภาพไว้ว่า “ภาวะของมนุษย์ที่สมบูรณ์ทั้งทางกาย ทางจิต ทางปัญญา และทางสังคม เชื่อมโยงกันเป็นองค์รวมอย่างสมดุล"[30] อันมีความหมายครอบคลุมทั้ง สุขภาพทั่วไป ความพิการ และสุขภาพจิต นอกจากนี้ กฎหมายฉบับดังกล่าวยังกำหนดให้ข้อมูลสุขภาพมีลักษณะเป็นข้อมูลความลับ จะเปิดเผยมิได้เว้นแต่เป็นไปตามความประสงค์ของเจ้าของข้อมูลหรืออาศัยกฎหมายในการเปิดเผย และการขอข้อมูลสุขภาพต้องกระทำโดยเจ้าของข้อมูลเท่านั้น[31] อันเป็นข้อจำกัดที่เข้มงวดกว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากในกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีการกำหนดการขอความยินยอมในข้อมูลส่วนบุคคลสำหรับผู้เยาว์ บุคคลไร้ความสามารถ และบุคคลเสมือนไร้ความสามารถให้สามารถให้ความยินยอมโดยผู้ใช้อำนาจ

---

[29] หทัยชนก หร่ายวงศ์, ‘ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2559) (2).

[30] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 มาตรา 3.

[31] พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 มาตรา 7.

Ref. code: 25646301033624ADV

ปกครองสำหรับผู้เยาว์ หรือ ผู้อนุบาลสำหรับบุคคลไร้ความสามารถ หรือผู้พิทักษ์สำหรับบุคคลเสมือนไร้ความสามารถได้[32] ซึ่งถือว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บัญญัติออกมาได้สอดคล้องกับประมวลกฎหมายแพ่งและพาณิชย์ และเหมาะสมกับการปฏิบัติจริงมากกว่า

ข้อมูลสุขภาพ ประวัติทางสุขภาพ และข้อมูลสุขภาพจิตนั้น เป็นอีกปัจจัยหนึ่งที่ก่อให้เกิดการเลือกปฏิบัติ ผู้เขียนขอยกตัวอย่างการเลือกปฏิบัติต่อผู้ติดเชื้อเอชไอวี เพราะเหตุที่บุคคลทั่วไปมีความรู้ความเข้าใจในการอยู่ร่วมกับผู้ติดเชื้อเอชไอวีไม่เพียงพอ ดังจะกล่าวต่อไปนี้

จากการศึกษาพบว่าผู้ติดเชื้อเอชไอวีที่รับบริการในคลินิก ARV โรงพยาบาลอากาศอำนวยมีประสบการณ์การได้รับบริการโดยถูกเลือกปฏิบัติเพราะเหตุตนเป็นผู้ป่วยเอชไอวีถึง 22.58% และมีผู้ติดเชื้อเอชไอวีที่ตัดสินใจไม่ไปเข้ารับบริการสุขภาพเพราะรู้สึกว่าตนเองไม่ควรได้รับการรักษาถึง 37.1%[33] ตัวเลขดังกล่าวสะท้อนให้เห็นว่าแม้แต่ผู้ปฏิบัติงานในสถานพยาบาลก็ยังเลือกปฏิบัติต่อบุคคลที่ติดเชื้อเอชไอวี จึงเป็นตัวอย่างที่สามารถอธิบายความอ่อนไหวของข้อมูลสุขภาพได้อย่างชัดเจน อย่างไรก็ตาม ในการรับประกันภัยนั้น มีการใช้ข้อมูลสุขภาพทั้งในลักษณะของการตอบคำถามเกี่ยวกับข้อมูลสุขภาพเพื่อรับประกันภัยตามหลักสุจริตอย่างยิ่ง การพิจารณารับประกันภัยโดยร้องขอหลักฐานการยืนยันด้านสุขภาพเพิ่มเติม หรือการเรียกร้องค่าสินไหมทดแทนโดยแนบหลักฐานการรักษาพยาบาลไปด้วย ซึ่งหากพิจารณาตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้ว การดำเนินการดังกล่าวของบริษัทประกันภัย นายหน้าประกันภัย และผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องอาจต้องอาศัยฐานความยินยอมโดยชัดแจ้ง

2.1.7 ข้อมูลสหภาพแรงงาน (trade union membership)

เป็นที่ทราบดีอยู่แล้วในบรรดานักกฎหมายว่าสหภาพแรงงานนั้นจัดตั้งขึ้นมาเพื่อต่อรองกับนายจ้างตามพระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 ทั้งกฎหมายก็ได้คุ้มครองมิให้มีการเลิกจ้างหรือโยกย้ายพนักงานที่อยู่ในสหภาพแรงงาน หลังจากมีการยื่นข้อเรียกร้องตามกฎหมายแล้ว[34] นอกจากนี้ กฎหมายยังมุ่งคุ้มครองการกระทำใดๆ ของสหภาพแรงงานด้วย การเปิดเผยเรื่องสมาชิกภาพของเจ้าของข้อมูลส่วนบุคคลย่อมส่งผลต่อการตัดสินใจจ้างงานของบริษัทใหม่ หรือบริษัท

---

[32] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 20.

[33] นาวา ผานะวงค์, ‘ผลการใช้โปรแกรมลดการตีตราและการเลือกปฏิบัติกับผู้ติดเชื้อเอชไอวีในโรงพยาบาลอากาศอำนวย จังหวัดสกลนคร ปี พ.ศ. 2562’ (2562) วารสารโรคเอดส์ 130 <https://he02.tci-thaijo.org/index.php/ThaiAIDSJournal/article/view/253772/172531> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

[34] พระราชบัญญัติแรงงานสัมพันธ์ พ.ศ. 2518 มาตรา 31.

Ref. code: 25646301033624ADV

อื่นที่พิจารณาว่าจ้างเจ้าของข้อมูล ข้อมูลดังกล่าวจึงถือว่ามีความอ่อนไหวต่อเจ้าของข้อมูล อย่างไรก็ตาม ในภาคธุรกิจประกันภัยก็มิได้มีการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

2.1.8 ข้อมูลพันธุกรรม (genetic data)

ข้อมูลพันธุกรรม หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับลักษณะทางพันธุกรรมที่สืบทอดหรือได้มาของบุคคลธรรมดา ซึ่งให้ข้อมูลเฉพาะเกี่ยวกับสรีรวิทยาหรือสุขภาพของบุคคลธรรมดานั้น และเป็นผลจากการวิเคราะห์ตัวอย่างทางชีววิทยาจากธรรมชาติโดยเฉพาะ และเป็นผลจากการวิเคราะห์ตัวอย่างทางชีววิทยาจากบุคคลในประเด็นโดยเฉพาะ[35] ซึ่งรวมถึง การวิเคราะห์ข้อมูลโครโมโซม ดีเอ็นเอ (DNA) หรือ อาร์เอ็นเอ (RNA) หรือการวิเคราะห์ประเภทอื่นใดที่ช่วยให้ได้รับข้อมูลที่เท่าเทียมกัน ซึ่งข้อมูลทางพันธุกรรมนั้น มิได้เป็นข้อมูลส่วนบุคคลโดยตัวของข้อมูลเอง แต่เมื่อมีการนำไปประมวลผลแล้วสามารถระบุได้ถึงตัวบุคคลได้ ซึ่งตรงกับความหมายของคำว่าข้อมูลส่วนบุคคลพิเศษตาม GDPR อย่างไรก็ตามในปัจจุบัน ประเทศไทยยังมิได้มีฐานข้อมูลพันธุกรรมในระดับประเทศ และการเก็บข้อมูลพันธุกรรมของบุคคล เป็นไปเพื่อคลี่คลายคดีอาชญากรรมหรือพิสูจน์บุคคลสูญหาย หรือรับรองความเป็นบิดามารดาเท่านั้น แต่ในต่างประเทศได้มีการจัดตั้งฐานข้อมูลทางพันธุกรรมระดับประเทศและตรากฎหมายเพื่อเป็นแนวทางในการจัดการไว้โดยเฉพาะ เช่น ประเทศอังกฤษ ประเทศออสเตรเลีย ประเทศญี่ปุ่น เป็นต้น[36] ด้วยบริบทและกรณีปัญหาการเก็บรวบรวม ใช้ และประมวลผลข้อมูลดังกล่าวยังไม่มากและแพร่หลายนัก จึงยังไม่อาจยกตัวอย่างความเสียหายจากความอ่อนไหวของข้อมูลได้ อย่างไรก็ตาม กฎหมายกำหนดให้ข้อมูลดังกล่าวมีความอ่อนไหว หากผู้ใดเก็บรวบรวม ใช้ หรือเปิดเผย ต้องปฏิบัติตามมาตรฐานการดูแลข้อมูลส่วนบุคคลที่เข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป

2.1.9 ข้อมูลชีวภาพ (biometric data)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดความหมายข้อมูลชีวภาพไว้ว่าเป็นข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ ทำให้สามารถยืนยันตัวตนของ

---

[35] UK General Data Protection Regulation Article 4 (13).

[36] วิภู วิมลเศรษฐ และศิริรัตน์ ชูสกุลเกรียง, ‘ฐานข้อมูลสารพันธุกรรมในประเทศไทย DNA Database in Thailand’ (2563) 3 วารสารกระบวนการยุติธรรม 61 < https://so04.tci-thaijo.org/index.php/JTJS/article/view/241983/169320> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

Ref. code: 25646301033624ADV

บุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ[37]

หากให้ยกตัวอย่างความเสียหายปัจจุบันที่เกิดขึ้นจากข้อมูลจำลองใบหน้า ม่านตา หรือลายนิ้วมือนั้น อาจยังไม่พบเห็นในปัจจุบันอย่างแพร่หลายมากนัก แต่ข้อมูลดังกล่าวหากถูกขโมยไปได้อาจเป็นกุญแจในการเข้าถึงระบบความปลอดภัยต่างๆ ได้ด้วย เช่น การเข้าถึงโทรศัพท์มือถือ และแอปพลิเคชันธนาคาร การเข้าที่อยู่อาศัยเมื่อใช้ระบบสแกนลายนิ้วมือหรือใบหน้าเป็นต้น การเข้าถึงข้อมูล หรือที่อยู่อาศัยข้างต้นอาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลได้โดยง่าย โดยเฉพาะการใช้ข้อมูลเพื่อก่ออาชญากรรม หรือปลอมแปลงตัวตน จึงเป็นข้อมูลส่วนบุคคลที่ควรต้องได้รับการดูแลเป็นพิเศษ

2.1.10 ข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ซึ่งปัจจุบัน (วันที่ 17 กรกฎาคม 2565) ยังมิได้มีการประกาศจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงยังคงเป็นการเปิดช่องว่างทางกฎหมายไว้สำหรับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

จากข้อมูลที่ได้ศึกษามาข้างต้น ผู้เขียนขอสรุปในขั้นต้นว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น เป็นข้อมูลส่วนบุคคลที่อาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป เช่น หากข้อมูลส่วนบุคคลที่มีความอ่อนไหวถูกเปิดเผยต่อสาธารณชนแล้ว เจ้าของข้อมูลอาจได้รับการเลือกปฏิบัติ การดูถูก หรือถูกเกลียดชังได้ หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวบางประเภทอาจส่งผลต่อความปลอดภัยในชีวิต ร่างกาย และทรัพย์สินของเจ้าของข้อมูลส่วนบุคคลมากเป็นพิเศษ จึงต้องได้รับการดูแลเป็นพิเศษเช่นกัน ผู้ประกอบธุรกิจต่างๆ จึงต้องจัดให้มีมาตรการในการบริหารจัดการเป็นพิเศษเพื่อคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว

2.2 แนวทางการจัดการกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ห้ามมิให้มีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยมิได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

---

[37] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสอง.

Ref. code: 25646301033624ADV

ส่วนบุคคล ดังนั้น ในการขอความยินยอมสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องกระทำโดยชัดแจ้งเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีดังกล่าวได้ นอกจากนี้ ผู้ควบคุมข้อมูลยังต้องมีการแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล โดยข้อความที่เข้าใจง่ายไม่ก่อให้เกิดความเข้าใจผิด[38] กฎหมายมิได้มีการกำหนดความแตกต่างระหว่างการขอความยินยอมตามมาตรา 19 และการขอความยินยอมโดยชัดแจ้งตามมาตรา 26 ไว้ และยังไม่มีเอกสารอย่างเป็นทางการมาบ่งชี้ความแตกต่างระหว่างการขอความยินยอมและการขอความยินยอมโดยชัดแจ้ง จึงต้องอาศัยคำอธิบายตามกฎหมายต่างประเทศซึ่งมีการตีความคำว่า การแสดงความยินยอมโดยชัดแจ้ง (explicit consent) ดังจะกล่าวต่อไปในบทนี้

ความยินยอมนั้นเป็นการกระทำที่ส่งผลต่อเรื่องคุณธรรม และสิทธิทางกฎหมาย รวมถึงหน้าที่ต่างๆ โดยความยินยอมส่งผลให้สิทธิที่ผู้ได้รับความยินยอมไม่มีสิทธิกระทำได้ กลับกลายเป็นสิทธิที่สามารถกระทำได้[39] เช่น การเปิดเผยข้อมูลเครดิต (NCB) ของเจ้าของข้อมูล การขอเข้าพื้นที่ส่วนบุคคล หรือการขอติดต่อผ่านทางช่องทางต่างๆ เป็นต้น ซึ่งประเภทของความยินยอมนั้นมีดังต่อไปนี้

- ความยินยอมโดยชัดแจ้ง (Explicit Consent) คือการแสดงออกหรือตอบรับอย่างชัดเจนว่าให้ความยินยอม เช่น การลงลายมือชื่อยืนยันว่ายินยอม การกดปุ่มคำว่ายินยอม เป็นต้น

- ความยินยอมโดยนิ่งเฉย (Tacit Consent) คือ การไม่แสดงออกใดๆ ที่ชี้ชัดว่าไม่เห็นด้วยกับการกระทำนั้นๆ เช่น กรณีที่มีการส่งจดหมายอิเล็กทรอนิกส์ (Email) โดยธนาคารส่งลิงค์สำหรับยกเลิกการติดต่อมาให้ แต่ผู้รับข้อมูลเพิกเฉยไม่กดลิงค์ดังกล่าว เป็นต้น

- ความยินยอมโดยปริยาย (Implied Consent) คือ การแสดงท่าทีบางอย่างที่อนุมานได้ว่าให้ความยินยอม เช่น การที่บุคคลยื่นแขนให้เจ้าหน้าที่พยาบาลฉีดวัคซีน เป็นต้น

- ความยินยอมที่พึงสันนิษฐานได้ (Presumed Consent) คือสถานการณ์ที่ผู้ยินยอมไม่อยู่ในสถานภาพที่สามารถให้ความยินยอมได้ เช่น ผู้ป่วยที่ไม่ได้สติ เป็นต้น กรณีลักษณะนี้เป็นเรื่องก้ำกึ่งระหว่างความยินยอมและความจำเป็น ซึ่งต้องอาศัยบรรทัดฐานของวิญญูชนในการพิจารณาว่าบุคคลนั้นให้ความยินยอมหรือไม่[40]

---

[38] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 19.

[39] Andreas Mueller and Peter Schaber, *The Routledge Handbook of the Ethics of Consent* (London: Taylor and Francis, Kindle Locations) 405.

[40] สุธินันท์ ศรีราษฎร์, 'ความยินยอมในกฎหมายคุ้มครองข้อมูลส่วนบุคคล' (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2561) 13-15.

Ref. code: 25646301033624ADV

ความยินยอมที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดลักษณะไว้นั้น ต้องเป็นความยินยอมโดยชัดแจ้ง (Explicit Consent) ซึ่งหากพิจารณาแล้วความยินยอมโดยชัดแจ้งอาจมิได้มีความแตกต่างจากความยินยอมโดยทั่วไป (Regular Consent) ที่มีคุณภาพสูงมากนัก เนื่องจากความยินยอมโดยทั่วไปที่มีคุณภาพสูง มักจะกำหนดให้เจ้าของข้อมูลส่วนบุคคลต้องกระทำการบางอย่างที่แสดงออกถึงความยินยอมซึ่งไม่เป็นการแสดงออกโดยการนิ่งเฉย การให้ความยินยอมโดยปริยาย หรือการให้ความยินยอมอันพึงสันนิษฐานได้โดยวิญญูชนทั่วไป นอกจากนี้ ความยินยอมโดยชัดแจ้งจะต้องทำให้เจ้าของข้อมูลเข้าใจอย่างชัดเจนว่าข้อมูลที่จะถูกประมวลผลคือข้อมูลชนิดใด การประมวลผลนั้นๆ มีการดำเนินการที่เกี่ยวข้องเป็นอย่างไร การประมวลผลมีวัตถุประสงค์เพื่ออะไร และการเปิดเผยว่ามีการกระทำใดที่อาจเกิดขึ้นกับข้อมูลที่ถูกประมวลผลนั้นด้วย[41] ยกตัวอย่างสถานการณ์การให้ความยินยอมในการเก็บข้อมูลสุขภาพของผู้สมัครงานเพื่อประกอบการพิจารณาคุณสมบัติการเข้าทำงาน เช่น การตอบคำถามเรื่องโรคประจำตัว ภาวะการตั้งครรภ์ ประวัติการรักษาพยาบาลเรื้อรัง เป็นต้น การให้ความยินยอมในเรื่องการเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ ต้องใช้ความยินยอมโดยชัดแจ้ง ซึ่งสำหรับสถานการณ์เช่นนี้ หากเป็นความยินยอมโดยทั่วไปนั้น บริษัทที่รับสมัครงานอาจมีการสอบถามข้อมูลดังกล่าวและเขียนข้อความกำกับว่า “ท่านสามารถเลือกที่จะให้ข้อมูลหรือไม่ให้ข้อมูลดังกล่าวแก่บริษัทก็ได้ และข้อมูลที่ท่านให้มานี้จะถูกเก็บเพื่อประกอบการพิจารณาคัดเลือกเข้าทำงาน” ซึ่งหากเจ้าของข้อมูลกรอกข้อมูลลงไปก็เป็นการให้ความยินยอมไปโดยปริยาย แต่หากเป็นกรณีขอความยินยอมโดยชัดแจ้งนั้น เจ้าของข้อมูลต้องมีการกระทำบางอย่างที่บ่งชี้ว่าได้ให้ความยินยอมอย่างชัดเจน เช่น มีการลงลายมือชื่อท้ายการให้ข้อมูลพร้อมข้อความให้ความยินยอมว่า “ข้าพเจ้าให้ความยินยอมแก่บริษัทในการเก็บและใช้ข้อมูลสุขภาพข้างต้นเพื่อประกอบการพิจารณาสมัครงาน ลงชื่อ_____”[42] เป็นต้น

---

[41] Susan Singleton, *Tolley's Data Protection Handbook* (4th edn, CPI Bath Press, 2006) 569.

[42] 'What is 'explicit consent'?' (Information Commissioner's Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=The%20key%20difference%20is%20likely,action%20(which%20would%20not).> สืบค้นเมื่อวันที่ 28 ธันวาคม 2564.

Ref. code: 25646301033624ADV

การให้ความยินยอมโดยชัดแจ้ง หรือ explicit consent ถูกกำหนดไว้ใน GDPR ข้อ 9 สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งข้อกำหนดในเรื่องความชัดแจ้งนี้ถูกยกขึ้นมาเพื่อยกระดับความยินยอมตาม GDPR สำหรับข้อมูลส่วนบุคคลที่ต้องการการคุ้มครองและบริหารความเสี่ยงอย่างเข้มงวด นอกจากนี้ ทั้งการให้ความยินยอม (Regular Consent) อย่างมีประสิทธิภาพ และการให้ความยินยอมโดยชัดแจ้งตาม GDPR นั้น ต้องมีลักษณะ ดังนี้

- ให้อิสระเจ้าของข้อมูลในการเลือกให้หรือไม่ให้ข้อมูล
- มีความเฉพาะเจาะจงว่าเก็บข้อมูลใดบ้าง เพื่อวัตถุประสงค์ใด
- ให้ข้อมูลครบถ้วน ไม่คลุมเครือ
- แยกส่วนการให้ความยินยอมออกมาจากข้อมูลอื่นๆ
- สื่อสารถึงเจ้าของข้อมูลโดยคำนึงถึงความยินยอมของเจ้าของข้อมูล
- มีหลักฐานในความยินยอม
- จัดให้มีการเพิกถอนความยินยอมได้โดยง่าย
- ไม่ปกปิดข้อมูล

ในการให้ความยินยอมโดยชัดแจ้งนั้น ต้องมีลักษณะเพิ่มเติมคือเจ้าของข้อมูลส่วนบุคคลต้องกระทำการบางอย่างเพื่อแสดงออกว่าตนได้ให้ความยินยอมอย่างชัดแจ้ง และผู้ควบคุมข้อมูลส่วนบุคคลต้องมีหลักฐานเป็นหนังสือ[43] หรือข้อมูลอิเล็กทรอนิกส์ที่สามารถพิสูจน์ได้ตามกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ นอกจากนี้ การขอรับความยินยอมตามแนวปฏิบัติของ GDPR นั้นยังอาจแยกออกจากกันตามลักษณะของข้อมูลส่วนบุคคลได้ เช่น การขอความยินยอมในข้อมูลส่วนบุคคลทั่วไปอาจใช้การขอความยินยอมรูปแบบหนึ่ง ส่วนการขอความยินยอมเพื่อประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจใช้การขอความยินยอมโดยแยกจากการขอความยินยอมสำหรับข้อมูลส่วนบุคคลทั่วไปก็ได้ เนื่องจาก การขอความยินยอมทั้งสองมีระดับการการขอความยินยอม

[43] Mary Kirwan and others, ‘What GDPR and the Health Research Regulations (HRRs) mean for Ireland: “explicit consent”—a legal analysis’ (2020) Irish Journal of Medical Science (1971 -) (2021) 516-517 <https://link.springer.com/content/pdf/10.1007/s11845-020-02331-2.pdf> สืบค้นเมื่อวันที่ 28 ธันวาคม 2564.

Ref. code: 25646301033624ADV

ที่แตกต่างกัน[44] และเป็นไปเพื่อกิจกรรมที่แตกต่างกัน

การตีความเพื่อกำหนดลักษณะของความยินยอมโดยชัดแจ้งตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงอาจกำหนดลักษณะตามแนวทางของ GDPR ซึ่งเป็นกฎหมายแม่แบบได้ จนกว่าจะมีแนวทางที่ชัดเจนจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศออกมา ซึ่งหากเปรียบเทียบระหว่างการให้ความยินยอมโดยทั่วไปกับการให้ความยินยอมโดยชัดแจ้งแล้ว อาจเปรียบเทียบได้ ดังนี้

ตารางที่ 2.1 ตารางเปรียบเทียบความยินยอมโดยทั่วไป และความยินยอมโดยชัดแจ้ง

หัวข้อที่เปรียบเทียบ	**ความยินยอมโดยทั่วไป**	**ความยินยอมโดยชัดแจ้ง**
1. ข้อมูลที่ปรับใช้	ข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว
2. การแสดงเจตนา	อาจกระทำโดยชัดแจ้ง โดยปริยาย หรือการกระทำอื่นที่พึงสันนิษฐานได้	ต้องกระทำโดยชัดแจ้งเท่านั้น
3. สิทธิในการเลือกที่จะให้หรือไม่ให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล	เจ้าของข้อมูลเลือกให้หรือไม่ให้ความยินยอมได้โดยอิสระ ทั้งนี้ ในการเข้าทำสัญญา หรือการให้บริการใดๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาหรือการให้บริการนั้นๆ	
4. แยกส่วนจากข้อสัญญาอื่น	แยกส่วนชัดเจน	
5. หลักฐาน	มีหลักฐานการให้ความยินยอม	
6. การเพิกถอน	มีช่องทางการเพิกถอนความยินยอมที่ง่ายเหมือนตอนให้ความยินยอม	

[44] Paul Quinn and Gianclaudio Malgieri, 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' (Cambridge University Press, 19 January 2022) <https://www.cambridge.org/core/ journals/german-law-journal/article/difficulty-of-defining-sensitive-datathe-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C900458 13F6C6> สืบค้นเมื่อวันที่ 4 มิถุนายน 2465.

Ref. code: 25646301033624ADV

นอกจากความยินยอมโดยชัดแจ้งแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังกำหนดข้อยกเว้นในการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่ต้องขอความยินยอมไว้ ดังนี้

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ เช่น การเปิดเผยข้อมูลระหว่างโรงพยาบาลเพื่อรักษาผู้ป่วยฉุกเฉินที่หมดสติ เป็นต้น

(2) การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

(3) ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น ข้อมูลการเป็นสมาชิกพรรคการเมืองที่ผู้สมัครรับเลือกตั้งเปิดเผยไว้บนสื่อสาธารณะต่างๆ เป็นต้น

(4) การจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ซึ่งรวมถึง การดำเนินคดีในชั้นศาลที่เกิดขึ้นและ/หรือที่จะเกิดขึ้นในอนาคต การดำเนินการตามคำแนะนำทางกฎหมาย การก่อตั้งสิทธิ ใช้สิทธิ หรือปกป้องสิทธิทางกฎหมายในลักษณะอื่นใด เช่น บริษัทถูกฟ้องจากลูกจ้างเกี่ยวกับอุบัติเหตุในที่ทำงานจึงเปิดเผยข้อมูลสุขภาพของลูกจ้างเพื่อขอคำปรึกษาทางกฎหมายกับทนายความ หรือการทดสอบอาการแพ้ยาในผู้ป่วยก่อนการรักษาแม้ยังไม่มีการก่อตั้งสิทธิทางกฎหมายประการใด แต่ก็เป็นการดำเนินการเพื่อป้องกันกรณีเกิดอาการแพ้ในผู้ป่วยและอาจเกิดการเรียกร้องทางกฎหมายจากเหตุนั้นได้[45] เป็นต้น ข้อยกเว้นเรื่องนี้กฎหมายไทยให้สิทธิแก่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลตามกฎหมายแม่แบบคือ GDPR ข้อ 9 (2) (f) ในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงอาจนำแนวทางดังกล่าวมาใช้เพื่อตีความพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไปได้

(5) การประมวลผลข้อมูลส่วนบุคคลที่จำเป็นต่อการดำเนินงานตามภารกิจของรัฐ เช่น การให้บริการด้านสุขภาพหรือด้านสังคม ประโยชน์สาธารณะด้านการสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิต เป็นต้น หรือ

---

[45] ‘What are the conditions for processing?’ (Information Commissioner’s Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions6> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

การประมวลผลข้อมูลเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย เช่น การประมวลผลข้อมูลของหน่วยงานรัฐเพื่อปฏิบัติหน้าที่ตามกฎหมาย หรือหน่วยงานเอกชนที่กฎหมายกำหนดให้มีภารกิจเพื่อประโยชน์สาธารณะ เป็นต้น[46]

อย่างไรก็ตาม การตีความข้างต้น อาศัยการศึกษาจากข้อมูลบนเว็บไซต์อย่างเป็นทางการของหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคลของประเทศอังกฤษ หรือ Information Commission's Office (ICO)[47] ประกอบกับข้อมูลจากบทความวิชาการในต่างประเทศ[48] และข้อมูลที่ไม่เป็นทางการของประเทศไทย[49]เท่านั้น นอกจากนี้ผู้เขียนได้ทำการศึกษาต่อจนพบร่างกฎหมายลำดับรอง และแนวปฏิบัติเบื้องต้น รวมถึงคำถามที่พบบ่อยที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยได้มีอธิบายไว้ในหน้าเว็บไซต์[50]อันจะได้อภิปรายในบทถัดไป

2.3 ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัย

การประกอบธุรกิจประกันภัยนั้น มีผู้ที่เกี่ยวข้องกับการประกอบธุรกิจหลายรายอันได้แก่ บริษัทรับประกันภัย นายหน้าประกันภัย ตัวแทนประกันภัย บริษัทประกันภัยต่อ บริษัทให้บริการจัดการค่าสินไหมทดแทน[51] อู่ซ่อมรถยนต์ สถานบริการด้านสุขภาพ ผู้สำรวจภัย เป็นต้น ซึ่งในการประกอบธุรกิจรับประกันภัย ทั้งการรับประกันชีวิต การรับประกันสุขภาพ และ

---

[46] ปิยะบุตร บุญอร่ามเรือง และคณะ (เชิงอรรถ 2) 87-89.

[47] 'For organisations' (Information Commissioner's Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/> สืบค้นเมื่อวันที่ 28 ธันวาคม 2564.

[48] Mary Kirwan and others (n 58) 516-517.

[49] ปิยะบุตร บุญอร่ามเรือง และคณะ (เชิงอรรถ 2).

[50] 'เอกสารเผยแพร่ประชาสัมพันธ์'(กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) <https://www.mdes.go.th/mission/detail/2316-%E0%B9%80%E0%B8%AD%E0%B8%81%E0%B8%AA%E0%B8%B2%E0%B8%A3%E0%B9%80%E0%B8%9C%E0%B8%A2%E0%B9%81%E0%B8%9E%E0%B8%A3%E0%B9%88%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%8A%E0%B8%B2%E0%B8%AA%E0%B8%B1%E0%B8%A1%E0%B8%9E%E0%B8%B1%E0%B8%99%E0%B8%98%E0%B9%8C> สืบค้นเมื่อวันที่ 3 มิถุนายน 2565.

[51] บรรเจิด ภาคาพันธุ์, 'ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต' (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2562) 95-99.

Ref. code: 25646301033624ADV

การรับประกันวินาศภัยนั้น ล้วนมีการเปิดเผยข้อมูลที่จำเป็นต่อการพิจารณารับประกันภัยตามหลักความสุจริตอย่างยิ่งซึ่งถือเป็นสาระสำคัญในสัญญาประกันภัยอันอาจทำให้สัญญาเป็นโมฆียะ และคู่สัญญาอาจบอกล้างบอกเลิกสัญญาได้[52] โดยข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นอย่างยิ่งต่อการรับประกันภัย ได้แก่ ข้อมูลสุขภาพของผู้เอาประกันภัย ยกตัวอย่างเช่น กรณีผู้มีโรคประจำตัวประสงค์จะทำประกันสุขภาพ บริษัทที่รับประกันสุขภาพอาจพิจารณาคิดค่าเบี้ยประกันเพิ่มเติม หรือให้ความคุ้มครองทั่วไปแต่ยกเว้นโรคประจำตัวที่เป็นมาก่อนการทำประกันสุขภาพ หรือขอเลื่อนการรับประกันสุขภาพออกไปก่อน หรืออาจปฏิเสธการรับประกันสุขภาพได้ หากโรคประจำตัวดังกล่าวเป็นโรคร้ายแรง[53]

นอกจากการเปิดเผยข้อมูลเพื่อพิจารณารับประกันภัยแล้ว ในช่วงระยะเวลาการรับประกันภัย หากเกิดเหตุการณ์ที่รับประกันภัยขึ้น เช่น มีการรับประกันอุบัติเหตุ และเกิดอุบัติเหตุขึ้น มีการรับประกันสุขภาพและผู้เอาประกันภัยเป็นโรคที่เอาประกันไว้ เป็นต้น ผู้เอาประกันภัยมีหน้าที่ต้องเปิดเผยข้อมูลการรักษาพยาบาลเพื่อเบิกค่ารักษาพยาบาล หรือค่าสินไหมทดแทนตามสัญญารับประกันภัย อันเป็นการเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อประโยชน์ในการปฏิบัติตามสัญญา อย่างไรก็ตาม ในข้อยกเว้นการขอความยินยอมโดยชัดแจ้งตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ไม่มีข้อยกเว้นในเรื่องการจำเป็นเพื่อการปฏิบัติตามสัญญา ซึ่งแตกต่างจากการขอความยินยอมสำหรับข้อมูลส่วนบุคคลทั่วไป ตามมาตรา 24 ที่ไม่ต้องขอความยินยอมในกรณีที่เป็นการจำเป็นเพื่อปฏิบัติตามสัญญา การจัดการกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัยจึงสามารถดำเนินการได้เพียงวิธีการขอความยินยอมโดยชัดแจ้งเท่านั้น แม้จะเป็นการดำเนินการตามวัตถุประสงค์ของสัญญาก็ตาม หากวิเคราะห์ตามเงื่อนไขของการขอความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว เห็นว่ามีความขัดกันกับหลักการที่ว่าสัญญาประกันภัย และการเบิกเงินค่าสินไหมทดแทนตามสัญญาประกันภัยนั้น ควรกระทำได้โดยง่ายเพื่อให้เกิดความคุ้มครองในความเสี่ยงภัยต่างๆ ทั้งทางธุรกิจ หรือความเสี่ยงในชีวิต ร่างกาย ทรัพย์สินของบุคคล และก่อให้เกิดประโยชน์สูงสุดแก่ผู้เอาประกันภัยตามวัตถุประสงค์ของสัญญาประกันภัยด้วย

ผู้เขียนจึงขอชี้ให้เห็นประเด็นปัญหาการขอความยินยอมในข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัย ดังนี้

---

[52] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865.

[53] ‘คำถามที่พบบ่อยก่อนทำประกันสุขภาพ’ (AIA Planer) <https://www.aiaplanner.com/faq/> สืบค้นเมื่อวันที่ 29 ธันวาคม 2564.

Ref. code: 25646301033624ADV

2.3.1 การขอความยินยอมในการเปิดเผยข้อมูลสุขภาพก่อนการทำสัญญาประกันชีวิตหรือประกันสุขภาพ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีอิสระในการเลือกที่จะให้หรือมิให้ความยินยอม และผู้ควบคุมข้อมูลต้องเปิดเผยสิทธิเช่นว่านั้นด้วย ดังนั้น ในการขอข้อมูลสุขภาพในใบสมัครเพื่อเอาประกันภัย จึงต้องมีข้อความการขอความยินยอมโดยชัดแจ้งตามแนวปฏิบัติของ GDPR[54] และแนวทางปฏิบัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศอังกฤษ[55]ดังที่ได้อภิปรายไปแล้วในข้อ 2.2 และอ้างอิงไปถึงนโยบายความเป็นส่วนตัวที่แจ้งสิทธิของเจ้าของข้อมูล ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฯลฯ ยกตัวอย่างเช่น

☐ ข้าพเจ้ายินยอมให้บริษัทประกันภัยเก็บรวบรวม ใช้ ข้อมูลสุขภาพของข้าพเจ้าเพื่อพิจารณารับประกันภัย และจัดเก็บ หรือเปิดเผยตามหน้าที่ที่กฎหมายกำหนด โดยข้าพเจาได้ศึกษารายละเอียดนโยบายคุ้มครองข้อมูลส่วนบุคคล <exampleinsurace.com/privacypolicy> แล้ว ลงชื่อ_____ผู้เอาประกันภัย

เป็นต้น หากเจ้าของข้อมูลไม่ให้ข้อมูล และ/หรือไม่ใส่เครื่องหมายเพื่อแสดงความยินยอมเช่นนี้บริษัทประกันภัยก็ไม่อาจเก็บและใช้ข้อมูลดังกล่าว หรือพิจารณารับประกันภัยตามสัญญาดังกล่าวได้ แม้ได้รับข้อมูลอื่นมาครบถ้วนแล้ว

การที่กฎหมายห้ามผู้ควบคุมข้อมูลกำหนดเงื่อนไขว่าหากเจ้าของข้อมูลไม่ให้ความยินยอมจะไม่สามารทำสัญญาได้นั้น ย่อมไม่อาจเกิดขึ้นได้ตามกรณีตัวอย่าง เนื่องจากผู้รับประกันภัยก็ไม่สามารถ พิจารณารับประกันภัยได้เพราะข้อมูลไม่เพียงพอต่อการพิจารณา และประเมินความเสี่ยงของการรับประกันภัย

2.3.2 การให้ข้อมูลสุขภาพ ประวัติการรักษาพยาบาล เพื่อเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัยนั้น ดำเนินการได้ 2 รูปแบบ ดังนี้

2.3.2.1 การดำเนินการโดยเจ้าของข้อมูลส่วนบุคคลเอง เช่น กรณีเรียกร้องค่าสินไหมทดแทนจากการบาดเจ็บในอุบัติเหตุทางรถยนต์ ซึ่งการบาดเจ็บดังกล่าวอาจมิใช่

---

[54] Paul Quinn and Gianclaudio Malgieri (n 59).

[55] 'Consent' (Information Commissioner's Office, Guideline to GDPR) <https://ico.org.uk /for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

การบาดเจ็บของผู้เอาประกันเท่านั้น เจ้าของข้อมูลต้องดำเนินการกรอกแบบฟอร์มของบริษัทรับประกันภัยเพื่อเปิดเผยข้อมูลสุขภาพพร้อมหลักฐานการจ่ายค่ารักษาพยาบาล ในแบบฟอร์มการเบิกค่าสินไหมทดแทนจึงต้องเพิ่มข้อความขอความยินยอมโดยชัดแจ้ง ยกตัวอย่างเช่น

☐ ข้าพเจ้ายินยอมให้บริษัทประกันภัยเก็บ ใช้ ข้อมูลสุขภาพของข้าพเจ้าเพื่อพิจารณาจ่ายค่าสินไหมทดแทนตามสัญญาประกันภัย รวมถึงยินยอมให้บริษัทประกันภัยสืบค้น สอบถามข้อมูลสุขภาพและประวัติการรักษาพยาบาลจากโรงพยาบาล หรือสถานพยาบาลอื่นซึ่งข้าพเจ้าได้ให้ความยินยอมไว้แล้ว และจัดเก็บหรือเปิดเผยตามหน้าที่ที่กฎหมายกำหนด รายละเอียดเพิ่มเติมตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทประกันภัย <exampleinsurace.com/privacypolicy> ลงชื่อ_____ผู้เอาประกันภัย

เป็นต้น ซึ่งหากในขั้นตอนแรกของการรับประกันภัย ผู้รับประกันภัยได้มีการขอความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อการพิจารณาจ่ายค่าสินไหมทดแทนแล้ว การขอความยินยอมเช่นว่านี้ ก็ไม่จำเป็นต้องปรากฏในแบบฟอร์มเบิกค่าสินไหมทดแทนอีก เว้นแต่ เป็นการเบิกค่าสินไหมทดแทนจากผู้เสียหายที่มิใช่ผู้เอาประกันภัย

2.3.2.2 กรณีโรงพยาบาลหรือสถานพยาบาล เป็นโรงพยาบาลหรือสถานพยาบาลซึ่งเป็นพันธมิตรทางธุรกิจกับบริษัทประกันภัย โรงพยาบาลหรือสถานพยาบาลดังกล่าวจะสามารถส่งเรื่องเพื่อขอเบิกค่ารักษาพยาบาลหรือค่าสินไหมทดแทนได้โดยตรง โดยผู้เอาประกันภัยไม่มีความจำเป็นดำเนินการใดเพื่ออำนวยความสะดวกต่อผู้เอาประกันภัย กรณีนี้ หากต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เอาประกันต้องดำเนินการให้ความยินยอมโดยชัดแจ้งต่อโรงพยาบาลในการเปิดเผยข้อมูลต่อบริษัทประกันภัย หรือต้องให้ความยินยอมโดยชัดแจ้งต่อบริษัทประกันภัยในการประมวลผลข้อมูลสุขภาพหรือประวัติการรักษาเพื่อพิจารณาจ่ายค่ารักษาพยาบาลหรือค่าสินไหมทดแทนด้วย ทั้งนี้ อาจรวมอยู่ในการขอความยินยอมในครั้งแรกเมื่อเข้าทำสัญญาประกันภัยก็ได้เช่นกัน

2.3.3 การดำเนินการทำประกันภัยที่ต้องเปิดเผยข้อมูลสุขภาพของเจ้าของข้อมูลส่วนบุคคลผ่านนายหน้าประกันภัย

เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมต่อทั้งนายหน้าประกันภัยและบริษัทรับประกันภัย เพราะนายหน้าประกันภัยนั้น มิใช่ตัวแทนของบริษัทประกันภัยบริษัทใดบริษัทหนึ่ง แต่นายหน้าประกันภัยมีลักษณะของการเป็นคนกลางที่มีความเป็นอิสระต่อบริษัทประกันภัย

Ref. code: 25646301033624ADV

สามารถเสนอผลิตภัณฑ์ของบริษัทประกันภัยใดก็ได้ให้แก่ลูกค้า[56] หรือเจ้าของข้อมูล จึงมิใช่ผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทประกันภัย นอกจากนี้ ในการรับประกันภัยบางประเภท นายหน้าต้องส่งข้อมูลเบื้องต้นให้บริษัทประกันภัยพิจารณาเบี้ยประกันภัยก่อน ซึ่งข้อมูลที่นายหน้าต้องส่งไปนั้น อาจรวมถึงข้อมูลสุขภาพด้วย เจ้าของข้อมูลส่วนบุคคลจึงมีความจำเป็นต้องให้ความยินยอมโดยชัดแจ้งต่อนายหน้าประกันภัยในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตั้งแต่กระบวนการแรกแม้ยังมิได้มีการตกลงทำสัญญาประกันภัย

2.3.4 การทำประกันชีวิตและประกันสุขภาพ ประเภทการทำประกันภัยแบบกลุ่ม

การทำประกันชีวิตและประกันสุขภาพประเภทกลุ่มขององค์กรต่างๆ เป็นไปเพื่อให้สวัสดิการแก่พนักงานหรือลูกจ้างซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลเพิ่มเติมจากประกันสังคมที่กฎหมายกำหนด การทำประกันภัยกลุ่มนั้น ดำเนินการโดยฝ่ายบุคคลหรือฝ่ายที่มีหน้าที่ดูแลพนักงานขององค์กร ซึ่งจะเก็บรวบรวมข้อมูลจากทะเบียนรายชื่อพนักงานและส่งข้อมูลให้แก่บริษัทประกันภัย บริษัทประกันภัยหรือตัวแทนประกันภัยจะมิได้มีการเก็บข้อมูลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ดังนั้น สิ่งที่บริษัทประกันภัยจะต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือ

2.3.4.1 แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ ซึ่งการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต้องได้รับการยกเว้นให้สามารถ เก็บ ใช้ และเปิดเผยได้ตามมาตรา 24 หรือมาตรา 26[57]

2.3.4.2 ในกรณีที่มีข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ไม่เข้าข้อยกเว้นให้เก็บ ใช้ และเปิดเผยได้ตามมาตรา 24 หรือมาตรา 26 ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน ซึ่งความยินยอมเช่นว่านั้น ต้องมีทั้งความยินยอมที่เจ้าของข้อมูลส่วนบุคคลให้แก่องค์กรที่ทำงาน และให้แก่บริษัทประกันภัยด้วย เพราะทั้งองค์กรที่ทำงาน และบริษัทประกันภัยต่างมิได้มีการประมวลผลข้อมูลภายใต้คำสั่งของอีกฝ่ายหนึ่ง ทั้งสองฝ่ายจึงมีสถานะเป็นผู้ควบคุมข้อมูล ไม่สามารถอาศัยผลประโยชน์จากหนังสือขอความยินยอมของอีกฝ่ายได้ เว้นแต่บริษัทผู้เอาประกันภัยและบริษัทรับประกันภัยจะได้มีการตกลงร่วมกันเพื่อทำหนังสือขอความยินยอมฉบับเดียวกัน

---

[56] ‘ตัวแทน/นายหน้าประกันภัย’ (เว็บไซต์การศึกษา, สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย) <https://www.oic.or.th/th/education/broker> สืบค้นเมื่อวันที่ 29 ธันวาคม 2564.

[57] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25.

Ref. code: 25646301033624ADV

2.3.5 ปัญหาการให้ความยินยอมที่มากเกินความจำเป็น

การดำเนินการในแต่ละขั้นตอนตลอดสัญญาประกันภัยนั้น มีการขอความยินยอมและให้ความยินยอมต่อผู้ควบคุมข้อมูลหลายราย และมีวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่หลากหลาย สร้างความยุ่งยากให้ผู้ที่เกี่ยวข้องในสัญญาประกันภัย และมิได้ก่อประโยชน์ใดแก่การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเพิ่มเติม เนื่องจาก ผู้ที่เข้าทำสัญญาประกันภัยย่อมรู้ดีอยู่แล้วว่าตนจะต้องให้ข้อมูลส่วนบุคคลของตนเพื่อการพิจารณารับประกันภัย หรือการเบิกค่าสินไหมทดแทน โดยผู้เขียนของยกตัวอย่างธุรกรรมที่อาจเกิดขึ้นตามสัญญาประกันภัยซึ่งมีผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่มีความเกี่ยวข้องหลายราย ดังนี้

ยกตัวอย่าง นาย ก. เป็นลูกจ้างบริษัท ข. ซึ่งทำประกันสุขภาพแบบกลุ่มผ่านนายหน้าประกันภัย ค. โดยมี ง. เป็นบริษัทประกันภัยที่รับประกันภัยดังกล่าว

จากกรณีตัวอย่าง นาย ก. ต้องให้ความยินยอมโดยชัดแจ้งเพื่อเปิดเผยข้อมูลสุขภาพของตน ดังนี้

1. ให้ความยินยอมต่อบริษัท ข. ในการเก็บ ใช้ เปิดเผยข้อมูลต่อบริษัท ค. และบริษัท ง. เพื่อทำสัญญาประกันสุขภาพแบบกลุ่ม

2. ให้ความยินยอมต่อบริษัท ค. เพื่อเก็บ ใช้ และเปิดเผยข้อมูลสุขภาพในการทำประกันภัยกับบริษัท ง.

3. ให้ความยินยอมต่อบริษัท ง. เพื่อพิจารณารับประกันภัย

ทั้งนี้ ในขั้นตอนดังกล่าวอาจมีการตกลงกันโดยผู้ควบคุมข้อมูลส่วนบุคคลทุกรายเพื่อขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นฉบับเดียวเพื่ออำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคล หรือจัดทำแยกจากกันก็ได้ ซึ่งการดำเนินการต่างๆ เหล่านี้ ย่อมส่งผลต่อต้นทุนในเชิงการบริการจัดการของผู้ประกอบธุรกิจที่เกี่ยวข้อง อันอาจส่งผลต่อค่าเบี้ยประกันภัยที่ต้องปรับตัวสูงขึ้น ทำให้กระทบต่อผู้เอาประกันภัยเช่นกัน

นอกจากนี้ เมื่อกำหนดให้มีการขอความยินยอมแล้ว สิทธิที่จะเกิดขึ้นต่อไปคือสิทธิในการถอนความยินยอม ซึ่งหากผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลในกระบวนการที่กล่าวมาทั้งหมด ได้เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามความยินยอมไปแล้ว และเจ้าของข้อมูลส่วนบุคคลยกเลิกความยินยอมในระหว่างอายุสัญญาประกันภัย ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลย่อมไม่สามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลดังกล่าวได้ อันส่งผลกระทบให้ไม่สามารถปฏิบัติหน้าที่ตามสัญญาประกันภัยต่อไปได้ และสัญญาประกันภัยย่อมไม่อาจบรรลุวัตถุประสงค์ของสัญญา เช่น ผู้เอาประกันภัยในขณะ

Ref. code: 25646301033624ADV

ทำประกันภัยได้แจ้งข้อมูลสุขภาพว่าตนเป็นโรคเบาหวาน โดยบริษัทประกันภัยได้รับประกันสุขภาพของลูกค้าดังกล่าวโดยมีข้อยกเว้นโรคเบาหวาน และการเจ็บป่วยที่เกิดจากโรคเบาหวาน ต่อมา เมื่อผู้เอาประกันภัยมีอาการเจ็บป่วยจึงขอเบิกค่ารักษาพยาบาลโดยไม่ยินยอมให้บริษัทประกันภัยเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลสุขภาพของตนต่อไป เช่นนี้ บริษัทประกันภัยก็ไม่อาจพิจารณาค่าสินไหมทดแทนได้ เนื่องจาก ไม่มีข้อมูลเพียงพอที่จะพิจารณาและจ่ายค่าสินไหมทดแทนตามวัตถุประสงค์ของสัญญาประกันภัย เป็นต้น

อย่างไรก็ตาม แม้เจ้าของข้อมูลส่วนบุคคลมิได้ให้ความยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว เจ้าของข้อมูลส่วนบุคคลก็อาจใช้สิทธิอื่นๆ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ เช่น สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน สิทธิในการคัดค้านการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลของตน สิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคลของตน หรือสิทธิในการขอแก้ไขข้อมูลของตนให้ถูกต้อง[58] เป็นต้น สิทธิที่ของเจ้าของข้อมูลส่วนบุคคลดังกล่าวเพียงพอที่จะให้ความเป็นธรรมต่อเจ้าของข้อมูลส่วนบุคคลแล้ว ดังนั้น ผู้เขียนจึงเห็นว่ากรณีการขอความยินยอมในวัตถุประสงค์ที่ไม่จำเป็นดังกล่าว เป็นประเด็นที่ต้องศึกษาเพื่อหาวิธีการทางกฎหมายในการลดปัญหาดังกล่าว ตามแนวทางของกฎหมายต่างประเทศ หรือวิธีการที่อาจดำเนินการได้อื่นๆ เพื่อจัดทำเป็นข้อเสนอแนะทางกฎหมายต่อไป

[58] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล.

Ref. code: 25646301033624ADV

บทที่ 3
วิเคราะห์กฎหมาย แนวทางการกำกับดูแล และแนวปฏิบัติในประเทศไทย

3.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่ประกาศในราชกิจจานุเบกษาตั้งแต่วันที่ 27 พฤษภาคม พ.ศ. 2562 โดยให้มีผลบังคับในวันดังกล่าว ยกเว้นบทบัญญัติในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7 ความในมาตรา 95 และมาตรา 96 ให้บังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป แต่เมื่อล่วงพ้นจนเวลาใกล้ครบกำหนด ปรากฏว่ามีประกาศพระราชกฤษฎีกาประกาศให้เลื่อนการบังคับใช้ถึงสองครั้ง โดยในการเลื่อนครั้งที่สองนี้ ให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ. 2565 ด้วยเหตุผลว่าหน่วยงานต่างๆ โดยเฉพาะในภาคเอกชนไม่พร้อมในการดำเนินการตามกฎหมาย เนื่องจากอยู่ในช่วงวิกฤติการณ์แพร่ระบาดของไวรัสโควิด-19[1] ซึ่งผู้เขียนมีความเห็นว่าแม้มิได้มีวิกฤติการณ์แพร่ระบาดของไวรัสโควิด-19 การบริหารจัดการเพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนก็ถือเป็นเรื่องยากในบริบทของสังคมไทย เพราะสาเหตุคือการขาดบุคลากรที่มีความรู้ความเข้าใจเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงก่อนหน้านี้ตลอดปี พ.ศ. 2562 ถึงปี พ.ศ.2564 นั้น ภาครัฐมิได้มีการประกาศแนวปฏิบัติ ออกกฎหมายลำดับรอง หรือสื่อสารผ่านช่องทางอื่นๆ เพื่อให้เกิดความรู้ความเข้าใจในการปฏิบัติตามกฎหมายอย่างถูกต้อง นอกจากนี้ความตระหนักเรื่องสิทธิในข้อมูลส่วนบุคคลของสังคมไทยนั้น มิได้มีความเด่นชัดเหมือนความตระหนักเรื่องความเป็นส่วนตัวหรือข้อมูลส่วนบุคคลในต่างประเทศ โดยในช่วงแรกของการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจจำนวนมากดำเนินการได้ไม่ตรงตามวัตถุประสงค์ของกฎหมาย โดยเฉพาะเรื่องของการขอความยินยอมเพื่อวัตถุประสงค์ที่กฎหมายกำหนดให้สามารถเก็บ ใช้ เปิดเผยได้โดยไม่ต้องขอความยินยอม เช่น การขอความยินยอมเพื่อปฏิบัติตามสัญญา

[1] ‘เลื่อนบังคับใช้ พ.ร.บ.ข้อมูลบุคคล’ ไทยรัฐฉบับพิมพ์ (20 พฤษภาคม 2563) <https://www.thairath.co.th/business/economics/1848624> สืบค้นเมื่อวันที่ 16 มกราคม 2565.

Ref. code: 25646301033624ADV

การขอความยินยอมเพื่อทำหน้าที่ตามกฎหมาย การขอความยินยอมเพื่อปฏิบัติตามผลประโยชน์โดยชอบด้วยกฎหมาย[2] เป็นต้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น แบ่งออกเป็น 7 หมวด โดยมีทั้งหมด 96 มาตรา มีเนื้อหาครอบคลุมถึงเรื่องต่างๆ ดังต่อไปนี้

3.1.1 คุณสมบัติ วาระการดำรงตำแหน่ง การพ้นสภาพ การประชุม หน้าที่ และอำนาจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3.1.2 มาตรการการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่มีความอ่อนไหว รวมถึง ฐานทางกฎหมาย ข้อยกเว้น และความยินยอมเพื่อการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่มีความอ่อนไหว

3.1.3 สิทธิของเจ้าของข้อมูลส่วนบุคคล อันได้แก่

3.1.3.1 สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตน

3.1.3.2 สิทธิในการขอให้โอนข้อมูลของตนให้แก่บุคคลภายนอก

3.1.3.3 สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน

3.1.3.4 สิทธิขอให้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

3.1.3.5 สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล

3.1.3.6 สิทธิในการขอให้ข้อมูลส่วนบุคคลของตนถูกต้องและเป็นปัจจุบัน

3.1.4 หน้าที่ของผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3.1.5 ขอบเขตการร้องเรียน และผู้รับเรื่องร้องเรียน และการบริหารจัดการเรื่องร้องเรียนอันเกี่ยวข้องกับพระราชบัญญัตินี้

---

[2] ‘นโยบายข้อมูลส่วนบุคคล และ แบบขอความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล’ (thaipdpa.com) <https://www.thaipdpa.com/upload /ex_form/%E0%B8%95%E0%B8%B1%E0%B8%A7%E0%B8%AD%E0%B8%A2%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%99%E0%B9%82%E0%B8%A2%E0%B8%9A%E0%B8%B2%E0%B8%A2%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B9%81%E0%B8%9A%E0%B8%9A%E0%B8%82%E0%B8%AD%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A2%E0%B8%B4%E0%B8%99%E0%B8%A2%E0%B8%AD%E0%B8%A1.pdf> สืบค้นเมื่อวันที่ 28 มีนาคม 2565.

Ref. code: 25646301033624ADV

3.1.6 ความรับผิดทางแพ่ง และบทกำหนดโทษ

และข้อมูลส่วนอื่นๆ ที่เกี่ยวข้องกับขอบเขตการบังคับใช้กฎหมาย และบทเฉพาะกาลต่างๆ

นอกจากเรื่องความยินยอมและฐานกฎหมายอื่นที่มีการอภิปรายไปใน บทที่ 2 ของรายงานฉบับนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีหัวข้อที่น่าสนใจซึ่งเกี่ยวข้องกับรายงานฉบับนี้คือ เรื่องการระบุถึงขอบเขตของกฎหมายเฉพาะ หรือกฎหมายกำกับดูแลต่างๆ ที่กำกับดูแลกิจการ หรือหน่วยงานใดอันเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ก่อนพระราชบัญญัติบังคับใช้ โดยกำหนดให้บังคับใช้ตามกฎหมายนั้น เว้นแต่ การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล บทกำหนดโทษ และเรื่องร้องเรียนให้พิจารณาบังคับตามพระราชบัญญัติฉบับนี้เป็นการเพิ่มเติม[3] อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีบทบัญญัติถึงกรณีที่มีข้อกฎหมายหรือแนวปฏิบัติใดขัดหรือแย้งกับพระราชบัญญัติดังกล่าว รวมถึง ไม่มีบทบัญญัติที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานกำกับดูแลใดสามารถกำหนดบทบัญญัติหรือแนวปฏิบัติของภาคธุรกิจเกี่ยวกับพระราชบัญญัตินี้เป็นอย่างอื่นนอกเหนือขอบเขตที่พระราชบัญญัติกำหนดไว้ โดยมิได้ตราเป็นพระราชกฤษฎีกา

3.2 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้ออกประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 เพื่อกำหนดแนวทางการดำเนินการของบริษัทประกันชีวิต นายหน้าประกันชีวิต และตัวแทนประกันชีวิตให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และเพื่อให้การทำธุรกิจประกันชีวิตมีการคุ้มครองข้อมูลส่วนบุคคลที่จำเป็นต่อการพิจารณารับประกันภัย การปฏิบัติตามสัญญาประกันภัย และการให้บริการลูกค้าอย่างมีประสิทธิภาพ และเพื่อประโยชน์สาธารณะ[4]

---

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 3.

[4] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564.

Ref. code: 25646301033624ADV

ประกาศดังกล่าวมีเนื้อหาที่กำหนดแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยออกมาเพื่อกำกับดูแลผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจประกันชีวิตตามกฎหมาย ตัวแทนประกันชีวิต และนายหน้าประกันชีวิต แบ่งออกเป็น 3 หมวด รวม 35 ข้อ หมวดที่ 1 เป็นข้อกำหนดสำหรับบริษัทประกันชีวิต หมวดที่ 2 เป็นข้อกำหนดสำหรับตัวแทนประกันชีวิต และหมวดที่ 3 เป็นข้อกำหนดสำหรับนายหน้าประกันชีวิต ดังนี้

3.2.1 บทบาทหน้าที่ของบริษัทประกันชีวิต

3.2.1.1 กำหนดแนวปฏิบัติในการสื่อสารนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงลูกค้า เมื่อมีการแก้ไขเปลี่ยนแปลงต้องสื่อสารนโยบายซ้ำ โดยต้องสื่อสารผ่านช่องทางที่ใช้ในการติดต่อกับลูกค้า[5]

3.2.1.2 ให้แบ่งประเภทข้อมูลส่วนบุคคลเพื่อเก็บ ใช้ และเปิดเผย เป็นข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งหากข้อมูลที่เก็บ ใช้ หรือเปิดเผย มีความเสี่ยงสูงที่อาจการกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล ต้องจัดให้มีการประเมินผลกระทบด้านข้อมูลส่วนบุคคลด้วย[6]

3.2.1.3 ให้ขอความยินยอมสำหรับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ไม่อาจอ้างฐานกฎหมายอื่นได้ เช่น การขอความยินยอมเพื่อการตลาดแบบตรงหรือการสื่อสารทางการตลาดที่ลูกค้าไม่อาจคาดหมายได้ หรือ การซื้อข้อมูลจากบริษัทอื่น เป็นต้น[7]

3.2.1.4 กำหนดให้ การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญาประกันภัยไปจนถึงกระบวนการจ่ายค่าสินไหมทดแทน เป็นการจำเป็นเพื่อปฏิบัติตามสัญญา

3.2.1.5 กำหนดให้ การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกค้าสำหรับการทำการตลาดแบบตรง หรือการสื่อสารทางการตลาดที่ลูกค้าอาจคาดหมายได้สำหรับผลิตภัณฑ์ที่ลูกค้ารายเดิมได้ซื้อไปแล้ว เป็นฐานประโยชน์โดยชอบด้วยกฎหมาย

---

[5] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 8.

[6] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 3.

[7] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 4.

Ref. code: 25646301033624ADV

3.2.1.6 กำหนดให้การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของลูกค้าเพื่อการจัดทำฐานข้อมูลเกี่ยวกับการฉ้อฉลประกันภัย และการส่งข้อมูลให้ คปภ. ตามกฎหมายกำกับดูแลเป็นฐานการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล

3.2.1.7 กำหนดให้ต้องขอความยินยอมโดยชัดแจ้งในการเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว เว้นแต่กรณีการเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวจากเจ้าของข้อมูล หรือบุคคลอื่นที่เกี่ยวข้องและจำเป็นต่อการพิจารณารับประกันภัย พิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทน ถือเป็นฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์อันเกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ[8]

3.2.1.8 กำหนดแนวปฏิบัติในการขอความยินยอมจากลูกค้า ผู้มุ่งหวัง หรือบุคคลที่เกี่ยวข้องกับการทำประกันภัย โดยกำหนดให้ผู้ควบคุมสามารถขอคำรับรองจากผู้เอาประกันภัยได้[9] รวมถึงกำหนดแนวปฏิบัติสำหรับการถอนความยินยอมด้วย[10]

3.2.1.9 กำหนดให้ในกิจการรับประกันชีวิต บริษัทที่รับประกันชีวิตเป็นผู้ควบคุมข้อมูล เว้นแต่ จะได้ดำเนินการประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูลอื่น[11] พร้อมทั้งกำหนดหน้าที่เพิ่มเติมสำหรับกรณีที่บริษัทประกันเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[12]

หลักสำคัญที่เกี่ยวข้องกับหัวข้อการศึกษา คือแนวปฏิบัติของธุรกิจประกันชีวิตต่อข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งประกาศฉบับนี้กำหนดไว้ว่า บริษัทประกันชีวิตอาจอาศัยฐาน

---

[8] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 5.

[9] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 6.

[10] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 7.

[11] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 10.

[12] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 11-14.

Ref. code: 25646301033624ADV

ทางกฎหมายอื่นในการเก็บ ใช้ เปิดเผย โดยไม่ต้องขอความยินยอม เช่น ฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ[13] สำหรับกรณีดังนี้

(1) การเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้า คู่สมรส ครอบครัวของลูกค้าหรือบุคคลอื่นที่เกี่ยวข้อง ในการพิจารณารับประกันภัย การเอาประกันภัยต่อ พิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัยแต่ละประเภท หรือชดใช้ค่าสินไหมทดแทนแต่ละประเภท

(2) การเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นเพื่อเปิดเผยให้สำนักงานกำกับและส่งเสริมการประกอบธุรกิจประกันภัยตามประกาศที่เกี่ยวข้อง เรื่อง ฉ้อฉลประกันภัย

(3) การเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นเพื่อเปิดเผยให้สำนักงานกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเพื่อประโยชน์ในการกำกับดูแลและส่งเสริมการประกอบธุรกิจประกันภัย[14]

การอ้างถึงฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยนั้น ในปัจจุบัน ยังไม่มีกฎหมาย หรือ แนวปฏิบัติ หรือคำสั่งใดจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานที่กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยตรงมารับรองการตีความเช่นว่านั้น รวมถึง เนื้อหาในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็ไม่มีการระบุถึงความหมาย เนื้อหา หรือแนวทางการตีความฐานการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ ตามมาตรา 26 (5) (จ) ไว้ อย่างไรก็ตาม พระราชบัญญัติดังกล่าว ได้กำหนดให้อำนาจหน่วยงานกำกับดูแลอาจกำหนดแนวปฏิบัติก่อนพระราชบัญญัติใช้บังคับได้ แต่แนวปฏิบัติที่เกี่ยวกับการเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลให้บังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเพิ่มเติมด้วย[15] และหากเป็นกรณีที่มีการกำหนดข้อยกเว้นสำหรับกิจการใดเพื่อการเก็บ ใช้ หรือเปิดเผยข้อมูลในลักษณะเฉพาะใดก็ตาม ต้องมีการตราเป็นพระราชกฤษฎีกา[16] การนำฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะมาใช้กับข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อธุรกรรมในข้อ (2)

---

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26.

[14] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 5.

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 3.

[16] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 วรรคสอง.

Ref. code: 25646301033624ADV

และ ข้อ (3) นั้น มิอาจปฏิเสธได้ว่าเป็นการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ อันเนื่องมาจากเป็นหน้าที่ตามกฎหมายของผู้อยู่ภายใต้การกำกับดูแลที่ต้องปฏิบัติตามหน่วยงานกำกับดูแลเพื่อวัตถุประสงค์ในการติดตาม และการกำกับให้เกิดความมั่นใจว่าธุรกิจประกันภัยนั้น ได้ดำเนินไปในทิศทางที่ถูกต้อง แต่การอ้างฐานดังกล่าวในวัตถุประสงค์การเก็บ ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม (1) นั้น อาจมีประเด็นปัญหาที่ต้องพิจารณาถึงการใช้ฐานกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญได้ นอกจากนี้ การเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของคู่สมรส ครอบครัว หรือผู้ที่เกี่ยวข้องนั้น เป็นการเก็บข้อมูลจากแหล่งข้อมูลอื่น ซึ่งต้องห้ามตามมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงเป็นอีกหนึ่งกรณีปัญหาว่าข้อกำหนดดังกล่าวของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยนั้น อาจมีการตีความแตกต่างจากวัตถุประสงค์เดิมของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการจะทำให้แนวปฏิบัติที่ตีความเช่นนี้มีประสิทธิผลสูงสุดนั้น ต้องมีการแก้ไขเพิ่มเติมกฎหมาย หรือการเพิ่มเติมแนวทางการตีความ หรือการรับรองแนวทางการตีความโดยผู้มีอำนาจโดยตรง คือคณะกรรมการคุ้มครองข้อมูลส่วนบคคล

นอกจากการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวของบริษัทประกันชีวิตข้างต้นแล้ว ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 ยังมีข้อกำหนดที่เกี่ยวกับการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวของตัวแทนและนายหน้าประกันภัย ซึ่งกำหนดไว้ ดังนี้

3.2.2 ข้อกำหนดซึ่งเกี่ยวกับตัวแทนประกันชีวิต

3.2.2.1 ตัวแทนประกันชีวิตเป็นผู้ประมวลข้อมูลส่วนบุคคลของบริษัทประกันชีวิต[17]

[17] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 15.

Ref. code: 25646301033624ADV

3.2.2.2 ตัวแทนประกันชีวิตสามารถอาศัยฐานปฏิบัติตามกฎหมายเรื่องประโยชน์สาธารณะที่สำคัญในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าได้เช่นเดียวกันกับบริษัทประกันชีวิต[18]

3.2.3 ข้อกำหนดซึ่งเกี่ยวกับนายหน้าประกันชีวิต

3.2.3.1 นายหน้าประกันชีวิตเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่กำหนดแนวทางและแนวปฏิบัติของตนเอง[19]

3.2.3.2 นายหน้าประกันชีวิตสามารถอาศัยฐานทางกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลสุขภาพของลูกค้าได้เช่นเดียวกันกับบริษัทประกันชีวิต[20]

หากพิจารณาแล้ว สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเป็นหน่วยงานกำกับดูแลซึ่งมีอำนาจกำกับดูแลธุรกิจประกันภัยตามพระราชบัญญัติคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย พ.ศ. 2550 จึงอาจกำหนดแนวปฏิบัติให้กับธุรกิจภายใต้การกำกับปฏิบัติตามได้ แต่ข้อกำหนดนั้น ต้องไม่ขัดหรือแย้งกับวัตถุประสงค์ของกฎหมายหลัก หรือเกินกว่าขอบเขตของกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะหลักการขอความยินยอมซึ่งควรต้องพิจารณาประกอบกับหลักการและเจตนารมณ์ของกฎหมายแม่แบบ หรือ GENERAL DATA PROTECTION REGULATION และกฎหมายหรือแนวปฏิบัติของประเทศอื่นๆ ประกอบ ดังนั้น การจะอ้างฐานปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญในการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าก็อาจมีมุมที่ต้องพิจารณาในหลากหลายมิติ นอกจากนี้ ผู้ที่มีบทบาทหน้าที่ในการกำหนดว่าการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ตามฐานกฎหมาย หรือที่เป็นข้อยกเว้นไม่ต้องขอความยินยอมสำหรับข้อมูลส่วน

---

[18] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 22 2) ข.

[19] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 24.

[20] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 ข้อ 26.

Ref. code: 25646301033624ADV

บุคคลหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น ควรเป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยตรง[21] อย่างไรก็ตาม ผู้ปฏิบัติงานในภาคธุรกิจประกันภัยก็ได้รับประโยชน์ในการปฏิบัติงานที่สะดวก รวดเร็ว ประหยัดต้นทุนมากขึ้น ส่วนผู้เอาประกันภัยทั้งที่เป็นเจ้าของข้อมูลส่วนบุคคล และมิใช่เจ้าของข้อมูลส่วนบุคคลก็ได้รับความสะดวกในการเข้าทำประกันภัย รวมถึงความสะดวกขั้นตอนของการจ่ายค่าสินไหมทดแทน และประโยชน์สำหรับค่าเบี้ยประกันภัยที่มีราคาถูก เนื่องจากต้นทุนในการทำประกันภัยไม่สูงเกินไป ผู้ปฏิบัติงานในภาคธุรกิจประกันภัยส่วนใหญ่จึงมีความคิดเห็นสนับสนุนแนวทางที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้ประกาศกำหนด[22]

นอกจากนี้ หลังจากมีประกาศแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวแล้ว ปรากฏว่ามีคำสั่งนายทะเบียนที่ 2/2565 เรื่อง หลักเกณฑ์การให้ความเห็นชอบ แบบและข้อความใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม และใบแถลงของผู้ชำระเบี้ยประกันภัยแบบมาตรฐาน ลงวันที่ 28 มกราคม 2565 อันเป็นการกำหนดแบบมาตรฐานของใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม ทั้งชนิดไม่มีคำถามสุขภาพ มีคำถามสุขภาพอย่างสั้น และมีคำถามสุขภาพอย่างละเอียด ซึ่งเมื่อพิจารณาตามแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยแล้ว ต้องไม่ปรากฏส่วนของการขอความยินยอมเรื่องการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวแล้ว แต่แบบมาตรฐานดังกล่าวยังคงปรากฏส่วนการขอความยินยอมอยู่ ดังภาพ[23]

---

[21] สัมภาษณ์ทางโทรศัพท์ สุวรรณโชติ ศิริมหาศาล, ที่ปรึกษาด้านการพัฒนาระบบและวิทยากรเรื่องข้อมูลส่วนบุคคล, สำนักงานพัฒนารัฐบาลดิจิทัล, (17 กรกฎาคม 2565).

[22] สัมภาษณ์ทาง Google Meet รุ่งเรือง สัมฤทธิ์ทรัพย์, เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล, บริษัท เอเอสเอ็นโบรกเกอร์ จำกัด (มหาชน), (16 กรกฎาคม 2565).

[23] คำสั่งนายทะเบียนที่ 2/2565 เรื่อง หลักเกณฑ์การให้ความเห็นชอบแบบและข้อความใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม และใบแถลงของผู้ชำระเบี้ยประกันภัยแบบมาตรฐาน.

Ref. code: 25646301033624ADV

ส่วนที่ ๖ ข้อความยืนยันถ้อยแถลงหรือคำตอบในใบคำขอเอาประกันชีวิตของผู้ขอเอาประกันภัยและการให้ความยินยอม

๑. ข้าพเจ้าขอยืนยันว่าคำตอบทุกข้อในใบคำขอเอาประกันชีวิตนี้ รวมถึงถ้อยแถลงที่ได้ตอบกับแพทย์ผู้ตรวจสุขภาพเป็นความจริงทุกประการ ซึ่งข้าพเจ้าเข้าใจดีว่า หากข้าพเจ้าไม่แถลงข้อความจริง บริษัทอาจจะปฏิเสธการรับประกันภัยและปฏิเสธการจ่ายเงินตามกรมธรรม์ประกันภัย

๒. ข้าพเจ้า และ/หรือผู้แทนโดยชอบธรรม ยินยอมให้แพทย์ หรือบริษัทประกันภัย หรือสถานพยาบาล หรือบุคคลอื่นใด ซึ่งมีข้อมูลสุขภาพ ความพิการ พฤติกรรมทางเพศ ข้อมูลชีวภาพ ข้อมูลพันธุกรรม เชื้อชาติ ของข้าพเจ้า และ/หรือผู้เยาว์ ที่ผ่านมา หรือจะมีขึ้นต่อไปในอนาคต สามารถเปิดเผยข้อมูลดังกล่าว ให้แก่บริษัทหรือผู้แทนของบริษัท เพื่อการขอเอาประกันภัย การพิจารณารับประกันภัย หรือการจ่ายเงินตามกรมธรรม์ประกันภัยได้

๓. ข้าพเจ้า และ/หรือผู้แทนโดยชอบธรรม ยินยอมให้บริษัทเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลสุขภาพ ความพิการ พฤติกรรมทางเพศ ข้อมูลชีวภาพ ข้อมูลพันธุกรรม เชื้อชาติ ของข้าพเจ้า และ/หรือผู้เยาว์ ต่อบริษัทประกันภัยอื่น บริษัทนายหน้าประกันภัยต่อ บริษัทประกันภัยต่อ หน่วยงานที่มีอำนาจตามกฎหมาย สถานพยาบาล แพทย์ บุคลากรทางการแพทย์ ตัวแทนประกันชีวิต หรือนายหน้าประกันชีวิต เพื่อการขอเอาประกันภัย การพิจารณารับประกันภัย หรือการจ่ายเงินตามกรมธรรม์ประกันภัย

๔. ข้าพเจ้าเข้าใจดีว่า หากข้าพเจ้าเพิกถอนความยินยอมตามข้อ ๒. หรือข้อ ๓. ที่ให้ไว้กับบริษัท จะมีผลกระทบต่อการพิจารณารับประกันภัย การจ่ายเงินตามกรมธรรม์ประกันภัย หรือการให้บริการใด ๆ ที่เกี่ยวข้องกับกรมธรรม์ประกันภัย อันจะส่งผลให้บริษัทไม่สามารถปฏิบัติตามเงื่อนไขในกรมธรรม์ประกันภัย ซึ่งจะมีผลทำให้ข้าพเจ้าไม่ได้รับความคุ้มครองตามกรมธรรม์ประกันภัย

๕. ข้าพเจ้ารับทราบว่า บริษัทจะเก็บรวบรวม ใช้ เปิดเผย และ/หรือโอนข้อมูลส่วนบุคคล รวมถึงข้อมูลที่อ่อนไหวของข้าพเจ้า เพื่อการขอเอาประกันภัย การพิจารณารับประกันภัย การจ่ายเงินตามกรมธรรม์ประกันภัย ตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทที่ปรากฏใน [โปรดใส่ link นโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัท] รวมทั้งรับทราบว่า บริษัทจะเปิดเผยข้อมูลส่วนบุคคลของข้าพเจ้าแก่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) เพื่อประโยชน์ในการกำกับดูแลและส่งเสริมธุรกิจประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและกฎหมายว่าด้วยคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย รายละเอียดการเก็บรวบรวม ใช้และเปิดเผยของสำนักงาน คปภ. ปรากฏตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน คปภ. ตามที่ปรากฏบนเว็บไซต์ www.oic.or.th

๖. เมื่อข้าพเจ้าเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นใดนอกจากของข้าพเจ้าให้แก่บริษัทเพื่อการขอเอาประกันภัย การพิจารณารับประกันภัย หรือการจ่ายเงินตามกรมธรรม์ประกันภัย

(๑) ข้าพเจ้ารับรองและรับประกันว่าได้ตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลส่วนบุคคลของบุคคลอื่นที่ข้าพเจ้าให้แก่บริษัท และจะแจ้งบริษัท หากมีการเปลี่ยนแปลงใด ๆ ในข้อมูลส่วนบุคคลของบุคคลอื่นที่ได้ให้ไว้ (หากมี)

(๒) ข้าพเจ้ารับรองและรับประกันว่า ข้าพเจ้าได้รับความยินยอมหรือสามารถอาศัยฐานทางกฎหมายอื่นสำหรับการเก็บรวบรวม ใช้ เปิดเผย และ/หรือโอนข้อมูลส่วนบุคคลของบุคคลอื่นนั้นตามกฎหมายที่ใช้บังคับ

(๓) ข้าพเจ้ารับรองและรับประกันว่า ข้าพเจ้าได้แจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทแก่บุคคลอื่นนั้นแล้ว [โปรดใส่ link นโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัท ซึ่งมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผย และ/หรือโอนข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) เพื่อประโยชน์ในการกำกับดูแลและส่งเสริมธุรกิจประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและกฎหมายว่าด้วยคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ซึ่งสำนักงาน คปภ. จะเก็บรวบรวม ใช้ เปิดเผย และ/หรือโอนข้อมูลส่วนบุคคลของบุคคลอื่นตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน คปภ. ตามที่ปรากฏบนเว็บไซต์ www.oic.or.th]

(๔) ข้าพเจ้ารับรองและรับประกันว่าบริษัทและสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยสามารถเก็บรวบรวม ใช้ เปิดเผย และ/หรือโอนข้อมูลส่วนบุคคลของบุคคลอื่นนั้นตามวัตถุประสงค์ที่กำหนดไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทและสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยที่เกี่ยวข้อง ซึ่งอาจมีการแก้ไขเป็นครั้งคราว รวมถึงวัตถุประสงค์ทั้งหมดที่กำหนดไว้ในเอกสารฉบับนี้ และที่เกี่ยวข้องกับการเอาประกันภัย

(ลงชื่อ).....

(.....)

ผู้ขอเอาประกันภัย

ภาพที่ 3.1 ส่วนที่ 6 ของใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม ชนิดมีคำถามสุขภาพอย่างสั้น ที่มาจากคำสั่งนายทะเบียนที่ 2/2565 เรื่อง หลักเกณฑ์การให้ความเห็นชอบแบบและข้อความ ใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม และใบแถลงของผู้ชำระเบี้ยประกันภัย แบบมาตรฐาน

แบบมาตรฐานเช่นนี้ บริษัทรับประกันชีวิตสามารถนำไปใช้ได้โดยไม่ต้องขออนุญาตจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยก่อน แต่หากมีการเปลี่ยนแปลงข้อความ ความหมาย หรือเงื่อนไขของผลิตภัณฑ์ไปจากแบบมาตรฐาน เช่น การตัดส่วนการขอความยินยอมออก การเพิ่มเติมเงื่อนไขการรับประกันชีวิต เป็นต้น บริษัทประกันชีวิตต้องได้รับอนุญาตจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยก่อน จึงจะสามารถ

Ref. code: 25646301033624ADV

นำแบบฟอร์มที่มีความแตกต่างไปใช้ได้ ดังนั้น จากภาพแบบมาตรฐานด้านบน ทำให้ผู้เขียนเห็นเป็นประเด็นปัญหาต่อไปว่า คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยก็ยังมิได้มีการปรับใช้ประกาศประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 อย่างเด็ดขาด เพื่อมิให้เกิดข้อกังวลต่อผู้ประกอบธุรกิจที่เกี่ยวข้อง และผู้เอาประกันภัย ดังนั้น เพื่อทำให้เกิดความมั่นใจของผู้ประกอบธุรกิจ และสร้างความชัดเจนต่อผู้เอาประกันภัย ในการอ้างฐานการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญในการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าประกันภัยนั้น ผู้เขียนเห็นว่าต้องมีแนวทางการแก้ไขกฎหมาย หรือแนวทางการตีความ หรือแนวทางการรับรองการตีความพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564

3.3 ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 นั้น มีเนื้อหาเป็นการกำหนดแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยออกมาเพื่อกำกับดูแลผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจประกันวินาศภัยตามกฎหมาย ตัวแทนประกันวินาศภัย และนายหน้าประกันวินาศภัย แบ่งออกเป็น 3 หมวด รวม 35 ข้อ เช่นเดียวกันกับประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 ที่ได้อภิปรายไปแล้วในข้อ 3.2 โดยประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 นี้ มีเนื้อหาในการกำหนดบทบาทหน้าที่ของบริษัทประกันวินาศภัย ตัวแทนประกันวินาศภัย และนายหน้าประกันวินาศภัยที่มิได้มีความแตกต่างไปจากบทบาทหน้าที่ของบริษัทประกันชีวิต ตัวแทนประกันชีวิต และนายหน้าประกันชีวิต

ผู้เขียนจึงขอยกข้อสังเกต และคำอภิปรายในข้อ 3.2 มาใช้กับผู้ประกอบธุรกิจประกันวินาศภัย ตัวแทนประกันวินาศภัย และนายหน้าประกันวินาศภัยด้วย อย่างไรก็ตาม ในการประกอบธุรกิจประกันวินาศภัยนั้น มีผู้ที่เกี่ยวข้องและอยู่ภายใต้การกำกับดูแลของ

Ref. code: 25646301033624ADV

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเพิ่มเติมอีกหนึ่งราย ได้แก่ ผู้ประเมินวินาศภัยตามกฎหมายว่าด้วยการประกันวินาศภัย ซึ่งคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยก็ได้มีการออกประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้เอาประกันภัยสำหรับการตรวจสอบและประเมินวินาศภัย พ.ศ. 2564 ด้วย โดยมีเนื้อหาทั้งหมด 14 ข้อ กำหนดหน้าที่ผู้ประเมินวินาศภัยให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคล และมีการแจ้งไปยังผู้เอาประกันภัยเมื่อมีการเปลี่ยนแปลง[24] นอกจากนี้ ยังมีการกำหนดแนวปฏิบัติในการขอและการถอนความยินยอมจากผู้เอาประกันภัย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลหลายประการที่สอดคล้องกับแนวปฏิบัติของบริษัทประกันภัย โดยประกาศฉบับนี้ กำหนดให้ผู้ประเมินวินาศภัยเป็นผู้ควบคุมข้อมูลส่วนบุคคล[25] เช่นเดียวกับบริษัทประกันภัยและนายหน้าประกันภัย

ในส่วนของแบบมาตรฐานสำหรับการรับประกันวินาศภัยนั้น ยังไม่พบว่ามีประกาศออกมาหลังจากแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศแล้ว อย่างไรก็ตาม หากเป็นแบบมาตรฐานของประกันสุขภาพ ยกตัวอย่างเช่น ใบคำขอเอาประกันภัย กรมธรรม์ประกันภัยสุขภาพเฉพาะโรคแบบส่วนบุคคล ดังภาพ

---

[24] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้เอาประกันภัยสำหรับการตรวจสอบและประเมินวินาศภัย พ.ศ.2564 ข้อ 3.

[25] ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้เอาประกันภัยสำหรับการตรวจสอบและประเมินวินาศภัย พ.ศ.2564 ข้อ 10.

Ref. code: 25646301033624ADV

ชื่อและที่อยู่บริษัท

ใบคำขอเอาประกันภัย
กรมธรรม์ประกันภัยสุขภาพเฉพาะโรค แบบส่วนบุคคล

1. รายละเอียดผู้ขอเอาประกันภัย
ชื่อ-นามสกุล .....
วัน/เดือน/ปีเกิด ..... อายุ.....ปี น้ำหนัก/ส่วนสูง ...../.....เชื้อชาติ / สัญชาติ ...../.....
เลขที่บัตรประจำตัวประชาชน .....

ที่อยู่ที่ติดต่อได้ .....
โทรศัพท์บ้าน ..... โทรศัพท์มือถือ ..... อีเมล์.....
อาชีพ.....สถานที่ทำงานหรือหน่วยงานที่สังกัด.....
ผู้รับประโยชน์.....ความสัมพันธ์กับผู้ขอเอาประกันภัย.....

2. ระยะเวลาขอเอาประกันภัย : เริ่มต้นวันที่ เวลา น. สิ้นสุดวันที่ เวลา 24.00 น.

3. แผนประกันภัยและ/หรือรายละเอียดที่ต้องการซื้อความคุ้มครอง

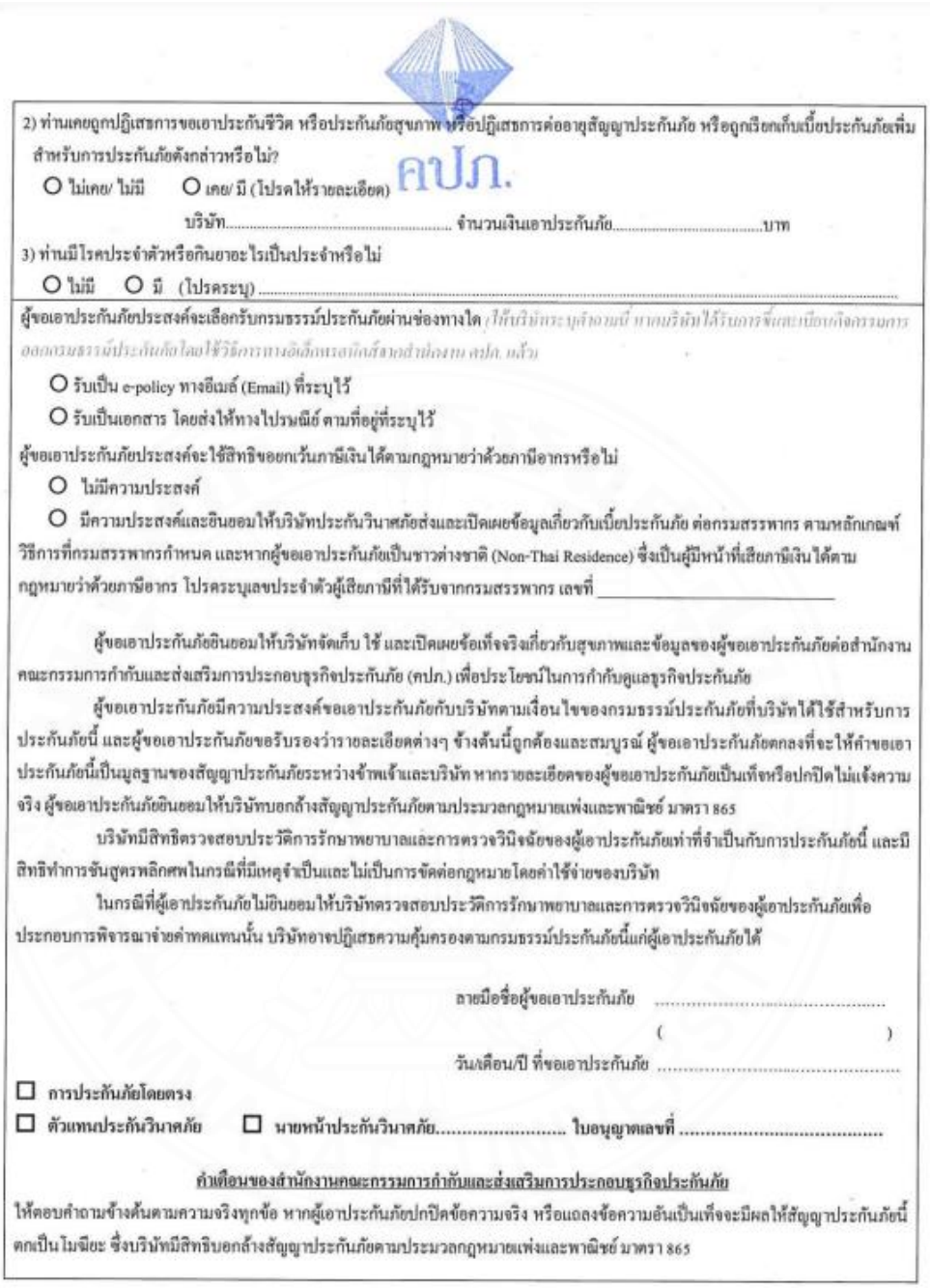
ข้อตกลงคุ้มครอง/เอกสารแนบท้าย	จำนวนเงินเอาประกันภัย (บาท)

การชำระเบี้ยประกันภัย ☐ รายปี ☐ ราย...เดือน
วิธีการชำระเบี้ยประกันภัย
O เงินสด
O ผ่านบัตรเครดิตธนาคาร _____ หมายเลขบัตรเครดิต _____ บัตรหมดอายุ _____
O ผ่านบัญชีเงินฝากธนาคาร _____ สาขา _____ บัญชีเลขที่ _____

คำถามเรื่องประวัติสุขภาพของผู้ขอเอาประกันภัย
1) ท่านมีหรือได้ขอเอาประกันชีวิต หรือประกันภัยสุขภาพไว้กับบริษัท หรือบริษัทอื่นหรือไม่?
O ไม่เคย/ ไม่มี O เคย/ มี (โปรดให้รายละเอียด)
บริษัท..... จำนวนเงินเอาประกันภัย.....บาท

ภาพที่ 3.2 ใบคำขอเอาประกันภัย กรมธรรม์ประกันภัยสุขภาพเฉพาะโรค แบบส่วนบุคคล หน้าที่ 1 ที่มาจากคำสั่งนายทะเบียนเลขที่ 62/2563 เรื่อง ให้ใช้แบบ ข้อความ และอัตราเบี้ยประกันภัยของกรมธรรม์ประกันภัยเฉพาะโรค แบบส่วนบุคคล และกรมธรรม์ประกันภัยเฉพาะโรค แบบกลุ่ม

Ref. code: 25646301033624ADV



2) ท่านเคยถูกปฏิเสธการขอเอาประกันชีวิต หรือประกันภัยสุขภาพ หรือปฏิเสธการต่ออายุสัญญาประกันภัย หรือถูกเรียกเก็บเบี้ยประกันภัยเพิ่ม สำหรับการประกันภัยดังกล่าวหรือไม่?

○ ไม่เคย/ ไม่มี ○ เคย/ มี (โปรดให้รายละเอียด)

บริษัท..... จำนวนเงินเอาประกันภัย.....บาท

3) ท่านมีโรคประจำตัวหรือกินยาอะไรเป็นประจำหรือไม่

○ ไม่มี ○ มี (โปรดระบุ).....

ผู้ขอเอาประกันภัยประสงค์จะเลือกรับกรมธรรม์ประกันภัยผ่านช่องทางใด (ให้บริษัทระบุข้อความนี้ หากบริษัทได้รับการขึ้นทะเบียนกิจกรรมการออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์จากสำนักงาน คปภ. แล้ว)

○ รับเป็น e-policy ทางอีเมล์ (Email) ที่ระบุไว้

○ รับเป็นเอกสาร โดยส่งให้ทางไปรษณีย์ ตามที่อยู่ที่ระบุไว้

ผู้ขอเอาประกันภัยประสงค์จะใช้สิทธิขอยกเว้นภาษีเงินได้ตามกฎหมายว่าด้วยภาษีอากรหรือไม่

○ ไม่มีความประสงค์

○ มีความประสงค์และยินยอมให้บริษัทประกันวินาศภัยส่งและเปิดเผยข้อมูลเกี่ยวกับเบี้ยประกันภัย ต่อกรมสรรพากร ตามหลักเกณฑ์วิธีการที่กรมสรรพากรกำหนด และหากผู้ขอเอาประกันภัยเป็นชาวต่างชาติ (Non-Thai Residence) ซึ่งเป็นผู้มีหน้าที่เสียภาษีเงินได้ตามกฎหมายว่าด้วยภาษีอากร โปรดระบุเลขประจำตัวผู้เสียภาษีที่ได้รับจากกรมสรรพากร เลขที่ _____

ผู้ขอเอาประกันภัยยินยอมให้บริษัทจัดเก็บ ใช้ และเปิดเผยข้อเท็จจริงเกี่ยวกับสุขภาพและข้อมูลของผู้ขอเอาประกันภัยต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) เพื่อประโยชน์ในการกำกับดูแลธุรกิจประกันภัย

ผู้ขอเอาประกันภัยมีความประสงค์ขอเอาประกันภัยกับบริษัทตามเงื่อนไขของกรมธรรม์ประกันภัยที่บริษัทได้ใช้สำหรับการประกันภัยนี้ และผู้ขอเอาประกันภัยขอรับรองว่ารายละเอียดต่างๆ ข้างต้นนี้ถูกต้องและสมบูรณ์ ผู้ขอเอาประกันภัยตกลงที่จะให้คำขอเอาประกันภัยนี้เป็นมูลฐานของสัญญาประกันภัยระหว่างข้าพเจ้าและบริษัท หากรายละเอียดของผู้ขอเอาประกันภัยเป็นเท็จหรือปกปิดไม่แจ้งความจริง ผู้ขอเอาประกันภัยยินยอมให้บริษัทบอกล้างสัญญาประกันภัยตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865

บริษัทมีสิทธิตรวจสอบประวัติการรักษาพยาบาลและการตรวจวินิจฉัยของผู้เอาประกันภัยเท่าที่จำเป็นกับการประกันภัยนี้ และมีสิทธิทำการชันสูตรพลิกศพในกรณีที่มีเหตุจำเป็นและไม่เป็นการขัดต่อกฎหมายโดยค่าใช้จ่ายของบริษัท

ในกรณีที่ผู้เอาประกันภัยไม่ยินยอมให้บริษัทตรวจสอบประวัติการรักษาพยาบาลและการตรวจวินิจฉัยของผู้เอาประกันภัยเพื่อประกอบการพิจารณาจ่ายค่าทดแทนนั้น บริษัทอาจปฏิเสธความคุ้มครองตามกรมธรรม์ประกันภัยนี้แก่ผู้เอาประกันภัยได้

ลายมือชื่อผู้ขอเอาประกันภัย .....

( )

วัน/เดือน/ปี ที่ขอเอาประกันภัย .....

☐ การประกันภัยโดยตรง

☐ ตัวแทนประกันวินาศภัย ☐ นายหน้าประกันวินาศภัย..... ใบอนุญาตเลขที่ .....

คำเตือนของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

ให้ตอบคำถามข้างต้นตามความจริงทุกข้อ หากผู้เอาประกันภัยปกปิดข้อความจริง หรือแถลงข้อความอันเป็นเท็จจะมีผลให้สัญญาประกันภัยนี้ตกเป็นโมฆียะ ซึ่งบริษัทมีสิทธิบอกล้างสัญญาประกันภัยตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 865

ภาพที่ 3.3 ใบคำขอเอาประกันภัย กรมธรรม์ประกันภัยสุขภาพเฉพาะโรค แบบส่วนบุคคล หน้าที่ 2 ที่มาจากคำสั่งนายทะเบียนเลขที่ 62/2563 เรื่อง ให้ใช้แบบ ข้อความ และอัตราเบี้ยประกันภัยของกรมธรรม์ประกันภัยเฉพาะโรค แบบส่วนบุคคล และกรมธรรม์ประกันภัยเฉพาะโรค แบบกลุ่ม

แบบฟอร์มมาตรฐานดังกล่าวประกาศเมื่อวันที่ 30 กันยายน พ.ศ.2563 ปรากฏข้อความเรื่องความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลผู้เอาประกันภัยเพื่อประโยชน์ใน

Ref. code: 25646301033624ADV

การกำกับดูแลของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ที่แตกต่างกับแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย แต่ยังคงมีสถานะบังคับใช้อยู่ในปัจจุบัน เว้นแต่ บริษัทประกันชีวิตหรือบริษัทประกันวินาศภัยจะได้ขออนุญาตไว้เป็นอย่างอื่น ซึ่งประเด็นนี้เห็นว่าอาจก่อให้เกิดความสับสนของผู้ปฏิบัติงานที่เกี่ยวข้องได้เช่นเดียวกันกับ ภาพที่ 3.1 ส่วนที่ 6 ของใบคำขอเอาประกันชีวิต ประเภทสามัญหรืออุตสาหกรรม ชนิดมีคำถามสุขภาพอย่างสั้น จึงควรมีการกำหนดให้นำฐานทางกฎหมายมายกเว้นการขอความยินยอมนี้ได้โดยเด็ดขาด

นอกจากนี้ เพื่อสำรวจความคิดเห็นของบุคลากรในบริษัทประกันภัย บริษัทนายหน้าประกันภัย ตัวแทนประกันภัย นายหน้าประกันภัยอิสระ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและบุคลากรในฝ่ายงานกำกับการปฏิบัติตามกฎหมายในหน่วยงานต่างๆ ซึ่งเป็นผู้มีความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เขียนได้จัดทำแบบสอบถามความคิดเห็น เรื่อง แบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง “แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564” โดยเป็นการสำรวจทางออนไลน์ตั้งแต่วันที่ 17 กรกฎาคม 2565 ถึงวันที่ 20 กรกฎาคม 2565 มีผู้ตอบแบบสำรวจทั้งหมด 47 ท่าน โดยแบ่งผลสรุปเป็น 3 ประเด็น ดังนี้

ประเด็นที่ 1 สำรวจว่าตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา ผู้ตอบแบบสอบถามพบการขอความยินยอมเพื่อเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำประกันภัยหรือไม่ โดยมีผู้ที่ตอบว่า พบการขอความยินยอม ร้อยละ 57.4 มีผู้ที่ตอบว่าไม่พบการขอความยินยอม ร้อยละ 8.5 และมีผู้ที่ตอบว่ายังไม่มีการทำประกันภัยในช่วงเวลาดังกล่าว ร้อยละ 34 ผลการตอบแบบสอบถามดังกล่าวสะท้อนว่าในปัจจุบันสัญญาประกันภัยส่วนใหญ่ยังคงมีการขอความยินยอมเพื่อเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว กล่าวคือ ผู้รับประกันภัยส่วนใหญ่ยังมิได้มีการปรับใช้ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

ประเด็นที่ 2 สำรวจความคิดเห็นของกลุ่มเป้าหมายว่าการรับประกันภัยเป็นประโยชน์สาธารณะที่สำคัญหรือไม่ มีผู้ตอบแบบสอบถามว่าใช่ ร้อยละ 61.7 และผู้ที่ตอบว่าไม่ใช่ ร้อยละ 38.3 ผลการตอบแบบสอบถามสะท้อนว่าผู้ตอบแบบสอบถามส่วนใหญ่ซึ่งเป็นบุคลากรในธุรกิจประกันภัยมีความคิดเห็นว่าการประกันภัยเป็นประโยชน์สาธารณะที่สำคัญ อย่างไรก็ตาม ยังมีผู้ที่มีความคิดเห็น

Ref. code: 25646301033624ADV

ว่าการประกันภัยนั้น ไม่ใช่ประโยชน์สาธารณะที่สำคัญอยู่เช่นกัน ซึ่งกลุ่มบุคคลเหล่านี้เมื่อต้องให้ข้อมูลส่วนบุคคลที่มีความอ่อนไหว อาจกังวลและให้ความสำคัญเรื่องการขอความยินยอม และสอบถามถึงการขอความยินยอมดังกล่าวด้วย[26] โดยผู้ที่มีความเห็นว่าการประกันภัยไม่ใช่ประโยชน์สาธารณะนั้น เป็นผู้ที่ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่มิใช่บุคลากรในธุรกิจประกันภัยถึง 10 ท่าน จากผู้ตอบคำถามว่าไม่ใช่ทั้งหมด 17 ท่าน ข้อมูลส่วนนี้สะท้อนให้เห็นว่าผู้ที่ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมิได้เป็นบุคลากรในธุรกิจประกันภัยนั้น ค่อนข้างมีความเห็นที่แตกต่างจากแนวทางการตีความที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยกำหนดเป็นแนวปฏิบัติ

ประเด็นที่ 3 สำรวจความคิดเห็นกลุ่มเป้าหมายว่าตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยที่มีการกำหนดให้การที่บริษัทประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัย อาจเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าและบุคคลอื่นที่จำเป็น เพื่อวัตถุประสงค์ในการพิจารณารับประกันภัย เอาประกันภัยต่อ การพิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัยโดยไม่ต้องขอความยินยอม ผู้ตอบแบบสอบถามเห็นด้วยหรือไม่นั้น มีผู้ตอบแบบสอบถามว่าเห็นด้วย ร้อยละ 61.7 และผู้ที่ตอบว่าไม่เห็นด้วย ร้อยละ 38.3 ผลสำรวจสะท้อนให้เห็นว่าบุคลากรในธุรกิจประกันภัยและผู้มีความรู้เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่วนใหญ่เห็นด้วยกับการประกาศดังกล่าว อย่างไรก็ตาม ยังมีผู้ที่มีความเห็นแตกต่างจากประกาศดังกล่าวอยู่ด้วยเช่นกัน โดยเฉพาะอย่างยิ่ง กลุ่มผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งอาจมีความกังวลในเรื่องการใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ[27]

---

[26] สัมภาษณ์ทางโทรศัพท์ สุวรรณโชติ ศิริมหาศาล, ที่ปรึกษาด้านการพัฒนาระบบและวิทยากรเรื่องข้อมูลส่วนบุคคล, สำนักงานพัฒนารัฐบาลดิจิทัล, (17 กรกฎาคม 2565).

[27] ‘ผลสำรวจการตอบแบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564’ (ภาคผนวก ฉ).

Ref. code: 25646301033624ADV

3.4 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 3.0)

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 3.0) เป็นแนวปฏิบัติที่จัดทำขึ้นโดยความร่วมมือของ ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย บริษัทที่ปรึกษาทางกฎหมาย และคณะอาจารย์กฎหมาย เพื่อก่อให้เกิดความตระหนักรู้เรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาครัฐและภาคเอกชนของประเทศไทย ซึ่งมีเนื้อหาทั้งหมด 668 หน้า ครอบคลุมเรื่องต่างๆ ดังนี้

3.4.1 แนวปฏิบัติเกี่ยวกับการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline on Personal Data Classification)

3.4.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (Guideline on Lawful Basis for Processing Personal Data)

3.4.3 แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมและผู้ประมวลผลข้อมูล (Guideline on Duties and Responsibilities of Controllers and Processors)

3.4.4 แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline on Data Protection Impact Assessment)

3.4.5 แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)

3.4.6 แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม (Guideline for Anonymization)

3.4.7 แนวปฏิบัติเกี่ยวกับข้อมูลอ่อนไหว (Guidelines for Sensitive Personal Data or Special Categories of Personal Data)

3.4.8 แนวปฏิบัติสำหรับฝ่ายขายและการตลาด (Guideline for Marketing and Sales)

3.4.9 แนวปฏิบัติเกี่ยวกับฝ่ายวิเคราะห์ข้อมูล (Guideline on Data Analytics)

3.4.10 แนวปฏิบัติเกี่ยวกับฝ่ายทรัพยากรบุคคล (Guideline for Human Resource Management)

3.4.11 แนวปฏิบัติเกี่ยวกับฝ่ายจัดซื้อจัดจ้าง (Guideline for Procurement Department)

3.4.12 แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศ (Guideline for IT Department)

Ref. code: 25646301033624ADV

3.4.13 แนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Guidelines for Data Protection Officer)

เอกสารฉบับนี้ ได้อธิบายแนวปฏิบัติสำหรับการทำงานกับข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว และยังจำแนกแนวปฏิบัติตามกลุ่มงานที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลอีกด้วย ซึ่งผู้เขียนมีความเห็นว่าเอกสารฉบับนี้เป็นแนวปฏิบัติที่ชัดเจนและสามารถนำมาใช้ได้จริง โดยเนื้อหาส่วนใหญ่ของเอกสารเป็นการนำแนวปฏิบัติของ GDPR และแนวปฏิบัติของหน่วยงานกำกับดูแลกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหราชอาณาจักรหรือประเทศอังกฤษมายกตัวอย่างและอภิปราย ซึ่งมีเนื้อหาแนวปฏิบัติสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยสรุป ดังนี้

(1) การประมวลผลข้อมูลที่มีความอ่อนไหวโดยวัตถุประสงค์ที่นอกเหนือจากที่กฎหมายกำหนดไว้นั้น ไม่สามารถทำได้

(2) การได้รับความยินยอมโดยชัดแจ้ง ต้องมีลักษณะให้อิสระในการเลือกแก่เจ้าของข้อมูล มีความเฉพาะเจาะจงทั้งข้อมูลส่วนบุคคลและวัตถุประสงค์ที่ประมวลผล ไม่ขอความยินยอมมาไว้เผื่อใช้ เนื้อหาต้องมีความชัดเจน ครบถ้วน และโปร่งใส โดยควรแยกความยินยอมในการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลจากความยินยอมประเภทอื่น

สำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นต่อการปฏิบัติตามสัญญา เช่น การทำประกันชีวิต หรือประกันสุขภาพนั้น แนวปฏิบัติดังกล่าวให้หลักไว้ว่าผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลไม่สามารถเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอาศัยฐานสัญญาได้ตามกฎหมายคุ้มครองข้อมูลของประเทศไทย ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ก็ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลเท่านั้น และหากไม่ได้รับความยินยอมหรือเจ้าของข้อมูลไม่ให้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นต่อการทำสัญญาต่อผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลอาจปฏิเสธการทำสัญญาเพราะไม่ได้รับข้อมูลที่จำเป็นต่อการทำสัญญาก็ได้

(3) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในฐานเรื่องความจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน ประกันสังคม และการคุ้มครองสังคม อาจเป็นกรณีดังตัวอย่างเช่น การขอข้อมูลสุขภาพของลูกจ้างเพื่อการใช้สิทธิต่างๆ เช่น การลาป่วย การลาทำหมัน การลาคลอด การขอข้อมูลสุขภาพเพื่อประเมินความสามารถในการปฏิบัติงานบางชนิด การขอข้อมูลการรักษาเพื่อให้สิทธิในการเบิกเงินรักษาพยาบาลหรือเบิกเงินประโยชน์ทดแทนจากกรณีประสบอันตราย หรือเจ็บป่วยจากประกันสังคม การใช้ข้อมูลสุขภาพเพื่อใช้สิทธิในการรักษาพยาบาลของผู้สูงอายุ ตามพระราชบัญญัติผู้สูงอายุ พ.ศ. 2546 เป็นต้น

Ref. code: 25646301033624ADV

(4) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวในฐานเพื่อการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของเจ้าของข้อมูล อาจเป็นกรณีตัวอย่างเช่น กรณีเกิดอุบัติเหตุร้ายแรงหรืออาจมีอันตรายต่อชีวิต และเจ้าของข้อมูลไม่มีสติที่จะให้ความยินยอมได้ เป็นต้น

(5) การอาศัยฐานการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ต้องมีวัตถุประสงค์เกี่ยวกับ การเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานเท่านั้น จะต้องเป็นการประมวลผลภายในให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรเท่านั้น

(6) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคลนั้น ต้องเป็นการเปิดเผยในรูปแบบสาธารณะ มิใช่กำหนดให้เห็นในวงจำกัด เช่น เพื่อนในเฟซบุ๊ก (Facebook) หรือกลุ่มจำกัดในไลน์ เป็นต้น

(7) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอาศัยฐานการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย อาจเป็นกรณีดังตัวอย่างเช่น การแจ้งความลงบันทึกประจำวัน การเตรียมคำฟ้อง หรือ ยกเป็นข้อต่อสู้ในคดี เป็นต้น

(8) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอาศัยฐานประโยชน์สาธารณะที่สำคัญนั้น ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่มีการระบุความหมาย กรณีตัวอย่าง หรือแนวทางการตีความไว้ แต่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษได้มีการระบุความหมายของคำดังกล่าวไว้ โดยกำหนดให้รวมถึงกรณีดังต่อไปนี้

- การปฏิบัติงานตามอำนาจหน้าที่ของหน่วยงานรัฐ
- การปฏิบัติหน้าที่ของสภานิติบัญญัติ
- การดำเนินการเพื่อสร้างความเท่าเทียม
- การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์
- การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย
- การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต
- การป้องกันการฉ้อโกง
- การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน
- การให้ความช่วยเหลือบุคคลผู้พิการหรือต้องได้รับความช่วยเหลือทางการแพทย์
- การให้คำปรึกษา การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง
- การช่วยเหลือทางด้านสวัสดิการ
- การประกันภัย

Ref. code: 25646301033624ADV

- การบำนาญ
- พรรคการเมือง
- การเผยแพร่คำพิพากษา
- การป้องกันการใช้สารต้องห้ามในการแข่งกีฬา

ซึ่งอาจนำมาพิจารณาเป็นแนวทางเพื่อการตีความฐานประโยชน์สาธารณะที่สำคัญตามมาตรา 26 (5) (จ) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไปได้

(9) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอาศัยฐานเพื่อการดูแลรักษาสุขภาพ และสังคมซึ่งเป็นการจำเป็นในการปฏิบัติตามกฎหมาย อาจเป็นกรณีดังตัวอย่างเช่น การตรวจสุขภาพของผู้ที่ต่อใบอนุญาตกับสำนักงานการบินพลเรือนแห่งประเทศไทย เป็นต้น

(10) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยอาศัยฐานเพื่อประโยชน์สาธารณะด้านการสาธารณสุข อาจเป็นกรณีดังตัวอย่างเช่น การประมวลผลข้อมูลของสถานพยาบาลเพื่อประโยชน์ด้านสาธารณสุข เป็นต้น

(11) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว อาจทำได้โดยอาศัยฐานเพื่อการวิจัย และสถิติ ซึ่งจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นและกระทำเท่าที่จำเป็น[28]

นอกจากนี้ แนวปฏิบัติดังกล่าวยังอภิปรายเรื่องแนวทางการจัดการกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยต้องประมวลผลข้อมูลตามวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบ การประมวลผลข้อมูลโดยให้น้อยที่สุดและเท่าที่จำเป็นเท่านั้น การรักษาความถูกต้องของข้อมูล เก็บรักษาข้อมูลภายในระยะเวลาที่จำกัด และมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และยังมีหัวข้อแนวปฏิบัติการจัดการข้อมูลสุขภาพภายใต้สถานการณ์ COVID-19 อีกด้วย

เอกสารฉบับนี้ แม้จะถูกจัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติโดยศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย แต่ก็มิได้มีผลทางกฎหมาย หรือมีการรับรองจากหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคลของประเทศไทย รวมถึง ทางศูนย์วิจัยกฎหมายและการพัฒนานั้นมิได้รับรอง หรือรับประกันความครบถ้วนของแนวปฏิบัติดังกล่าว[29] แนวปฏิบัติฉบับนี้จึง

---

[28] ปิยะบุตร บุญอร่ามเรือง และคณะ, ‘แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 3.0)’ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) 305-327 <https://www.law.chula.ac.th/wp-content/uploads /2020/12/TDPG3.0-C5-20201208.pdf> สืบค้นเมื่อวันที่ 2 มิถุนายน 2565.

[29] เพิ่งอ้าง 4.

Ref. code: 25646301033624ADV

มิได้มีสถานะเป็นกฎหมาย หรือแนวปฏิบัติทางกฎหมายที่สามารถใช้ยืนยันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ เพราะอำนาจการกำกับดูแลรวมถึงการตัดสินถูกผิดในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ต้องเป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายเป็นผู้วินิจฉัย ผู้เขียนมีความเห็นว่าเนื้อหาในแนวปฏิบัตินี้เป็นประโยชน์และมีความจำเป็นต่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะเป็นประโยชน์อย่างมากแก่ผู้ประกอบธุรกิจภาคเอกชน นอกจากนี้ แนวปฏิบัติฉบับนี้ มีเนื้อหาที่เกี่ยวข้องกับการพิจารณาความหมายของฐานประโยชน์สาธารณะ อันได้อ้างอิงมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษซึ่งสนับสนุน เรื่องการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อบริษัทประกันภัย ตัวแทนประกันภัย และนายหน้าประกันภัยตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยในข้อ 3.2 และข้อ 3.3 แต่อย่างไรก็ตาม ทางผู้เขียนเห็นว่า การปฏิบัติตามแนวปฏิบัติดังกล่าว ควรกำหนดให้มีกฎหมายลำดับรอง การรับรอง หรือความเห็นชอบจากหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคล คือ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเพิ่งมีคำสั่งแต่งตั้งประธานและกรรมการผู้ทรงคุณวุฒิรวม 10 ท่าน ในวันที่ 18 มกราคม พ.ศ. 2565 ที่ผ่านมา[30]

3.5 แนวปฏิบัติของภาคธุรกิจประกันภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นอกจากประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยแล้ว ทางสมาคมประกันวินาศภัยไทยและสมาคมประกันชีวิตไทยก็ได้จัดทำแนวปฏิบัติให้แก่ภาคธุรกิจด้วย ซึ่งมีเนื้อหาแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

3.5.1 แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ทางสมาคมประกันวินาศภัยไทยภายใต้ความร่วมมือของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้ประกาศแนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีแนวปฏิบัติครอบคลุมการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้แก่ผู้ประกอบธุรกิจประกันวินาศภัย เช่น คำนิยามศัพท์ หลักการพื้นฐาน แนวทางการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตัวอย่างสถานการณ์ในกรณี

---

[30] ประกาศสำนักนายกรัฐมนตรี เรื่อง แต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล.

Ref. code: 25646301033624ADV

การเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และแนวทางอื่นๆ เป็นต้น ซึ่งแนวปฏิบัติฉบับนี้มิได้ประกาศให้สาธารณชนทราบ แต่เป็นการประกาศในกลุ่มสมาชิกสมาคมในลักษณะจดหมายเวียน อย่างไรก็ตาม ผู้เขียนได้ร้องขอแนวปฏิบัติดังกล่าวไปยังสมาคมประกันวินาศภัยไทย และทางสมาคมก็ได้จัดส่งให้แก่ผู้เขียนเพื่อประโยชน์ในการศึกษา ซึ่งเมื่อได้ศึกษาถึงแนวปฏิบัติที่เกี่ยวข้องกับหัวข้อปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวในภาคธุรกิจประกันภัยแล้ว พบว่ามีประเด็นที่น่าสนใจคือ ข้อมูลแนวปฏิบัติเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยอาศัยฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะ (Substantial Public Interest) โดยกำหนดไว้ว่า การประกันภัยที่ต้องมีการสอบถามข้อมูลสุขภาพ ประวัติการรักษาพยาบาล หรือตอบแบบสอบถามประเมินสุขภาพเบื้องต้น บริษัทประกันวินาศภัยไม่มีความจำเป็นต้องขอความยินยอมโดยพิจารณาการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลทั่วไปเป็นการปฏิบัติตามสัญญาประกันภัย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (3) และพิจารณาการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นการปฏิบัติเกี่ยวกับการก่อตั้งสิทธิเรียกร้องตามกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (4) หรือประโยชน์สาธารณะที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (จ) ซึ่งมีส่วนที่สอดคล้องกับประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 กล่าวคือมีการอ้างฐานประโยชน์สาธารณะที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (จ) เช่นเดียวกัน

3.5.2 แนวปฏิบัติของภาคธุรกิจประกันชีวิตตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เช่นเดียวกับสมาคมประกันวินาศภัยไทย ทางสมาคมประกันชีวิตไทยก็มีแนวปฏิบัติของภาคธุรกิจประกันชีวิตด้วยเช่นกัน โดยผู้เขียนได้ส่งจดหมายอิเล็กทรอนิกส์เพื่อขอแนวปฏิบัติดังกล่าวแล้ว แต่ทางสมาคมประกันชีวิตไทยติดต่อกลับทางโทรศัพท์แจ้งว่าไม่สามารถเปิดเผยแนวปฏิบัติดังกล่าวให้แก่บุคคลภายนอกได้ เนื่องจากแนวปฏิบัติยังไม่สมบูรณ์

3.6 ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. ....

เมื่อวันที่ 20 มิถุนายน พ.ศ. 2565 ราชกิจจานุเบกษาได้มีประกาศ ดังต่อไปนี้

Ref. code: 25646301033624ADV

(1) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565

(2) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

(3) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

และเมื่อวันที่ 11 กรกฎาคม พ.ศ. 2565 ราชกิจจานุเบกษาได้มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกหนึ่งฉบับ คือ เรื่อง คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565

ซึ่งประกาศกฎหมายลำดับรองที่มีอยู่ในปัจจุบัน ยังมิได้มีการกล่าวถึงประเด็นปัญหาตามรายงานฉบับนี้ ทั้งเรื่องการอ้างฐานการจำเป็นเพื่อการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ ประเด็นการขอความยินยอม หรือประเด็นการออกแนวปฏิบัติของหน่วยงานกำกับดูแลธุรกิจเฉพาะ

นอกจากนี้ เมื่อวันที่ 19 ถึง 25 พฤษภาคม พ.ศ. 2565 มีการประกาศรับฟังความคิดเห็นร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จำนวน 2 ฉบับ ได้แก่

(1) ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. ....

(2) ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. ....[31]

ซึ่งมีความสำคัญ เกี่ยวข้องกับรายงานฉบับนี้ โดยร่างแนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. .... นั้น มีเนื้อหาโดยสรุป ดังนี้

3.6.1 ภายใต้มาตรา 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีที่มีหน่วยงานเฉพาะ หน่วยงานควบคุมและกำกับดูแล สภาวิชาชีพ สมาคม และกลุ่มอุตสาหกรรม หรือองค์กรที่มีกฎหมายเฉพาะรองรับอำนาจเรื่องการขอความยินยอม และแบบหรือ

---

[31] ‘ขอเชิญแสดงความคิดเห็น (ร่าง) แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จำนวน 2 ฉบับ’ (เพจเฟซบุ๊ค PDPC Thailand, วันที่ 19 พฤษภาคม 2565) <https://www.facebook.com/pdpc.th>สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

รายละเอียดในการขอความยินยอมโดยกฎหมายดังกล่าวไม่ขัดหรือแย้งกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงานภายใต้การควบคุมและกำกับดูแลจากหน่วยงานดังกล่าวสามารถใช้แบบฟอร์มขอความยินยอมของหน่วยงานดังกล่าวได้อาทิเช่น การออกหลักเกณฑ์เรื่องการขอความยินยอมของธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

3.6.2 การขอความยินยอมต้องชัดแจ้งซึ่งวัตถุประสงค์ รายละเอียดในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล โดยต้องกระทำโดยชัดแจ้ง (explicit) โดยอาจทำเป็นหนังสือลายลักษณ์อักษรหรือผ่านระบบอิเล็กทรอนิกส์ก็ได้

3.6.3 การถอนความยินยอม เจ้าของข้อมูลส่วนบุคคลต้องสามารถถอนความยินยอมได้โดยง่ายโดยผู้ควบคุมข้อมูลส่วนบุคคล ต้องแสดงรายละเอียด วิธีการ เงื่อนไข แบบฟอร์ม ในการถอนความยินยอมในบริเวณที่เห็นได้ชัดเจนในแบบฟอร์มกระดาษหรือสื่ออิเล็กทรอนิกส์ที่ขอความยินยอม[32]

นอกจากนี้ยังมีการกำหนดมาตรฐานในการขอความยินยอมจากผู้เยาว์ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถด้วย

อย่างไรก็ตาม ร่างกฎหมายดังกล่าวถือเป็นการสนับสนุนประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ที่กำหนดเกี่ยวกับการขอความยินยอมไว้ ให้เป็นแนวปฏิบัติสำหรับภาคธุรกิจประกันภัยได้อย่างถูกต้อง และสร้างความมั่นใจให้ผู้ประกอบธุรกิจภายใต้การกำกับดูแลของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยสำหรับประเด็นการขอความ

---

[32] ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง แนวทางและวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พ.ศ. .... <https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/%E0%B8%A3%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%AF%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%82%E0%B8%AD%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A2%E0%B8%B4%E0%B8%99%E0%B8%A2%E0%B8%AD%E0%B8%A1.pdf> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

ยินยอมตามรูปแบบที่คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้กำหนดแนวปฏิบัติหรือมีประกาศกำหนดรูปแบบในแบบฟอร์มใบคำขอประกันภัยต่อไปในภายหลัง

3.7 ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. ....

ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. .... นั้น มีเนื้อหาโดยสรุป ดังนี้

3.7.1 ภายใต้มาตรา 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีที่มีหน่วยงานเฉพาะ หน่วยงานควบคุมและกำกับดูแล สภาวิชาชีพ สมาคม และกลุ่มอุตสาหกรรมหรือองค์กรที่มีกฎหมายเฉพาะรองรับอำนาจเรื่องการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลโดยกฎหมายดังกล่าวไม่ขัดหรือแย้งกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงานภายใต้การควบคุมและกำกับดูแลจากหน่วยงานดังกล่าวสามารถใช้แบบฟอร์มการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้องมูลส่วนบุคคลของหน่วยงานดังกล่าวได้อาทิเช่น การออกหลักเกณฑ์ เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

3.7.2 ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล ภายใต้หลักเกณฑ์เรื่องความเป็นธรรม ซึ่งต้องเป็นการเก็บ ใช้ และเปิดเผยโดยจำกัดวัตถุประสงค์ ต้องขอความยินยอมในวัตถุประสงค์ที่กฎหมายกำหนด การอ้างผลประโยชน์โดยชอบด้วยกฎหมายต้องใช้ความระมัดระวังอย่างยิ่งเพื่อปกป้องผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

3.7.3 การกำหนดรายละเอียดที่ต้องแจ้งเมื่อมีการเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง

3.7.4 การกำหนดรายละเอียดที่ต้องแจ้งเมื่อมีการเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นตามมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อยกเว้นที่ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลในกรณีดังกล่าว

Ref. code: 25646301033624ADV

3.7.5 กำหนดวิธีการและช่องทางการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล[33]

นอกจากนี้ประกาศทั้งสองฉบับที่กล่าวมานั้น มีข้อกำหนดตอนท้ายว่า หน่วยงานควบคุมและกำกับดูแล สภาวิชาชีพ สมาคม และกลุ่มอุตสาหกรรมอาจร่วมกันรูปแบบวิธีการและมาตรฐานขั้นต่ำของการแจ้งวัตถุประสงค์และรายละเอียดที่เหมาะสมให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาและให้คำแนะนำเพิ่มเติมรวมถึงแก้ไขเพื่อให้เป็นแนวนโยบายคุ้มครองข้อมูลส่วนบุคคลมาตรฐานได้ด้วย อันเป็นการเกิดช่องทางให้แก่หน่วยงานกำกับดูแลที่เกี่ยวข้องได้ดำเนินการส่งแนวปฏิบัติในธุรกิจต่างๆ ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้พิจารณาเพิ่มเติม

---

[33] ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. .... <https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/%E0%B8%A3%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%AF%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%81%E0%B8%88%E0%B9%89%E0%B8%87%E0%B8%A7%E0%B8%B1%E0%B8%95%E0%B8%96%E0%B8%B8%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%AA%E0%B8%87%E0%B8%84%E0%B9%8C.pdf> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

บทที่ 4
วิเคราะห์และอภิปรายกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างประเทศ

4.1 GENERAL DATA PROTECTION REGULATION (GDPR) and Recital

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR นั้น เป็นข้อบังคับของสหภาพยุโรปเพื่อกำหนดกฎเกณฑ์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของบุคคลธรรมดาในสหภาพยุโรป ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้น ได้กระทำในหรือนอกสหภาพยุโรป[1] ซึ่งการมีข้อกำหนดเช่นนี้ ถือเป็นข้อบังคับแรกของสหภาพยุโรปที่มีผลบังคับใช้ไปถึงประเทศนอกสหภาพยุโรปด้วย[2] และด้วยเหตุดังกล่าวนั้น ทำให้ GDPR กลายเป็นกฎหมายแม่แบบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในนานาประเทศ ซึ่งรวมถึงประเทศไทย

4.1.1 GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR มีเนื้อหาทั้งหมด 11 บท มีข้อกำหนดทั้งหมด 99 ข้อ โดยกำหนดเนื้อหาความหมาย หรือประเภทข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือข้อมูลชนิดพิเศษ (special categories of personal data / sensitive data) ไว้ในข้อ 9[3] ซึ่งมีข้อกำหนดว่า

“การประมวลข้อมูลส่วนบุคคลชนิดพิเศษ คือ

1. การประมวลผลข้อมูลส่วนบุคคลที่เปิดเผยต้นกำเนิดทางเชื้อชาติและชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกสหภาพวิชาชีพ และการประมวลผลข้อมูลพันธุกรรม ข้อมูลชีวมาตราเพื่อวัตถุประสงค์ในการระบุอัตลักษณ์บุคคลธรรมดาอย่างเฉพาะเจาะจงข้อมูลเกี่ยวข้องกับสุขภาพหรือข้อมูลเกี่ยวกับชีวิตทางเพศหรือวิถีทางเพศของบุคคลธรรมดาจะกระทำมิได้

---

[1] GENERAL DATA PROTECTION REGULATION (GDPR) Article 1 and 3.

[2] Gaham J H Smith Bird & Bird, *Internet Law and Regulation* (4th Edition, Sweet & Maxwell 2007) 687.

[3] Peter Carey, *Data Protection A Practical Guide to UK and EU law* (2nd Edition, Oxford University Press 2004) 21.

Ref. code: 25646301033624ADV

2. อนุมาตรา 1 ไม่มีผลบังคับใช้ในกรณีดังต่อไปนี้

(ก) เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างชัดเจนถึงการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์โดยเฉพาะอย่างใดอย่างหนึ่งหรือมากกว่า เว้นแต่ว่าเมื่อกฎหมายของสหภาพหรือรัฐสมาชิกได้กำหนห้ามตามที่อ้างไว้ในอนุมาตรา 1 จะไม่สามารถถูกยกเว้นได้โดยผู้ถูกประมวลผลข้อมูล

(ข) การประมวลผลจำเป็นต่อวัตถุประสงค์ในการปฏิบัติตามพันธกรณีและใช้สิทธิบางประการของผู้ควบคุมหรือผู้ถูกประมวลผลข้อมูลในด้านที่เกี่ยวกับกฎหมายการจ้างงาน กฎหมายความมั่นคงทางสังคมและการให้การคุ้มครองทางสังคมตราบเท่าที่ได้อำนาจโดยกฎหมายของสหภาพหรือรัฐสมาชิก หรือข้อตกลงร่วมดังที่ระบุไว้ในกฎหมายของรัฐสมาชิกที่บัญญัติไว้เพื่อคุ้มครองสิทธิขั้นพื้นฐาน และผลประโยชน์ของผู้ถูกประมวลผลข้อมูลตามสมควร

(ค) การประมวลผลที่จำเป็นต่อการคุ้มครองผลประโยชน์อันเกี่ยวเนื่องถึงชีวิตของผู้ถูกประมวลผลข้อมูลหรือบุคคลธรรมดาอื่น เมื่อผู้ถูกประมวลผลไม่สามารถให้ความยินยอมเองได้ด้วยเหตุผลทางกายภาพหรือทางกฎหมาย

(ง) การประมวลผลถูกดำเนินการโดยเป็นส่วนหนึ่งของกิจกรรมอันชอบธรรมของมูลนิธิสมาคมหรือองค์กรไม่แสวงหาผลกำไรอื่น ๆ ที่มีจุดมุ่งหมายในด้านการเมือง ปรัชญา ศาสนา การรวมกลุ่มทางวิชาชีพ โดยมีการคุ้มครองข้อมูลตามสมควรและอยู่บนเงื่อนไขของการประมวลผลที่สัมพันธ์กับสมาชิกหรืออดีตสมาชิกขององค์กรหรือบุคคลที่ติดต่อกับองค์กรอย่างสม่ำเสมอโดยเชื่อมโยงกับวัตถุประสงค์ขององค์กรเท่านั้น และข้อมูลส่วนบุคคลจะไม่ถูกเปิดเผยสู่ภายนอกองค์กรดังกล่าวโดยไม่มีความยินยอมของผู้ถูกประมวลผลข้อมูล

(จ) การประมวลผลสัมพันธ์กับข้อมูลส่วนบุคคลที่ผู้ถูกประมวลผลข้อมูลทำให้เป็นข้อมูลสาธารณะโดยเป็นที่รับรู้ทั่วไป

(ฉ) การประมวลผลจำเป็นต่อการเริ่ม ใช้หรือคุ้มครองการอ้างสิทธิตามกฎหมายหรือเมื่อใดก็ตามที่ศาลปฏิบัติหน้าที่ในกระบวนการยุติธรรม

(ช) การประมวลผลจำเป็นด้วยเหตุผลของประโยชน์สาธารณะที่สำคัญชัดเจนตามหลักกฎหมายของสหภาพหรือรัฐสมาชิกอันจะต้องได้ส่วนกับเป้าหมายที่ต้องการ เคารพสาระสำคัญของสิทธิในการคุ้มครองข้อมูลส่วนบุคคลและกำหนดให้มีมาตรการที่เหมาะสมและเฉพาะเจาะจงเพื่อคุ้มครองสิทธิขั้นพื้นฐานและผลประโยชน์ของผู้ถูกประมวลผล

(ซ) การประมวลผลจำเป็นต่อวัตถุประสงค์ด้านเวชศาสตร์ป้องกันหรือเวชศาสตร์โรคจากการทำงาน เพื่อประเมินสถานการณ์ของความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคการจัดหาบริการทางสาธารณสุขและสังคม หรือการรักษาหรือจัดการระบบและ

Ref. code: 25646301033624ADV

บริการสาธารณสุข และสังคมตามหลักของกฎหมายของสหภาพหรือรัฐสมาชิกหรือตามที่ระบุไว้ในสัญญาระหว่างผู้ประกอบวิชาชีพสาธารณสุขและอยู่ภายใต้เงื่อนไขและการคุ้มครองตามที่ถูกอ้างถึงในอนุมาตรา 3 ของมาตรานี้

(ฌ) การประมวลผลจำเป็นด้วยเหตุผลของประโยชน์สาธารณะในด้านสาธารณสุข เช่น การป้องกันภัยคุกคามร้ายแรงต่อสุขภาพที่สามารถแพร่กระจายข้ามพรมแดนหรือเพื่อรับประกันภัย มาตรฐานความปลอดภัยของบริการสาธารณสุขและผลิตภัณฑ์ทางการแพทย์หรือบริการทางการแพทย์ในระดับสูงตามหลักกฎหมายของสหภาพหรือรัฐสมาชิกที่กำหนดให้มีมาตรการที่เหมาะสมและเฉพาะเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพของผู้ถูกประมวลผลข้อมูลโดยเฉพาะอย่างยิ่งกับความลับทางวิชาชีพ

(ญ) การประมวลผลสำหรับวัตถุประสงค์ในการทำจดหมายเหตุอันเป็นไปเพื่อประโยชน์สาธารณะ วัตถุประสงค์ในการวิจัยวิทยาศาสตร์หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติโดยเป็นไปตาม (1) ในข้อ 89 บนฐานของกฎหมายของสหภาพหรือรัฐสมาชิก ซึ่งจะต้องได้สัดส่วนกับเป้าหมายที่ต้องการเคารพสารสำคัญของสิทธิในการเข้าถึงการคุ้มครองข้อมูลและกำหนดให้มาตรการที่เหมาะสมและเฉพาะเจาะจงสามารถเกิดขึ้นได้เพื่อคุ้มครองสิทธิขั้นพื้นฐานและผลประโยชน์ของผู้ถูกประมวลผลข้อมูล

3. ข้อมูลส่วนบุคคลที่ถูกอ้างถึงในอนุมาตรา 1 ของมาตรานี้อาจถูกประมวลผลเพื่อวัตถุประสงค์ในข้อ (ซ) ของอนุมาตรา 2 เมื่อข้อมูลส่วนบุคคลเหล่านั้นถูกประมวลผลโดยหรือภายใต้ความรับผิดชอบของเจ้าหน้าที่วิชาชีพที่ถูกกำหนดโดยพันธกรณีเกี่ยวกับความลับทางวิชาชีพภายใต้กฎหมายของสหภาพหรือรัฐสมาชิกหรือกฎที่ตั้งโดยหน่วยงานที่มีอำนาจในระดับชาติ

4. รัฐสมาชิกยังอาจใช้หรือนำเงื่อนไขอื่น ๆ อันรวมถึงการกำหนดขอบเขตมาใช้ในประเด็นที่เกี่ยวข้องกับการประมวลผลข้อมูลพันธุกรรม ข้อมูลชีวมาตราหรือข้อมูลที่เกี่ยวข้องกับสุขภาพ”[4]

4.1.2 ความแตกต่างของ GDPR ข้อ 9 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น ได้กำหนดความหมายของข้อมูลส่วนบุคคลชนิดพิเศษ

[4] นคร เสรีรักษ์ และคณะ, *General Data Protection Regulation ฉบับภาษาไทย* (P.Press 2563) 114-117.

Ref. code: 25646301033624ADV

หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวแตกต่างจากกฎหมายแม่แบบที่ได้กล่าวมาเพียงสองประการ ได้แก่

4.1.2.1 ใน GDPR ข้อ 9 ไม่มีการระบุว่าข้อมูลส่วนบุคคลชนิดพิเศษนี้รวมถึงเรื่อง ประวัติอาชญากรรม และข้อมูลความพิการ โดย GDPR ระบุข้อมูลอาชญากรรมไว้แยกต่างหากในข้อ 10 และกำหนดให้ประวัติอาชญากรรมถูกควบคุมเป็นกรณีพิเศษโดยเจ้าหน้าที่ที่มีอำนาจตามกฎหมายเท่านั้น ส่วนข้อมูลความพิการนั้น หากพิจารณาตามถ้อยคำใน GDPR คำว่า “data concerning health” แล้ว ก็อาจตีความหมายรวมถึงข้อมูลความพิการได้ แม้มิได้มีการระบุไว้อย่างชัดเจนก็ตาม

4.1.2.2 มาตรา 26 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการกำหนดฐานทางกฎหมายสำหรับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ส่วน GDPR ข้อ 9 2. (c) กำหนดไว้เฉพาะกรณีป้องกันอันตรายต่อชีวิต ร่างกาย หรือสุขภาพเท่านั้น มิได้มีการระบุรวมไปถึงการระงับอันตรายเพื่อการดังกล่าว

4.1.3 GDPR recitals and articles

สหภาพยุโรปมีเอกสาร GDPR recitals and articles ซึ่งประกาศออกมาเพื่อเป็นแนวทางการปฏิบัติตาม GDPR ให้แก่รัฐสมาชิก โดยมีเนื้อหาเป็นการอธิบายรายละเอียด และตีความ GDPR ในประเด็นที่ไม่อาจกำหนดอย่างเฉพาะเจาะจงในข้อบังคับได้ ซึ่งผู้เขียนได้นำข้อสรุปในการตีความข้อกำหนดที่เกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่น่าสนใจและเกี่ยวข้องกับข้อมูลสุขภาพมาอภิปราย ดังนี้

4.1.3.1 การประมวลผลข้อมูลส่วนบุคคลควรได้รับการพิจารณาว่าชอบด้วยกฎหมายในกรณีที่จำเป็นต้องปกป้องชีวิต ร่างกายของเจ้าของข้อมูล หรือบุคคลอื่นด้วย ซึ่งการประมวลผลบางประเภทอาจตอบวัตถุประสงค์ทั้งในเรื่องประโยชน์สาธารณะและเพื่อประโยชน์ในการปกป้องชีวิต ร่างกายของเจ้าของข้อมูลหรือบุคคลอื่น เช่น การเฝ้าระวังโรคระบาดและการแพร่กระจาย หรือในสถานการณ์ฉุกเฉินต่างๆ โดยเฉพาะอย่างยิ่งในสถานการณ์ที่เป็นภัยธรรมชาติ และภัยที่มนุษย์สร้างขึ้น[5]

[5] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (46).

Ref. code: 25646301033624ADV

4.1.3.2 การประมวลผลภาพถ่ายไม่ถูกกำหนดให้เป็นการประมวลผลข้อมูลอ่อนไหว เพราะการประมวลผลที่เป็นข้อมูลอ่อนไหวในกรณีเช่นนี้นั้น หมายถึงการประมวลผลข้อมูลทางชีวภาพซึ่งใช้เทคนิคพิเศษในการระบุตัวตน[6]

4.1.3.3 รัฐสมาชิกต้องกำหนดกฎหมาย และนโยบายภายในเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษให้ไม่แตกต่างไปจากข้อกำหนดใน GDPR เพื่อคุ้มครองข้อมูลส่วนบุคคล และสิทธิขั้นพื้นฐานอย่างเท่าเทียมในรัฐสมาชิก การกำหนดกฎหมายหรือข้อกำหนดของรัฐสมาชิกอาจกระทำเพื่อวัตถุประสงค์ด้านสุขภาพ ซึ่งรวมถึง การบริการสาธารณสุข และการบริการด้านสุขภาพ โดยเฉพาะอย่างยิ่งเพื่อให้มั่นใจได้ว่าขั้นตอนการบริการและการจ่ายค่าสินไหมทดแทนของระบบประกันสุขภาพเป็นไปอย่างมีประสิทธิภาพ[7]

4.1.3.4 การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ ต้องประมวลผลโดยมาตรฐานการคุ้มครองข้อมูลที่สูงกว่ามาตรฐานทั่วไป ภายใต้วัตถุประสงค์ที่จำเป็นเพื่อประโยชน์ของบุคคล และสังคมในการจัดการด้านสุขภาพหรือประกันสังคม รวมถึงการบริหารจัดการข้อมูลของหน่วยงานสาธารณสุขแห่งชาติ[8]

4.1.3.5 การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวอาจมีความจำเป็นด้วยเหตุผลที่เป็นประโยชน์สาธารณะในด้านสาธารณสุขโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลก็ได้ (คำว่า “สาธารณสุข” หมายความว่า องค์ประกอบทั้งหมดที่เกี่ยวข้องกับสุขภาพ ได้แก่ สถานภาพทางสุขภาพซึ่งหมายความรวมถึงการเจ็บป่วยและความทุพพลภาพ ปัจจัยต่างๆ ที่มีผลกระทบต่อสถานภาพทางสุขภาพ ความต้องการสำหรับการดูแลสุขภาพ ทรัพยากรสำหรับการดูแลสุขภาพ การจัดหา และการเข้าถึงการดูแลสุขภาพ ตลอดจนรายจ่ายและการเงินด้านการดูแลสุขภาพ และสาเหตุของการตาย[9]) การประมวลผลข้อมูลที่เกี่ยวข้องกับสุขภาพดังกล่าวด้วยเหตุผลที่เป็น

---

[6] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (51).

[7] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (52).

[8] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (53).

[9] Official Journal of the European Union, REGULATION (EC) No 1338/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (16 December 2008) Article 3.

Ref. code: 25646301033624ADV

สาธารณประโยชน์นั้น ต้องไม่รวมถึงการประมวลผลเพื่อวัตถุประสงค์อื่นโดยบุคคลที่สาม เช่น นายจ้าง บริษัทประกันภัย หรือธนาคาร เป็นต้น[10]

4.1.3.6 การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว อาจได้รับอนุญาตด้วยเหตุผลที่เป็นประโยชน์สาธารณะ ซึ่งต้องกำหนดให้มีการป้องกันที่เหมาะสม[11]

หากพิจารณาตามเอกสาร GDPR recitals and articles ของสหภาพยุโรปแล้ว พบว่ามีข้อกำหนดที่เกี่ยวข้องกับประกันภัยหลักๆ อยู่ 2 ประการ คือ

ประการที่ 1 คือ รัฐสมาชิกอาจกำหนดกฎหมายหรือข้อกำหนดในการจัดการข้อมูลสุขภาพโดยคำนึงถึงประสิทธิภาพในการบริการและการจ่ายค่าสินไหมทดแทนของระบบประกันสุขภาพในรัฐของตนได้

ประการที่ 2 คือการดำเนินการประมวลผลโดยบริษัทประกันภัยนั้น ไม่อาจอ้างได้ว่ากระทำเพื่อวัตถุประสงค์ในลักษณะของสาธารณประโยชน์ได้ การประมวลผลเช่นว่านั้น จึงต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

ดังนั้น จึงอาจกล่าวโดยสรุปได้ว่ารัฐสมาชิกในสหภาพยุโรปอาจกำหนดการจัดการข้อมูลสุขภาพให้แตกต่างจากการจัดการข้อมูลที่มีความอ่อนไหวตาม GDPR ข้อ 9 ได้ โดยจำกัดวัตถุประสงค์เพียงเพื่อการบริการ และจ่ายค่าสินไหมทดแทนสำหรับประกันสุขภาพ แต่ไม่อาจอ้างได้ว่าการประมวลผลเช่นว่านั้นเป็นการกระทำเพื่อสาธารณประโยชน์ หรือสาธารณสุขตามข้อกำหนดของสหภาพยุโรป

4.1.4 ตัวอย่างแนวทางจัดการข้อมูลสุขภาพในสหภาพยุโรป

ประเทศต่างๆ ในสหภาพยุโรปได้กำหนดกฎหมายภายในสำหรับเรื่องการใช้ข้อมูลสุขภาพให้เหมาะสมกับวิธีการบริหารงานด้านการสาธารณสุขภายในประเทศ ทั้งในแง่ของการใช้ข้อมูลสุขภาพของภาครัฐและภาคเอกชน ซึ่งผู้เขียนขอยกตัวอย่างมา ดังนี้

---

[10] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (54).

[11] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (56).

Ref. code: 25646301033624ADV

4.1.4.1 ประเทศสาธารณรัฐฝรั่งเศส มีกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลด้านสุขภาพที่สำคัญหลายฉบับ เช่น

- Act no.78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (La loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

- The Shared Healthcare Information Systems Agency (L'agence des systèmes d'information partagés de santé)

- Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties (Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

- Law no. 2002-303 of 4 March 2002 relative to the rights of the sick and the quality of the health system (Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé)

เป็นต้น โดยจากกฎหมายดังกล่าวนั้น มีข้อกำหนดที่บัญญัติภายใต้หลักการอยู่ 3 ประการคือ

(1) หลักการเก็บรวบรวมและใช้ข้อมูลสุขภาพ ซึ่งกำหนดให้ภาครัฐหรือภาคเอกชนที่จะมีการเก็บข้อมูลสุขภาพภายในสาธารณรัฐฝรั่งเศสต้องได้รับอนุญาตจากหน่วยงานคุ้มครองระบบข้อมูลด้านสุขภาพที่ใช้ร่วมกันก่อน

(2) หลักการปกปิดข้อมูลด้านสุขภาพ กำหนดให้ผู้ประกอบวิชาชีพทางด้านสาธารณสุขต้องปกปิดข้อมูลด้านสุขภาพเป็นความลับ

(3) หลักการเข้าถึงและขอแก้ไขข้อมูลสุขภาพที่เกี่ยวกับตน โดยกฎหมายของสาธารณรัฐฝรั่งเศสกำหนดให้เจ้าของข้อมูลสามารถขอเข้าถึงข้อมูลสุขภาพของตนได้

อย่างไรก็ตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศสนั้น ได้กำหนดข้อยกเว้นในการเก็บข้อมูลสุขภาพไว้เช่นกัน เช่น กรณีได้รับความยินยอมจากเจ้าของข้อมูล กรณีแลกเปลี่ยนข้อมูลระหว่างผู้ประกอบวิชาชีพด้านสาธารณสุขเพื่อประโยชน์ในการรักษาสุขภาพ

Ref. code: 25646301033624ADV

ของเจ้าของข้อมูล การปกป้องชีวิตเจ้าของข้อมูล การวินิจฉัยทางการแพทย์ การจัดการบริการสุขภาพ การบำบัด หรือกรณีได้รับการยกเว้นตามกฎหมายอย่างชัดเจน[12] เป็นต้น

ข้อสังเกตสำคัญสำหรับสาธารณรัฐฝรั่งเศสนั้น คือนอกจากข้อกำหนดทั่วไปที่เป็นไปตามหลักการของ GDPR แล้ว กรณีที่ภาคเอกชนจะมีการเก็บ ใช้ข้อมูลสุขภาพได้นั้น อาจต้องขออนุญาตหน่วยงานกำกับดูแลการใช้ข้อมูลก่อน จึงจะสามารถเก็บ และใช้ข้อมูลดังกล่าวได้ ซึ่งเป็นข้อกำหนดที่เข้มงวดยิ่งไปกว่า GDPR

4.1.4.2 ประเทศสหพันธ์สาธารณรัฐเยอรมนี มีกฎหมาย Bundesdatenshutzgesetz (BDSG) บังคับใช้ในการประมวลผลข้อมูลในสหพันธ์สาธารณรัฐเยอรมนี นอกจากนี้ ยังมีกฎหมายที่ใช้ระดับรัฐให้ใช้บังคับเฉพาะในแต่ละรัฐอีกด้วย โดยผู้เขียนขอยกมาเพียงกฎหมาย BDSG ที่มีเนื้อหาหลักเป็นการกำหนดหลักการเก็บ และใช้ข้อมูลสุขภาพซึ่งกำหนดให้หน่วยงานของรัฐในระดับสหพันธรัฐ หน่วยงานเอกชน และรัฐวิสาหกิจเก็บข้อมูลสุขภาพได้ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลหรือกรณีที่กฎหมายกำหนดเท่านั้น นอกจากนี้ยังมีการกำหนดให้หน่วยงานเอกชนที่มีข้อมูลด้านสุขภาพต้องปกปิดข้อมูลเป็นความลับโดยมีสัญญารักษาความลับเป็นลายลักษณ์อักษรกับพนักงานภายใต้สังกัดของตน และกฎหมายยังกำหนดให้เจ้าของข้อมูลสามารถเข้าถึงและแก้ไขข้อมูลสุขภาพของตน หากพบว่าข้อมูลนั้นไม่ถูกต้องอีกด้วย

ทั้งนี้ BDSG ยังได้กำหนดข้อยกเว้นสำหรับการเก็บและใช้ข้อมูลสุขภาพและการปกปิดข้อมูลสุขภาพให้เป็นความลับสำหรับหน่วยงานเอกชนและรัฐวิสาหกิจไว้ ดังนี้

- กรณีได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- กรณีจำเป็นเพื่อปกป้องชีวิตของเจ้าของข้อมูลหรือบุคคลอื่นที่ไม่อยู่ในสถานการณ์ที่สามารถให้ความยินยอมได้
- กรณีที่เจ้าของข้อมูลเปิดเผยต่อสาธารณะอย่างชัดเจน
- กรณีจำเป็นเพื่อการใช้สิทธิเรียกร้องตามกฎหมาย
- กรณีจำเป็นเพื่อประโยชน์สาธารณะ[13]

ข้อสังเกตสำคัญ ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสหพันธ์สาธารณรัฐเยอรมนีคือเรื่องของข้อกำหนดที่หน่วยงานเอกชนต้องมีการทำสัญญารักษา

---

[12] หทัยชนก หร่ายวงศ์, ‘ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2559) น. 93-100.

[13] เพิ่งอ้าง 100-105.

Ref. code: 25646301033624ADV

ความลับกับพนักงานของตนเพื่อรักษาความลับเกี่ยวกับการเก็บใช้ข้อมูลสุขภาพด้วย ซึ่งเป็นหนึ่งข้อที่เข้มงวดกว่า GDPR

ตัวอย่างของทั้งสองประเทศในสหภาพยุโรปที่กล่าวมานั้น ต่างก็มีระบบการดูแลทางด้านข้อมูลสุขภาพที่แยกย่อยและแตกต่างกันไปตามแต่ละระบบบริหารจัดการด้านสาธารณสุข ระบบประกันสุขภาพ และประโยชน์สาธารณะของประเทศ ในบางกรณีอาจมีข้อกำหนดที่เข้มงวดยิ่งไปกว่า GDPR ซึ่งภาคเอกชนที่ประกอบธุรกิจในประเทศดังกล่าว มีความจำเป็นต้องดำเนินการตามข้อบังคับของสหภาพยุโรป หรือ GDPR และกฎหมายท้องถิ่นของแต่ละประเทศหรือรัฐที่ปฏิบัติงานอยู่ด้วย

4.2 Data Protection Act 2018

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นรูปธรรมฉบับแรกนั้น เกิดขึ้นที่สหราชอาณาจักรหรือประเทศอังกฤษ ซึ่งกฎหมายดังกล่าวมีชื่อว่า Data Protection Act 1984 โดยแรกเริ่มของกฎหมายฉบับนี้ กำหนดให้ผู้ที่ดำเนินการประมวลผลข้อมูลส่วนบุคคลต้องทำการจดทะเบียนกับหน่วยงานชื่อ Data Protection Registar และถ้าหากไม่ปฏิบัติตามจะมีโทษทางอาญาอีกด้วย นอกจากนี้ เจ้าของข้อมูลส่วนบุคคลยังสามารถร้องขอเพื่อเข้าถึงข้อมูลของตน และหากเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการใช้ข้อมูลอย่างไม่ถูกต้อง การสูญหาย หรือการเปิดเผยโดยไม่มีสิทธิกระทำได้ ก็สามารถนำเรื่องการประมวลผลข้อมูลที่ไม่ถูกต้องตามกฎหมายนี้ไปฟ้องต่อศาล หรือดำเนินคดีเพื่อเรียกร้องค่าเสียหายได้[14]

ในอดีตประเทศอังกฤษเคยเป็นสมาชิกในสหภาพยุโรปและบังคับใช้กฎหมายภายใต้การกำกับของสหภาพยุโรป ซึ่งรวมถึง GDPR ด้วย แต่เมื่อวันที่ 1 มกราคม 2021 ประเทศอังกฤษได้บรรลุข้อตกลงเบร็กซิท (Brexit) เพื่อออกจากการเป็นรัฐสมาชิกของสหภาพยุโรปแล้ว[15] จึงไม่ถือว่าประเทศอังกฤษเป็นประเทศในสหภาพยุโรปอีกต่อไป อย่างไรก็ตาม กฎหมายส่วนใหญ่ของสหภาพยุโรปยังคงถูกบังคับใช้ในประเทศอังกฤษ รวมถึง GDPR โดยถูกแก้ไขเป็น United Kingdom General Data Protection Regulation หรือ UK GDPR โดยมีเนื้อหาเหมือน GDPR ฉบับของ

---

[14] Peter Carey (n 3) 3-4.

[15] 'Brexit: What you need to know about the UK leaving the EU' BBC News (30 December 2020) < https://www.bbc.com/news/uk-politics-32810887> accessed 23 January 2022.

Ref. code: 25646301033624ADV

สหภาพยุโรป แต่มีข้อแตกต่างในเรื่องการโอนข้อมูลจากประเทศในสหภาพยุโรปมาที่ประเทศอังกฤษนั้น มิใช่การโอนข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว แต่ต้องปฏิบัติต่อประเทศอังกฤษเหมือนอย่างประเทศอื่นที่ไม่มีสถานภาพสมาชิกในสหภาพยุโรป ซึ่งในการพิจารณานำกฎหมายมาบังคับใช้ต้องพิจารณาถึง UK GDPR ควบคู่กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะของประเทศอังกฤษด้วย[16] ในปัจจุบันประเทศอังกฤษมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ชื่อ Data Protection Act 2018 (แก้ไขเพิ่มเติมเมื่อ 31 ธันวาคม ค.ศ. 2020) และมีหน่วยงานกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ ชื่อ Information Commissioner's Office (ICO.)

Data Protection Act 2018 มีบทบัญญัติเรื่องการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวใน มาตรา 10 และมาตรา 11 ซึ่งมีเนื้อหาเป็นการอ้างอิงถึงการให้ความหมาย และฐานทางกฎหมายในการประมวลผลข้อมูลที่มีความอ่อนไหวตาม GDPR ข้อ 9 ประกอบกับการปฏิบัติตามกฎหมายภายในของประเทศอังกฤษ[17] นอกจากนี้ สำหรับข้อมูลอาชญากรรมซึ่งเป็นข้อมูลอ่อนไหวอีกชนิดหนึ่งนั้น Data Protection Act 2018 ก็ได้อ้างอิงถึงฐานการประมวลผลตามกฎหมาย GDPR ข้อ 10[18] ซึ่งโดยหลักทั่วไปแล้ว ข้อกำหนดในการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวของ Data Protection Act 2018 จึงมิได้มีความแตกต่างไปจาก GDPR แต่อย่างใด

อย่างไรก็ตาม Data Protection Act 2018 มีบทบัญญัติที่ขยายความ หรือตีความเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวไว้ใน เอกสารแนบท้าย 1 (Schedule 1) ซึ่งมีการอธิบายและตีความเรื่องต่างๆ ที่เกี่ยวข้อง ดังนี้

- เรื่องของเงื่อนไขการประมวลผลที่เกี่ยวข้องกับการจ้างงาน สุขภาพและการวิจัย
- เงื่อนไขสำหรับการประมวลผลข้อมูลในฐานประโยชน์สาธารณะที่สำคัญ
- เงื่อนไขเพิ่มเติมที่เกี่ยวข้องกับการตัดสินลงโทษทางอาญา
- นโยบายคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและการป้องกันเพิ่มเติม

โดยในหัวข้อการประมวลผลข้อมูลในฐานประโยชน์สาธารณะที่สำคัญนั้น มีข้อความที่ครอบคลุมเรื่องการประมวลผลข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์เพื่อการประกันภัยมีเนื้อหา ดังนี้

---

[16] ชนิดา เกิดกรณ์, 'ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลต่อฐานข้อมูลการประกันภัยในธุรกิจประกันวินาศภัย' (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2563) 34.

[17] Data Protection Act 2018 section 10.

[18] Data Protection Act 2018 section 11.

Ref. code: 25646301033624ADV

4.2.1 หากการประมวลผลข้อมูลเชื้อชาติหรือชาติพันธุ์ ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกสหภาพแรงงาน ข้อมูลทางพันธุกรรมหรือข้อมูลเกี่ยวกับสุขภาพนั้น เป็นไปเพื่อการจำเป็นสำหรับการประกันภัย โดยมีมาตรการเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ในวัตถุประสงค์อื่นเกี่ยวกับตัวเจ้าของข้อมูล หรือก่อสิทธิหรือภาระผูกพันอื่นที่เจ้าของข้อมูลไม่อาจคาดหมายได้ การประมวลผลดังกล่าวสามารถกระทำได้โดยถือเป็นประโยชน์สาธารณะ

4.2.2 มีการกำหนดความหมายคำว่าเพื่อวัตถุประสงค์ในการประกันภัยไว้ ให้หมายถึง การให้คำปรึกษา การจัดสรร การพิจารณาเพื่อรับประกันภัย การให้บริการเกี่ยวกับการประกันภัย การดำเนินการเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัย การใช้สิทธิตามสัญญาหรือภาระผูกพันที่เกิดขึ้นตามสัญญาประกันภัย หรือกฎหมาย หรือหลักนิติธรรม[19]

ข้อสังเกตอย่างหนึ่งเกี่ยวกับ Data Protection Act 2018 คือ แม้ประเทศอังกฤษจะออกจากการเป็นรัฐสมาชิกของสหภาพยุโรปแล้ว แต่ GDPR ก็ยังคงมีอิทธิพลกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษเช่นเดิม อย่างไรก็ตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษได้กำหนดเรื่องการประกันภัยว่าถือเป็นประโยชน์สาธารณะ หากเป็นการประมวลผลข้อมูลส่วนบุคคลของผู้เอาประกันหรือผู้ที่เกี่ยวข้องกับสัญญาประกันภัย เช่น ผู้เอาประกันภัย ผู้รับผลประโยชน์ตามสัญญาประกันภัย ผู้เสียหายที่ต้องได้รับค่าสินไหมทดแทนตามสัญญาประกันภัย เป็นต้น โดยการประมวลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเช่นว่านั้น ต้องเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการให้คำปรึกษา การจัดสรร การพิจารณาเพื่อรับประกันภัย การให้บริการเกี่ยวกับการประกันภัย การดำเนินการเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัย การใช้สิทธิตามสัญญาหรือภาระผูกพันที่เกิดขึ้นตามสัญญาประกันภัย หรือกฎหมาย ดังนั้น บริษัทประกันภัย ตัวแทนประกันภัยหรือนายหน้าประกันภัยในประเทศอังกฤษ สามารถเก็บ ใช้ เปิดเผยข้อมูลสุขภาพของผู้เอาประกันภัยเพื่อพิจารณารับประกันภัย หรือเก็บ ใช้ เปิดเผยเพื่อกิจกรรมในการชดใช้ค่าสินไหมทดแทนโดยไม่ต้องข้อความยินยอมจากเจ้าของข้อมูลก่อนหรือขณะการนำข้อมูลมาใช้สำหรับกรณีข้างต้น แต่หากเป็นการใช้เพื่อโทรขายสินค้า หรือติดต่อลูกค้าในกรณีอื่นนอกเหนือจากวัตถุประสงค์ที่มีความเกี่ยวข้องกับสัญญาประกันภัย หรือนอกเหนือความคาดหมายทั่วไปของผู้เอาประกันภัยแล้ว บริษัทประกันภัยและผู้ที่เกี่ยวข้องยังคงต้องขอความยินยอมเช่นเดิม ซึ่งหากพิจารณาแล้วจะเห็นว่าประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้กำหนดแนวปฏิบัติในธุรกิจประกันภัยโดยสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษฉบับนี้

---

[19] Data Protection Act 2018, Schedule 1.

Ref. code: 25646301033624ADV

4.3 Personal Data Protection Act 2012

ประเทศสิงคโปร์เป็นอีกประเทศหนึ่งในทวีปเอเชียที่มีกฎหมายคุ้มครองข้อมูลแล้ว โดยประกาศตั้งแต่วันที่ 2 มกราคม ค.ศ. 2013 และมีผลบังคับใช้ในส่วนของกฎการคุ้มครองข้อมูลส่วนบุคคลในวันที่ 2 กรกฎาคม ค.ศ. 2014 ต่อมาในปี ค.ศ. 2020 ประเทศสิงคโปร์ได้มีการแก้ไขเพิ่มเติมกฎหมายฉบับดังกล่าว ในวันที่ 2 พฤศจิกายน และบังคับให้มีผลในวันที่ 1 กุมภาพันธ์ ค.ศ. 2021[20] นอกจากนี้ ยังมีการประกาศข้อบังคับและกฎหมายลำดับรองมาเพื่อเป็นแนวทางในการปฏิบัติให้กับหน่วยงานต่างๆ ปฏิบัติตาม Personal Data Protection Act 2012 ด้วย โดยใน Personal Data Protection Act 2012 มีแนวทางสำหรับธุรกิจประกันภัยซึ่งเกี่ยวข้องโดยตรงกับหัวข้อรายงานการค้นคว้าอิสระนี้โดยตรง ดังนี้

4.3.1 มีการกำหนดให้การรับประกันภัยบุคคล หรือ ทรัพย์สิน หรือการต่อประกันภัยบุคคลหรือทรัพย์สินนั้น เป็นหนึ่งใน “การประมวลผลข้อมูลส่วนบุคคลเพื่อการประเมิน” (Evaluation purpose)[21]

4.3.2 มีการกำหนดให้การประมวลผลข้อมูลส่วนบุคคลเพื่อการประเมินเป็นการเก็บ ใช้ และเปิดเผยข้อมูลที่ไม่ต้องขอความยินยอม[22]

4.3.3 มีการกำหนดให้กรมธรรม์ แผนบำเหน็จบำนาญ เงินรายปี กองทุนสำรองเลี้ยงชีพ หรือแผนอื่นที่คล้ายคลึงกัน เป็น “แผนผลประโยชน์” (benefit plan)[23]

4.3.4 การเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในการดำเนินการตามแผนผลประโยชน์แก่เจ้าของข้อมูล รวมถึงการจัดการต่างๆ เกี่ยวกับแผนประกันภัยโดยผู้จัดการแผนผลประโยชน์ด้วย[24]

---

[20] ‘PDPA Overview’, (PERSONAL DATA PROTECTION COMMITTEE SINGAPORE) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> สืบค้นเมื่อวันที่ 10 มิถุนายน 2565.

[21] Personal Data Protection Act 2012, Part 1 PRELIMINARY Section 2.

[22] Personal Data Protection Act 2012, FIRST SCHEDULE Collection, use and disclosure of personal data without consent PART 3 LEGITIMATE INTERESTS, Article 2.

[23] Personal Data Protection Act 2012, Part 1 PRELIMINARY Section 2.

[24] Personal Data Protection Act 2012, FIRST SCHEDULE Collection, use and disclosure of personal data without consent PART 3 LEGITIMATE INTERESTS, Article 7.

Ref. code: 25646301033624ADV

ทั้งนี้ ใน Personal Data Protection Act 2012 ไม่มีการแบ่งแยก ข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว แต่ก็มีแนวปฏิบัติจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ในเรื่องของการใช้ข้อมูลที่มีความอ่อนไหว เช่น คู่มือการใช้ข้อมูลที่เกี่ยวกับสุขภาพกายและสุขภาพจิต เป็นต้น ต้องได้รับการดูแลความปลอดภัยที่เหมาะสมกับข้อมูลส่วนบุคคลนั้นๆ เท่านั้น[25] ผู้ประกอบธุรกิจประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัยในประเทศสิงคโปร์จึงไม่ต้องขอความยินยอมจากเจ้าของข้อมูล เมื่อเก็บข้อมูลสุขภาพหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำสัญญาประกันภัย เพราะถือเป็นกิจกรรมที่ได้รับการยกเว้นไม่ต้องขอความยินยอม และมิได้มีมาตรฐานในการแยกข้อมูลว่าเป็นข้อมูลส่วนบุคคลทั่วไปหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่กำหนดแนวปฏิบัติไว้แตกต่างกัน

4.4 กรณีศึกษาการใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวในธุรกิจประกันภัย

เนื่องจากกรณีศึกษาและการลงโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ยังไม่เกิดขึ้นจริงในประเทศไทย กลุ่มกรณีศึกษาต่างๆ จึงต้องนำมาจากต่างประเทศ ซึ่งมีกรณีที่น่าสนใจเกี่ยวกับการใช้ข้อมูลสุขภาพที่อาจนำมาพิจารณาเพื่อหาแนวทางป้องกัน และปรับปรุงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลของประเทศไทยอันเกี่ยวเนื่องกับการใช้ข้อมูลส่วนบุคคลในธุรกิจประกันภัยได้ ผู้เขียนจึงขอยกกรณีศึกษาที่น่าสนใจ ดังนี้

4.4.1 กรณีการเก็บ ใช้ เปิดเผยข้อมูลสุขภาพสำหรับการเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัย

The Office of the Data Protection Ombudsman หน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคลของประเทศฟินแลนด์ได้สอบสวนกระบวนการขอข้อมูลผู้ป่วยของศูนย์ประกันภัยรถยนต์ ในกรณีที่ศูนย์ประกันภัยรถยนต์ได้เก็บข้อมูลผู้ป่วยเป็นจำนวนมากและร้องขอข้อมูลสุขภาพที่เป็นข้อมูลต้นฉบับของผู้ป่วยเพื่อพิจารณาค่าสินไหมทดแทน นอกจากนี้ ยังขอข้อมูลการนัดหมายผู้ป่วยจากผู้ให้บริการด้านสุขภาพเพื่อพิจารณาว่าได้มีการนัดหมายที่ไม่จำเป็น หรือเก็บค่าบริการที่ไม่เกี่ยวข้องกับอุบัติเหตุทางถนนหรือไม่ และยังร้องขอข้อมูลอื่นๆ ที่ไม่จำเป็นต่อการพิจารณาค่าสินไหมทดแทนอย่างแท้จริงอีกด้วย โดยศูนย์ประกันภัยรถยนต์ถูกตัดสินว่าละเมิด

---

[25] ‘Singapore’ (DLA Piper, 21 December 2021) <https://www.dlapiperdataprotection.com/index.html?t=law&c=SG&c2=> สืบค้นเมื่อวันที่ 11 มิถุนายน 2565.

Ref. code: 25646301033624ADV

กฎหมายคุ้มครองข้อมูลส่วนบุคคลในเรื่องของการขอข้อมูลทั้งหมดของผู้ป่วยแทนที่จะขอเพียงแต่ข้อมูลที่จำเป็นสำหรับการพิจารณาค่าสินไหมทดแทน ซึ่งพระราชบัญญัติประกันภัยทางจราจร (Traffic Insurance Act) ของประเทศฟินแลนด์ ก็มิได้มีข้อกำหนดให้ผู้รับประกันภัยอาจเข้าถึง หรือร้องขอข้อมูลทั้งหมดของผู้ป่วย แต่พระราชบัญญัติดังกล่าวกำหนดให้ข้อมูลที่ร้องขอจะต้องมีความจำเป็นต่อการเรียกร้องค่าสินไหมทดแทนเท่านั้น โดยสมาคมการแพทย์ฟินแลนด์ได้ให้คำแนะนำว่าข้อมูลสุขภาพที่ควรเปิดเผยให้กับบริษัทประกันภัยนั้น ควรมีลักษณะเป็นความเห็นทางการแพทย์เท่านั้น มิใช่ข้อมูลต้นฉบับที่เป็นการวินิจฉัยอาการของผู้ป่วย ด้วยเหตุดังกล่าว คณะกรรมการตัดสินของ The Office of the Data Protection Ombudsman ลงโทษปรับศูนย์ประกันภัยรถยนต์ของฟินแลนด์เป็นเงิน 52,000 ยูโร และได้สั่งให้แก้ไขแนวปฏิบัติในเรื่องการขอข้อมูลผู้ป่วยให้สอดคล้องกับระเบียบข้อบังคับด้านการคุ้มครองข้อมูล อย่างไรก็ตาม ศูนย์ประกันภัยรถยนต์อยู่ระหว่างการอุทธรณ์คำตัดสินดังกล่าว[26]

ถึงแม้ว่ากรณีศึกษาดังกล่าวจะยังไม่มีคำตัดสินออกมาถึงที่สุด ผู้ควบคุมข้อมูลที่เกี่ยวข้อง เช่น บริษัทประกันและสถานพยาบาลต่างๆ ในประเทศไทย ก็อาจนำกรณีศึกษาดังกล่าวมาพิจารณาถึงแนวปฏิบัติการเก็บ ใช้ และเปิดเผยข้อมูลสุขภาพของผู้ป่วยระหว่างโรงพยาบาลและบริษัทประกันภัยในประเทศไทย สำหรับการพิจารณาค่าสินไหมทดแทนได้ ซึ่งอาจนำมากำหนดเป็นกฎหมาย นโยบาย หรือแนวปฏิบัติของโรงพยาบาล สถานพยาบาล สมาคมประกันชีวิต และสมาคมประกันวินาศภัย โดยมีวัตถุประสงค์เพื่อก่อให้เกิดความมั่นใจแก่เจ้าของข้อมูลส่วนบุคคล ผู้ใช้บริการสถานพยาบาลที่มีประกันชีวิต ประกันวินาศภัยหรือประกันสุขภาพได้

4.4.2 กรณีการเก็บข้อมูลเกินเวลาที่กำหนดไว้ และการบันทึกเสียงสำหรับการโทรศัพท์โดยไม่แจ้งสิทธิ

ในปี 2019 Commission Nationale de l'Informatique et des Libertés หรือ CNIL หน่วยงานกำกับดูแลของประเทศสาธารณรัฐฝรั่งเศสได้เข้าตรวจสอบบริษัทประกันภัยแห่งหนึ่งของประเทศสาธารณรัฐฝรั่งเศสและพบว่าบริษัทดังกล่าวเก็บข้อมูลส่วนบุคคลของลูกค้าหลายล้านรายเกินเวลาที่ได้กำหนดไว้ และยังละเมิดข้อกำหนดเกี่ยวกับการโทรศัพท์ของบริษัทประกันภัยด้วย จึงตัดสินให้บริษัทประกันภัยดังกล่าว ล้มเหลวในการปฏิบัติตาม GDPR ข้อ 5-1-e ข้อ 13 และข้อ 14

---

[26] Administrative fine imposed on the Finnish Motor Insurers' Centre for the collection of unnecessary patient information <https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-finnish-motor-insurers-centre-collection_en> สืบค้นเมื่อวันที่ 13 มีนาคม 2565.

Ref. code: 25646301033624ADV

สำหรับความผิดในการไม่สามารถปฏิบัติตาม GDPR ข้อ 5-1-e ในกรณีเก็บข้อมูลของลูกค้าที่ไม่มีการติดต่อใดๆ กับบริษัทเลยมาเป็นระยะเวลาตั้งแต่ 3-5 ปี ประมาณ 2,000 ราย และการเก็บข้อมูลของลูกค้าซึ่งรวมถึงข้อมูลสุขภาพมากกว่า 2 ล้านรายที่เกินระยะเวลานั้น บริษัทได้ดำเนินการแก้ไขแนวทางปฏิบัติบางส่วนและให้คำมั่นว่าจะดำเนินการปฏิบัติตามในเรื่องของการกำจัดข้อมูลที่เก็บไว้เกินระยะเวลาที่กฎหมายกำหนด

สำหรับความผิดในการไม่สามารถปฏิบัติตาม GDPR ข้อ 13 และข้อ 14 นั้น เนื่องจากบริษัทบันทึกเสียงโดยไม่ได้ขออนุญาตลูกค้า และยังไม่แจ้งสิทธิในการคัดค้านการเก็บ ใช้ข้อมูลของลูกค้าด้วยนั้น บริษัทประกันภัยดังกล่าวก็ได้ดำเนินการปรับปรุงกระบวนการที่เกี่ยวข้องเพื่อให้สอดคล้องกับ GDPR แล้ว อย่างไรก็ตาม ในกรณีนี้ บริษัทดังกล่าวถูกปรับจากการไม่ปฏิบัติตาม GDPR เป็นเงิน 1.7 ล้านยูโร[27]

การไม่ปฏิบัติตามกฎหมายเรื่องระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลนั้น อาจพิจารณาเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทยได้ อย่างไรก็ตาม ในการพิจารณาถึงระยะเวลาที่เหมาะสมนั้น ในประเทศไทยยังไม่มีแนวปฏิบัติ หรือข้อกฎหมายที่กำหนดให้บริษัทประกันภัยเก็บข้อมูลไว้ได้เท่าใด จึงยังมีการอ้างอิงระยะเวลาการดำเนินคดีตามกฎหมายแพ่งและพาณิชย์ กฎหมายเกี่ยวกับป้องกันและปราบปรามการฟอกเงิน ซึ่งจัดเก็บข้อมูลสูงสุดถึง 10 ปี แต่ในแง่ของการเก็บข้อมูลของลูกค้าที่มิได้มีนิติสัมพันธ์กับบริษัทนั้น ยังคงเป็นระยะเวลาที่บริษัทกำหนดได้อย่างอิสระเนื่องจากไม่มีเกณฑ์ใดมาบังคับ นอกจากนี้ การจะลงโทษบริษัทต่างๆ ในประเทศไทย ด้วยเหตุดังกล่าวนั้น ภาครัฐหรือหน่วยงานกำกับดูแลควรมีการกำหนดแนวปฏิบัติหรือแนวทางที่ชัดเจนก่อนจึงจะสามารถสั่งปรับบริษัทเหล่านั้นได้ กรณีตัวอย่างในเรื่องนี้จึงอาจนำมาพิจารณาปรับปรุงการดำเนินงานทั้งของภาครัฐเพื่อควบคุมดูแลผู้ประกอบกิจการภาคเอกชน และในส่วนของภาคเอกชนเองอาจนำมาพิจารณาเพื่อเป็นแนวทางการปรับปรุงการดำเนินงานโดยการกำหนดนโยบายการจัดเก็บข้อมูลลูกค้าเป็นระยะเวลาที่เหมาะสมและกำจัดข้อมูลที่เกินกำหนดนั้นๆ ตานโยบายที่ได้เขียนไว้

---

[27] French DPA: 1.75 million penalty against AG2R LA MONDIALE <https://edpb.europa.eu/news/national-news/2021/french-dpa-175-million-penalty-againstag2r-la-mondiale_en> สืบค้นเมื่อวันที่ 20 มีนาคม 2565.

Ref. code: 25646301033624ADV

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ได้กำหนดประเด็นสำคัญซึ่งเป็นประเด็นปัญหาของหัวข้อการค้นคว้าอิสระฉบับนี้ คือ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าเพื่อการประกันภัย ซึ่งกำหนดให้สามารถกระทำได้โดยไม่ต้องขอความยินยอม โดยใช้การประมวลผลข้อมูลฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์อันเป็นประโยชน์สาธารณะที่สำคัญ อันมีประเด็นปัญหาที่ต้องพิจารณาหาแนวทางแก้ไขเพื่อให้สอดคล้องกับความคิดเห็นทั้งสำหรับผู้ที่เห็นด้วย[1]และผู้ที่ไม่เห็นด้วย[2] กับประเด็นดังกล่าว[3] ทั้งนี้ จากการศึกษากฎหมายภายนอกและภายในประเทศ รวมถึง การสัมภาษณ์และจัดทำแบบสอบถามความคิดเห็นเกี่ยวกับแนวทางดังกล่าวแล้วนั้น ผู้เขียนมีความเห็นว่าประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยดังกล่าว มีปัญหาตีความที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยเหตุผลดังต่อไปนี้

1. จากการสำรวจความคิดเห็นและสัมภาษณ์บุคลากรผู้มีความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น พบว่ามีผู้ที่มีข้อสงสัยและไม่เห็นด้วยในการระบุว่า

---

[1]สัมภาษณ์ทาง Google Meet รุ่งเรือง สัมฤทธิ์ทรัพย์, เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล, บริษัท เอเอสเอ็นโบรกเกอร์ จำกัด (มหาชน), (16 กรกฎาคม 2565).

[2] สัมภาษณ์ทางโทรศัพท์ สุวรรณโชติ ศิริมหาศาล, ที่ปรึกษาด้านการพัฒนาระบบและวิทยากรเรื่องข้อมูลส่วนบุคคล, สำนักงานพัฒนารัฐบาลดิจิทัล, (17 กรกฎาคม 2565).

[3] ‘ผลสำรวจการตอบแบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564’ (ภาคผนวก ฉ).

Ref. code: 25646301033624ADV

การประกันภัยเป็นประโยชน์สาธารณะที่สำคัญ โดยเฉพาะอย่างยิ่งกลุ่มผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มิใช่บุคลากรในธุรกิจประกันภัย นอกจากนี้ แม้แนวทางการตีความของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเป็นแนวทางเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ แต่ใน GDPR ซึ่งเป็นกฎหมายแม่แบบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีข้อกำหนดที่แตกต่างออกไปคือบริษัทประกันภัยไม่สามารถอาศัยประโยชน์ในฐานกฎหมายเพื่อยกเว้นการขอความยินยอมจากลูกค้าได้[4]

2. แบบสัญญามาตรฐานของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ยังคงมีการขอความยินยอมเพื่อเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวสำหรับวัตถุประสงค์เพื่อการประกันภัยอยู่ด้วย แม้เป็นแบบสัญญามาตรฐานที่ประกาศออกมาหลังประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ก็ตาม ซึ่งสะท้อนให้เห็นว่าการบ่งชี้ว่าบริษัทประกันภัยจะไม่ขอความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยใช้การประมวลผลข้อมูลฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์อันเป็นประโยชน์สาธารณะนั้น ยังมิได้เป็นมาตรฐานที่ถูกนำมาใช้โดยเด็ดขาด

3. การออกประกาศดังกล่าวมิได้ครอบคลุมไปถึงผู้ที่เกี่ยวข้องในสัญญาประกันภัย แต่มิได้อยู่ภายใต้การกำกับของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เช่น โรงพยาบาล สถานพยาบาล อู่ซ่อมรถยนต์ เป็นต้น ส่งผลให้ผู้ที่มิได้อยู่ภายใต้การกำกับเหล่านี้อาจโต้แย้งแนวปฏิบัติของผู้ประกอบธุรกิจภายใต้การกำกับได้ โดยเฉพาะเมื่อไม่มีการขอความยินยอมก่อนหรือขณะเก็บรวบรวม ใช้ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

4. การระบุให้มีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลจากแหล่งข้อมูลอื่น เช่น การเก็บข้อมูลส่วนบุคคลของคู่สมรส บุคคลในครอบครัว หรือบุคคลอื่นที่จำเป็นจากผู้เอาประกันภัย หรือการเก็บข้อมูลส่วนบุคคลของพนักงานในสังกัดผู้เอาประกันภัยกลุ่มนั้น เห็นควรดำเนินการตามมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบกับแนวปฏิบัติของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยด้วย กล่าวคือ นอกจากมีการเก็บคำรับรองจากผู้ให้ข้อมูลหรือผู้เอาประกันภัยว่าได้มีการแจ้งนโยบายคุ้มครอง

---

[4] Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) (54).

Ref. code: 25646301033624ADV

ข้อมูลส่วนบุคคลของผู้รับประกันภัย และได้มีการจัดทำความยินยอมเมื่อจำเป็นต้องขอความยินยอมแล้วนั้น ผู้รับประกันภัยในฐานะผู้ควบคุมข้อมูลควรแจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทางช่องทางใดช่องทางหนึ่งที่ผู้เอาประกันภัยแจ้ง เช่น ข้อความสั้นทางโทรศัพท์ จดหมายอิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ เพื่อให้เป็นไปตามเจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. โดยบทบาทหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา16 (3) นั้น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรเป็นผู้ออกประกาศที่จะกำหนดความหมาย หรือแนวปฏิบัติในการอ้างฐานทางกฎหมายสำหรับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้การบังคับใช้ครอบคลุมไปถึงบุคคลและผู้ประกอบธุรกิจในทุกภาคส่วนอย่างเท่าเทียมกัน ซึ่งรวมถึงการพิจารณาบทลงโทษอันเนื่องมาจากการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลด้วย

5.2 ข้อเสนอแนะ

เพื่อแก้ปัญหาการตีความที่แตกต่างกันของกลุ่มบุคลากรในธรุกิจประกันภัย และบุคคลอื่นซึ่งศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อการพิจารณารับประกันภัย การเอาประกันภัยต่อ พิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัยแต่ละประเภท หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้ฐานการประมวลผข้อมูลเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์อันเกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ และไม่ต้องขอความยินยอมนั้น ผู้เขียนมีข้อเสนอแนะ ดังต่อไปนี้

5.2.1 เสนอให้มีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

มาตรา 3 กำหนดว่า “ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติ เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติ แห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการ

Ref. code: 25646301033624ADV

นั้นหรือไม่ก็ตาม” อันแสดงให้เห็นว่าหากกิจการประเภทใดที่มีหน่วยงานกำกับดูแลกำหนดแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอยู่แล้ว กระทำการใดที่เป็นความผิดในการละเมิดข้อมูลส่วนบุคคล อาจทำให้ผู้ประกอบกิจการรายนั้นถูกลงโทษทั้งจากหน่วยงานกำกับดูแลและจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น หากบริษัทประกันภัยแห่งหนึ่งดำเนินการละเมิดข้อมูลส่วนบุคคล บริษัทประกันภัยรายนั้นจะได้รับโทษจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทั้งโทษทางปกครองและทางอาญาในการกระทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และจะได้รับโทษจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย–เนื่องจากการกระทำความผิดตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ซึ่งมีบทลงโทษทั้งทางปกครองและทางอาญาเช่นกัน ทำให้ธุรกิจที่อยู่ภายใต้การกำกับของหน่วยงานกำกับดูแลโดยเฉพาะอยู่แล้วนั้นไม่ได้รับความเป็นธรรม ผู้เขียนจึงขอเสนอให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลปรับปรุงมาตรา 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้เป็น “ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมาย ว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติ เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติ แห่งพระราชบัญญัตินี้แทน”

มาตรา 26 เสนอให้แก้ไขเพิ่มเติมโดยเติมข้อความดังต่อไปนี้เป็นวรรคท้าย

“การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว หากเป็นไปเพื่อการจำเป็นสำหรับการประกันภัย โดยมีมาตรการเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ในวัตถุประสงค์อื่น หรือก่อสิทธิหรือภาระผูกพันอื่นที่เจ้าของข้อมูลไม่อาจคาดหมายได้ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลดังกล่าวสามารถกระทำได้โดยถือเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ”

ทั้งนี้ เป็นไปตามแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคลประเทศอังกฤษ หรือ Data Protection Act 2018

5.2.2 เสนอให้รัฐมนตรีว่าการกระทรวงการคลังพิจารณาเสนอร่างกฎหมายพระราชกฤษฎีกา เรื่อง การเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลในกิจการประกันภัยที่ถือเป็นการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่เป็นประโยชน์สาธารณะที่สำคัญ

โดยมีเนื้อหาระบุกรณีตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับ

Ref. code: 25646301033624ADV

ธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ที่ถือเป็นประโยชน์สาธารณะ ได้แก่ “ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยใช้การประมวลผลฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อบรรลุวัตถุประสงค์ที่เกี่ยวข้องกับสาธารณะประโยชน์ที่สำคัญตามมาตรา 26 (4) (จ) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล สำหรับกรณีดังต่อไปนี้

(1) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต เพื่อพิจารณารับประกันภัย การเอาประกันภัยต่อ พิจารณารับประกันภัยต่อ การปฏิเสธการรับประกันภัยแต่ละประเภท หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัย

(2) การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นเพื่อเปิดเผยให้สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อรายงานเกี่ยวกับการฉ้อฉลประกันภัย หรือรายงานอื่นตามกฎหมายที่เกี่ยวข้อง

(3) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่สำเป็นเพื่อเปิดเผยให้สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเพื่อประโยชน์ในการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และกฎหมายอื่น”

โดยผู้เขียนขอเสนอให้มีการจำกัดข้อมูลส่วนบุคคลที่มีความอ่อนไหวใน (1) เพียงข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต เพื่อลดข้อกังวลและความเสี่ยงในการถูกร้องเรียนหรือยกประเด็นโต้แย้งของผู้ที่ไม่เห็นด้วยกับแนวทางการตีความดังกล่าว และการดำเนินการตามข้อเสนอ 5.2.2 นี้

ทั้งนี้ ข้อเสนอนี้เป็นการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 วรรคสอง

5.2.3 เสนอให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดกิจการที่ถือเป็นเป็นประโยชน์สาธารณะที่สำคัญ

โดยมีเนื้อหาระบุถึงกรณีต่างๆ ที่ถือเป็นประโยชน์สาธารณะที่สำคัญและสามารถเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอม และมีตอนหนึ่งระบุให้การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลดังต่อไปนี้ เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26 (5) (จ)

Ref. code: 25646301033624ADV

(1) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต เพื่อพิจารณารับประกันภัย การเอาประกันภัยต่อ พิจารณารับประกันภัยต่อ การปฏิเสธการรับประกันภัยแต่ละประเภท หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัย

(2) การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่จำเป็นเพื่อเปิดเผยให้สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อรายงานเกี่ยวกับการฉ้อฉลประกันภัย หรือรายงานอื่นตามกฎหมายที่เกี่ยวข้อง

(3) การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่สำเป็นเพื่อเปิดเผยให้สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยเพื่อประโยชน์ในการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และกฎหมายอื่น

5.2.4 เสนอให้มีการส่งประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณา

ผู้เขียนขอเสนอให้คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย นำส่งประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อพิจารณาและให้คำแนะนำเพิ่มเติมตาม ร่าง แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล พ.ศ. ....

ทั้งนี้ ข้อเสนอแนะ ข้อที่ 5.2.1 ถึง ข้อที่ 5.2.4 นั้น อาจดำเนินการเพียงข้อใดข้อหนึ่งเพื่อลดปัญหาการตีความที่ไม่ชัดเจน ข้อกังวลของผู้ประกอบธุรกิจเกี่ยวกับการประกันภัย และความเสี่ยงในการถูกร้องเรียนจากการไม่ขอความยินยอมเพื่อเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำสัญญาประกันภัยจากผู้ที่มีความเห็นแตกต่างสำหรับการตีความดังกล่าว โดยหากพิจารณาถึงบทบาทหน้าที่และความรวดเร็วของขั้นตอนการดำเนินการออกกฎหมายหรือประกาศแล้ว ผู้เขียนมีความเห็นว่าการดำเนินการตามข้อ 5.2.3 ถือเป็นทางเลือกที่เหมาะสมและรวดเร็วที่สุด

Ref. code: 25646301033624ADV

5.2.5 เสนอให้แก้ไขประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

นอกจากประเด็นเรื่องการใช้การประมวลผลฐานการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์อันเกี่ยวข้องกับประโยชน์สาธารณะที่สำคัญ และไม่ต้องขอความยินยอมดังที่กล่าวมาแล้วนั้น ผู้เขียนมีข้อเสนแนะเพิ่มเติมเพื่อป้องกันข้อร้องเรียน และข้อพิพาทเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในกรณีผู้รับประกันภัยได้ข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องในสัญญาประกันภัยจากผู้เอาประกันภัยซึ่งถือเป็นการได้ข้อมูลมาจากแหล่งอื่นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 25 นั้น เดิมมีแนวปฏิบัติกำหนดให้บริษัทผู้เอาประกันภัยให้คำรับรองต่อบริษัทผู้รับประกันภัยว่าได้แจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทประกันภัย และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเปิดเผยข้อมูลกับบริษัทประกันแล้ว โดยอาจเก็บหนังสือดังกล่าวไว้ที่ผู้เอาประกันได้นั้น[5] ผู้เขียนขอเสนอให้มีการเพิ่มเติมการแจ้งถึงการเก็บรวบรวมข้อมูลและแจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลภายใน 30 วันนับแต่วันที่ได้รับข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ร่วมกับการดำเนินการตามเดิมด้วย

หากมีการดำเนินการตามข้อเสนอแนะข้อที่ 5.2.1 ถึง ข้อที่ 5.2.4 ข้อใดข้อหนึ่งแล้วนั้น การดำเนินการในข้อเสนอแนะข้อที่ 5.2.5 นี้ จะถือว่าเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่องการนำข้อมูลจากแหล่งอื่นมาเก็บรวบรวม ใช้ และเปิดเผยเช่นกัน

---

[5] ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต ข้อ 6 (4) (ก).

Ref. code: 25646301033624ADV

บรรณานุกรม

หนังสือและบทความในหนังสือ

ภาษาไทย

กฤษฎ์ อุทัยรัตน์, *บทสรุป PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล หลักการ แนวคิด ข้อกฎหมาย กรณีศึกษาและแนวปฏิบัติ* (บริษัท ธรรมนิติ เพรส จำกัด 2563).

นคร เสรีรักษ์, *ความเป็นส่วนตัว* (พิมพ์ครั้งที่ 2, บริษัท พี.เพรส จำกัด 2563).

นคร เสรีรักษ์ และคณะ, *General Data Protection Regulation ฉบับภาษาไทย* (บริษัท พี.เพรส จำกัด 2563).

ปรีดี หงษ์สต้น และ อัมพร หมาดเด็น, *ศาสนากับความรุนแรง* (พิมพ์ครั้งที่ 1, สำนักพิมพ์ Illuminations Edition 2562).

ภาษาต่างประเทศ

Andreas Mueller and Peter Schaber, *The Routledge Handbook of the Ethics of Consent* (London: Taylor and Francis, Kindle Locations).

Gaham J H Smith Bird & Bird, *Internet Law and Regulation* (4th Edition, Sweet & Maxwell 2007).

Noriswadi Ismal, *Understanding Personal Data Protection Law* (Percetakan Jiwabaru Sdn Bhd).

Peter Carey, *Data Protection A Practical Guide to UK and EU law* (2nd Edition, Oxford University Press 2004).

Robert Walters and others, *Data Protection Law, A Comparative Analysis of Asia-Pacific and European Approaches* (Markono Print Media Pte Ltd, 2019).

Sanjay Sharma, *Data Privacy and GDPR Handbook* (United States of America 2020).

Susan Singleton, *Tolley's Data Protection Handbook* (4th edn, CPI Bath Press, 2006).

Ref. code: 25646301033624ADV

บทความวารสาร

ภาษาไทย

กิตติศักดิ์ จันเส, ‘มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต’ <http://www.research.rmutt.ac.th/wp-content/uploads/2012/05/%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%83%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5.pdf> สืบค้นเมื่อวันที่ 8 พฤษภาคม 2565.

จรีลักษณ์ รัตนาพันธ์, ‘เพศวิถีศึกษา : ผลกระทบต่อสถาบันทางสังคม’ (2563) 2 วารสารอิเล็กทรอนิกส์การเรียนรู้ทางไกลเชิงนวัตกรรม 28-30 <https://so01.tci-thaijo.org/index.php/e-jodil/article/view/244879/165675> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

นาวา ผานะวงค์, ‘ผลการใช้โปรแกรมลดการตีตราและการเลือกปฏิบัติกับผู้ติดเชื้อเอชไอวีในโรงพยาบาลอากาศอำนวย จังหวัดสกลนคร ปี พ.ศ. 2562’ (2562) วารสารโรคเอดส์ 130 <https://he02.tci-thaijo.org/index.php/ThaiAIDSJournal/article/view/253772/172531> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

วิภู วิมลเศรษฐ และศิริรัตน์ ชูสกุลเกรียง, ‘ฐานข้อมูลสารพันธุกรรมในประเทศไทย DNA Database in Thailand’ (2563) 3 วารสารกระบวนการยุติธรรม 61 < https://so04.tci-thaijo.org/index.php/JTJS/article/view/241983/169320> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

ภาษาต่างประเทศ

Chloe Flascher ‘LGBTQ+ and protecting your privacy in the UK’ (10 June 2020) Withersworldwide <https://www.withersworldwide.com/en-gb/insight/lgbtq-and-protecting-your-privacy-in-the-uk> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

Graison Dangor, ‘Facebook Overpaid FTC Fine By Billions To Protect Zuckerberg, Lawsuits Say’ (2021) <https://www.forbes.com/sites/graisondangor/2021/09/21/facebook-overpaid-ftc-fine-by-billions-to-protect-zuckerberg-lawsuits-say/?sh=25169fe8352e> สืบค้นเมื่อวันที่ 27 มีนาคม 2565.

Luke Irwin, ‘The GDPR: What is sensitive personal data?’ (it governance, 3 December 2020) <https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data> สืบค้นเมื่อวันที่ 2 มิถุนายน 2565.

Mary Kirwan and others, ‘What GDPR and the Health Research Regulations (HRRs) mean for Ireland: “explicit consent”—a legal analysis’ (2020) Irish Journal of Medical Science (1971 -) (2021) 516-517 <https://link.springer.com/content/pdf/10.1007/s11845-020-02331-2.pdf> สืบค้นเมื่อวันที่ 28 ธันวาคม 2564.

Paula Peñacoba, ‘Identified by religion: Religion on national ID cards’ (Underground Network) <https://underground.net/identified-by-religion-religion-on-national-id-cards/> สืบค้นเมื่อวันที่ 5 มิถุนายน 2565.

Paul Quinn and Gianclaudio Malgieri, ‘The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework’ (Cambridge University Press, 19 January 2022) <https://www.cambridge.org/core/journals/german-law-journal/article/difficulty-of-defining-sensitive-datathe-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C90045813F6C6> สืบค้นเมื่อวันที่ 4 มิถุนายน 2465.

Selin Esen and Levent Gonenç, ‘Religious Information on Identity Cards: A Turkish Debate’ (Cambridge University Press, 24 April 2015) <https://www.cambridge.org/core/journals/journal-of-law-and-religion/article/abs/religious-information-on-identity-cards-a-turkish-debate/A992BF6304C33E8922FB028F18075B5C> สืบค้นเมื่อวันที่ 5 มิถุนายน 2565.

---,‘Consent’ (Information Commissioner’s Office, Guideline to GDPR) <https://ico.org.uk/ for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

Ref. code: 25646301033624ADV

---, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ (2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> สืบค้นเมื่อวันที่ 3 มิถุนายน 2565.

---, ‘What are the conditions for processing?’ (Information Commissioner’s Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions6> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

---, ‘What is ‘explicit consent’?’ (Information Commissioner’s Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=The%20key%20difference%20is%20likely,action%20(which%20would%20not).> สืบค้นเมื่อวันที่ 28 ธันวาคม 2564.

---, ‘Why is this data special?’ (Information Commissioner’s Office, Guideline to GDPR) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

บทความหนังสือพิมพ์

ภาษาไทย

กุลธิดา สามะพุทธิ, ‘พริษฐ์ ชิวารักษ์: จดหมายจากเรือนจำ น้ำตาของแม่และการเดินทางไกลของหญิงวัย 51 ปี’ BBC NEWS (2 มีนาคม 2564) <https://www.bbc.com/thai/56182261> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

ธันยพร บัวทอง, ‘รุ้ง ปนัสยา: ฟังพี่สาวเล่าเรื่องน้องคนเล็กผู้กลายเป็นแกนนำ “ราษฎร” และผู้ต้องหามิ่นสถาบันฯ’ BBC NEWS (25 ธันวาคม 2563) <https://www.bbc.com/thai/thailand-55442292> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

---, ‘เลื่อนบังคับใช้ พ.ร.บ.ข้อมูลบุคคล’ ไทยรัฐฉบับพิมพ์ (20 พฤษภาคม 2563) <https://www.thairath.co.th/business/economics/1848624> สืบค้นเมื่อวันที่ 15 ธันวาคม 2564.

Ref. code: 25646301033624ADV

ภาษาต่างประเทศ

---, ‘Brexit: What you need to know about the UK leaving the EU’ BBC News (30 December 2020) <https://www.bbc.com/news/uk-politics-32810887> accessed 23 January 2022.

---, ‘US election 2020: Why racism is still a problem for the world's most powerful country’ BBC News (30 October 2020) <https://www.bbc.com/news/election-us-2020-54738922> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

วิทยานิพนธ์

ชนิดา เกิดกรณ์, ‘ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลต่อฐานข้อมูลการประกันภัยในธุรกิจประกันวินาศภัย’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2563).

บรรเจิด ภาคาพันธุ์, ‘ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2562).

สุธินันท์ ศรีราษฎร์, ‘ความยินยอมในกฎหมายคุ้มครองข้อมูลส่วนบุคคล’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2561).

สุวเพ็ญ ค้ำจุน. ‘ผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีต่ออุตสาหกรรมประกันภัยในประเทศไทย’ (การค้นคว้าอิสระ บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2563).

หทัยชนก หร่ายวงศ์, ‘ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2559).

สื่ออิเล็กทรอนิกส์

ภาษาไทย

ปิยะบุตร บุญอร่ามเรือง และคณะ, ‘แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 3.0)’ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) <https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

เอมผกา เตชะอภัยคุณ, ‘สรุปสาระสำคัญจากเสวนาวิชาการหัวข้อ สถานการณ์กฎหมายเกี่ยวกับความหลากหลายทางเพศ’ (สรุปสาระสำคัญจากเสวนาวิชาการหัวข้อ “สถานการณ์กฎหมาย

Ref. code: 25646301033624ADV

เกี่ยวกับความหลากหลายทางเพศ", คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 26 มิถุนายน 2564) <https://www.law.tu.ac.th/seminar-summary-law-and-lgbtq/> สืบค้นเมื่อวันที่ 27 มีนาคม 2565.

PDPC Thailand, 'ขอเชิญแสดงความคิดเห็นร่างกฎหมายลำดับรองภายใต้ PDPA จำนวน 3 ฉบับ' (เพจเฟซบุ๊ค PDPC Thailand, วันที่ 19 พฤษภาคม 2565) <https://www.facebook.com/pdpc.th>สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

PDPC Thailand, 'ขอเชิญแสดงความคิดเห็น (ร่าง) แนวทางการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จำนวน 2 ฉบับ' (เพจเฟซบุ๊ค PDPC Thailand, วันที่ 19 พฤษภาคม 2565) <https://www.facebook.com/pdpc.th>สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

---, 'คำถามที่พบบ่อยก่อนทำประกันสุขภาพ' (AIA Planer) <https://www.aiaplanner.com/faq/> สืบค้นเมื่อวันที่ 29 ธันวาคม 2564.

---, 'ตัวแทน/นายหน้าประกันภัย' (เว็บไซต์การศึกษา, สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย) <https://www.oic.or.th/th/education/broker> สืบค้นเมื่อวันที่ 29 ธันวาคม 2564.

---, 'นโยบายความเป็นส่วนตัวที่จอดรถ' (บริษัท สยามฟิวเจอร์ดีเวลอปเมนท์ จำกัด (มาหชน)) <https://www.siamfuture.com/th/policy/privacy-policy-parking-lot> สืบค้นเมื่อวันที่ 27 มีนาคม พ.ศ.2565.

---, 'พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554' <https://dictionary.orst.go.th/> สืบค้นเมื่อวันที่ 26 ธันวาคม 2564.

---, 'สคส. เปิดรับฟังความคิดเห็นและข้อเสนอแนะต่อร่างกฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562' (หอการค้าไทย สภาหอการค้าไทย, วันที่ 10 พฤษภาคม 2565) <https://thaichamber.org/activity/%E0%B8%AA%E0%B8%84%E0%B8%AA--%E0%B9%80%E0%B8%9B%E0%B8%B4%E0%B8%94%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%9F%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%84%E0%B8%B4%E0%B8%94%E0%B9%80%E0%B8%AB%E0%B9%87%E0%B8%99%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B9%80%E0%B8%AA%E0%B8%99%E0%B8%AD%E0%B9%81%E0%B8%99%E0%B8%B0%E0%B8%95%E0%B9%88%E0%B8%AD%E0%B8%A3%E0%B9%88%E0%B8%B2

%E0%B8%87%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B8%A5%E0%B8%B3%E0%B8%94%E0%B8%B1%E0%B8%9A%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%A0%E0%B8%B2%E0%B8%A2%E0%B9%83%E0%B8%95%E0%B9%89%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%9A%E0%B8%B1%E0%B8%8D%E0%B8%8D%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5-%E0%B8%9E-%E0%B8%A8--2562> สืบค้นเมื่อวันที่ 4 มิถุนายน 2565.

---, ‘เอกสารเผยแพร่ประชาสัมพันธ์’(กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) <https://www.mdes.go.th/mission/detail/2316-%E0%B9%80%E0%B8%AD%E0%B8%81%E0%B8%AA%E0%B8%B2%E0%B8%A3%E0%B9%80%E0%B8%9C%E0%B8%A2%E0%B9%81%E0%B8%9E%E0%B8%A3%E0%B9%88%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%8A%E0%B8%B2%E0%B8%AA%E0%B8%B1%E0%B8%A1%E0%B8%9E%E0%B8%B1%E0%B8%99%E0%B8%98%E0%B9%8C> สืบค้นเมื่อวันที่ 3 มิถุนายน 2565.

---, ‘UTMOST GOOD FAITH’ (เว็บไซต์คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย) <https://www.oic.or.th/th/node/27334> สืบค้นเมื่อวันที่ 18 ธันวาคม 2564.

ภาษาต่างประเทศ

Lilla Farkas, ‘The meaning of racial or ethnic origin in EU law: between stereotypes and identities’ (January 2017) 57 < https://op.europa.eu/en/publication-detail/-/publication/c1cf6b78-094c-11e7-8a35-01aa75ed71a1/language-en> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

---, ‘Administrative fine imposed on the Finnish Motor Insurers’ Centre for the collection of unnecessary patient information’ <https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-finnish-motor-insurers-centre-collection_en> สืบค้นเมื่อวันที่ 13 มีนาคม 2565

---, ‘Europe and the Refugee Crisis: A Challenge to Our Civilization’ United Nation <https://www.un.org/en/academic-impact/europe-and-refugee-crisis-challenge-our-civilization> สืบค้นเมื่อวันที่ 25 ธันวาคม 2564.

สัมภาษณ์

สัมภาษณ์ทางโทรศัพท์ สุวรรณโชติ ศิริมหาศาล, ที่ปรึกษาด้านการพัฒนาระบบและวิทยากรเรื่องข้อมูลส่วนบุคคล, สำนักงานพัฒนารัฐบาลดิจิทัล, (17 กรกฎาคม 2565).

สัมภาษณ์ทาง Google Meet รุ่งเรือง สัมฤทธิ์ทรัพย์, เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล, บริษัท เอเอสเอ็นโบรกเกอร์ จำกัด (มหาชน), (16 กรกฎาคม 2565).

Ref. code: 25646301033624ADV

ภาคผนวก

Ref. code: 25646301033624ADV

ภาคผนวก ก

General Data Protection Regulation (GDPR)

Chapter 1 General provisions

Ariticle 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.

Ariticle 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. 1For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. 2Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be

Ref. code: 25646301033624ADV

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.

Ariticle 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.

Ariticle 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;

Ref. code: 25646301033624ADV

(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) 1‘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.

Ref. code: 25646301033624ADV

2However, 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

Ref. code: 25646301033624ADV

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:

Ref. code: 25646301033624ADV

(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 (1);

(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.

Ref. code: 25646301033624ADV

Chapter 2 Principles

Ariticle 5 Principles relating to processing of personal data

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   (a) 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’);
   (b) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
   (c) 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’);
   (d) 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’);
2. 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’).

Ref. code: 25646301033624ADV

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Ariticle 6 Lawfulness of processing

1. 1Processing 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.

   2Point (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

Ref. code: 25646301033624ADV

processing including for other specific processing situations as provided for in Chapter IX.

3. 1The 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.

   2The 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. 3That 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. 4The 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;

Ref. code: 25646301033624ADV

(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.

Ariticle 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. 1If 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. 2Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. 1The data subject shall have the right to withdraw his or her consent at any time. 2The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 3Prior to giving consent, the data subject shall be informed thereof. 4It 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.

Ref. code: 25646301033624ADV

Ariticle 8 Conditions applicable to child's consent in relation to information society services

1. 1Where 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. 2Where 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.
2. 3Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
3. 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.
4. 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.

Ariticle 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

Ref. code: 25646301033624ADV

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

Ref. code: 25646301033624ADV

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.

Ariticle 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. 2Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Ref. code: 25646301033624ADV

Ariticle 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. 2In 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 3 Rights of the data subject

Section 1 Transparency and modalities

Ariticle 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. 2The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. 3When 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. 2In 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.

Ref. code: 25646301033624ADV

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. 2That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 3The 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. 4Where 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. 2Where 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

Ref. code: 25646301033624ADV

intended processing. 2Where 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

Ariticle 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:

Ref. code: 25646301033624ADV

(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.

Ariticle 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:

Ref. code: 25646301033624ADV

(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;

Ref. code: 25646301033624ADV

(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.

Ariticle 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.

Ref. code: 25646301033624ADV

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. 2For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. 3Where 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

Ariticle 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. 2Taking 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.

Ariticle 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.

Ref. code: 25646301033624ADV

Ariticle 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.

Ariticle 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.

Ref. code: 25646301033624ADV

Ariticle 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. 2That 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

Ariticle 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. 2The 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.

Ref. code: 25646301033624ADV

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.

Ariticle 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.

Ref. code: 25646301033624ADV

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

Ariticle 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 matters, public health and social security;
   (f) the protection of judicial independence and judicial proceedings;

Ref. code: 25646301033624ADV

(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 4 Controller and processor

Section 1 General obligations

Ariticle 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. 2Those measures shall be reviewed and updated where necessary.

Ref. code: 25646301033624ADV

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.

Ariticle 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. 2That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 3In 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.

Ref. code: 25646301033624ADV

Ariticle 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. 2They 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. 3The 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. 2The 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.

Ariticle 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.

Ref. code: 25646301033624ADV

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.

Ariticle 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

Ref. code: 25646301033624ADV

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

Ref. code: 25646301033624ADV

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. 2Where 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.

Ref. code: 25646301033624ADV

Ariticle 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.

Ariticle 30

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. 2That 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

Ref. code: 25646301033624ADV

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.

Ariticle 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

Ariticle 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

Ref. code: 25646301033624ADV

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.

Ariticle 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

Ref. code: 25646301033624ADV

rights and freedoms of natural persons. 2Where 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.

Ariticle 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).

Ref. code: 25646301033624ADV

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

Ariticle 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. 2A 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.

Ref. code: 25646301033624ADV

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. 2The 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. 2The 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;

Ref. code: 25646301033624ADV

(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.

Ariticle 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.

Ref. code: 25646301033624ADV

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. 2That period may be extended by six weeks, taking into account the complexity of the intended processing. 3The 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

Ref. code: 25646301033624ADV

controller in the public interest, including processing in relation to social protection and public health.

Section 4 Data protection officer

Ariticle 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 or 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. 2The 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.

Ref. code: 25646301033624ADV

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.

Ariticle 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. 2He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. 3The 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. 2The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Ariticle 39 Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

Ref. code: 25646301033624ADV

(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

Ariticle 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;

Ref. code: 25646301033624ADV

(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). 2Such 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. 2The 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. 2Those 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.

Ariticle 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 requirements 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

Ref. code: 25646301033624ADV

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. 2It 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 requirements 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.

Ariticle 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. 2The 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). 2Such 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.

Ref. code: 25646301033624ADV

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. 2Where 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 criteria continue to be met. 2Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria 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.

Ariticle 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

Ref. code: 25646301033624ADV

pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. 2Member 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[1] 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 requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. 2In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation

Ref. code: 25646301033624ADV

(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. 2The 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. 2The supervisory authorities shall also transmit those requirements and criteria to the Board.
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. 2Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Ref. code: 25646301033624ADV

Chapter 5 Transfers of personal data to third countries or international organisations

Ariticle 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. 2All 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.

Ariticle 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. 2Such 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

Ref. code: 25646301033624ADV

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. 2The 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. 3The 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. 4The 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

Ref. code: 25646301033624ADV

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. 2Those 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.

Ariticle 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.

Ref. code: 25646301033624ADV

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.

Ref. code: 25646301033624ADV

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. 2Decisions 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.

Ariticle 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;

Ref. code: 25646301033624ADV

(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

Ref. code: 25646301033624ADV

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. 2Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Ariticle 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.

Ref. code: 25646301033624ADV

Ariticle 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

Ref. code: 25646301033624ADV

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. 3The controller shall inform the supervisory authority of the transfer. 4The 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. 2Where 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. 2Member 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.

Ariticle50 International cooperation for the protection of personal data

Ref. code: 25646301033624ADV

1. 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 6 Independent supervisory authorities

Section 1 Independent status

Ariticle51 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. 2For 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

Ref. code: 25646301033624ADV

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.

Ariticle52 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.

Ref. code: 25646301033624ADV

Ariticle53 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.

Ariticle 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;

Ref. code: 25646301033624ADV

(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. 2During 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

Ariticle 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. 2In 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.

Ariticle56 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

Ref. code: 25646301033624ADV

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. 2Within 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. 2The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. 3The 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.

Ariticle57 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;

Ref. code: 25646301033624ADV

(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);

Ref. code: 25646301033624ADV

(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 requirements 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. 2The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Ariticle58 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;

Ref. code: 25646301033624ADV

(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);

Ref. code: 25646301033624ADV

(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. 2The exercise of those powers shall not impair the effective operation of Chapter VII.

Ariticle59 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.

Ref. code: 25646301033624ADV

Chapter 7 Cooperation and consistency

Section 1 Cooperation

Ariticle60 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. 2The 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. 2That 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

Ref. code: 25646301033624ADV

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

Ref. code: 25646301033624ADV

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.

Ariticle61 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. 2Mutual 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. 2Such 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. 2Information 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. 2The requested supervisory authority

Ref. code: 25646301033624ADV

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).

Ariticle62 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

Ref. code: 25646301033624ADV

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.

Ref. code: 25646301033624ADV

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. 2In 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

Ariticle63 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.

Ariticle64 Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. 2To 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 requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);
   (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

Ref. code: 25646301033624ADV

(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. 2That opinion shall be adopted within eight weeks by simple majority of the members of the Board. 3That period may be extended by a further six weeks, taking into account the complexity of the subject matter. 4Regarding 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.

Ref. code: 25646301033624ADV

6. The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.
7. The competent 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 competent supervisory authority referred to in paragraph 1 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.

Ariticle65 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 supervisory authority and the lead supervisory authority has not followed the objection or 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.

Ref. code: 25646301033624ADV

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. 2That period may be extended by a further month on account of the complexity of the subject-matter. 3The 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. 2Where 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. 2It shall inform the Commission thereof. 3The 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. 2The 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. 3The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). 4The 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

Ref. code: 25646301033624ADV

in accordance with paragraph 5 of this Article. 5The final decision shall attach the decision referred to in paragraph 1 of this Article.

Ariticle66 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. 2The 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.

Ref. code: 25646301033624ADV

Ariticle67 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

Ariticle68 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

Ref. code: 25646301033624ADV

to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Ariticle69 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 Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Ariticle70 Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. 2To 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;

Ref. code: 25646301033624ADV

(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;

(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);

Ref. code: 25646301033624ADV

(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) approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);

(p) approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;

(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;

Ref. code: 25646301033624ADV

(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.

Ariticle71 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. 2The 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.

Ariticle72 Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

Ref. code: 25646301033624ADV

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Ariticle73 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.

Ariticle74 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.

Ariticle75 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,

Ref. code: 25646301033624ADV

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.

Ariticle76 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.

Chapter 8 Remedies, liability and penalties

Ariticle77 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

Ref. code: 25646301033624ADV

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.

Ariticle78 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 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.

Ariticle79 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.

Ref. code: 25646301033624ADV

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.

Ariticle80 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.

Ariticle81 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.

Ref. code: 25646301033624ADV

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.

Ariticle82 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. [2]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.

Ref. code: 25646301033624ADV

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).

Ariticle83 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. [1]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). [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:
3. 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;
4. the intentional or negligent character of the infringement;
5. any action taken by the controller or processor to mitigate the damage suffered by data subjects;
6. 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;
7. any relevant previous infringements by the controller or processor;
8. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
9. the categories of personal data affected by the infringement;
10. 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;

Ref. code: 25646301033624ADV

11. 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;
12. adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
13. 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.
14. 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.
15. 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:
16. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
17. the obligations of the certification body pursuant to Articles 42 and 43;
18. the obligations of the monitoring body pursuant to Article 41(4).
19. 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:
20. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
21. the data subjects' rights pursuant to Articles 12 to 22;
22. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
23. any obligations pursuant to Member State law adopted under Chapter IX;

Ref. code: 25646301033624ADV

24. 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).
25. 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.
26. 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.
27. 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.
28. [1]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. [2]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.

Ariticle84 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

Ref. code: 25646301033624ADV

to ensure that they are implemented. [2]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 9 Provisions relating to specific processing situations

Ariticle85 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.

Ariticle86 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

Ref. code: 25646301033624ADV

access to official documents with the right to the protection of personal data pursuant to this Regulation.

Ariticle87 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.

Ariticle88 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.

Ref. code: 25646301033624ADV

Ariticle89 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. [4]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.

Ref. code: 25646301033624ADV

Ariticle90 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. [2]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.

Ariticle91 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 10 Delegated acts and implementing acts

Ariticle92 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.

Ref. code: 25646301033624ADV

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. 4It 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. 2That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Ariticle93 Committee procedure

1. The Commission shall be assisted by a committee. 2That 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.

Ref. code: 25646301033624ADV

Chapter 11 Final provisions

Ariticle94 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. 2References 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.

Ariticle95 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.

Ariticle96 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.

Ariticle97 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. 2The 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:

Ref. code: 25646301033624ADV

(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.

Ariticle98 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.

Ariticle99 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.

Ref. code: 25646301033624ADV

ภาคผนวก ข

Data Protection Act 2018

An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

[23rd May 2018]

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1 Preliminary

1 Overview

(1) This Act makes provision about the processing of personal data.

(2) Most processing of personal data is subject to the GDPR.

(3) Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter 3).

(4) Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.

(5) Part 4 makes provision about the processing of personal data by the intelligence services.

(6) Part 5 makes provision about the Information Commissioner.

(7) Part 6 makes provision about the enforcement of the data protection legislation.

(8) Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament.

Ref. code: 25646301033624ADV

2 Protection of personal data

(1) The GDPR, the applied GDPR and this Act protect individuals with regard to the processing of personal data, in particular by—

(a) requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis,

(b) conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and

(c) conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing their provisions.

(2) When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.

3 Terms relating to the processing of personal data

(1) This section defines some terms used in this Act.

(2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) an identifier such as a name, an identification number, location data or an online identifier, or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

(4) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as—

(a) collection, recording, organisation, structuring or storage,

(b) adaptation or alteration,

(c) retrieval, consultation or use,

Ref. code: 25646301033624ADV

(d) disclosure by transmission, dissemination or otherwise making available,

(e) alignment or combination, or

(f) restriction, erasure or destruction,

(subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3), which make provision about references to processing in the different Parts of this Act).

(5) "Data subject" means the identified or identifiable living individual to whom personal data relates.

(6) "Controller" and "processor", in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies, have the same meaning as in that Chapter or Part (see sections 5, 6, 32 and 83 and see also subsection (14)(d))

(7) "Filing system" means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

(8) "The Commissioner" means the Information Commissioner (see section 114).

(9) "The data protection legislation" means—

(a) the GDPR,

(b) the applied GDPR,

(c) this Act,

(d) regulations made under this Act, and

(e) regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

(10) "The GDPR" means 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 (General Data Protection Regulation).

(11) "The applied GDPR" means the GDPR as applied by Chapter 3 of Part 2.

(12) "The Law Enforcement Directive" means 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

Ref. code: 25646301033624ADV

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.

(13) "The Data Protection Convention" means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was opened for signature on 28 January 1981, as amended up to the day on which this Act is passed.

(14) In Parts 5 to 7, except where otherwise provided—

(a) references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2 ;

(b) references to Chapter 2 of Part 2, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part 2;

(c) references to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies;

(d) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.

(15) There is an index of defined expressions in section 206

PART 2

GENERAL PROCESSING

CHAPTER 1 SCOPE AND DEFINITIONS

4 Processing to which this Part applies

(1) This Part is relevant to most processing of personal data.

(2) Chapter 2 of this Part—

(a) applies to the types of processing of personal data to which the GDPR applies by virtue of Article 2 of the GDPR, and

(b) supplements, and must be read with, the GDPR.

(3) Chapter 3 of this Part—

(a) applies to certain types of processing of personal data to which the GDPR does not apply (see section 21), and

(b) makes provision for a regime broadly equivalent to the GDPR to apply to such processing.

5 Definitions

(1) Terms used in Chapter 2 of this Part and in the GDPR have the same meaning in Chapter 2 as they have in the GDPR.

(2) In subsection (1), the reference to a term's meaning in the GDPR is to its meaning inthe GDPR read with any provision of Chapter 2 which modifies the term's meaning for the purposes of the GDPR.

(3) Subsection (1) is subject to any provision in Chapter 2 which provides expressly for the term to have a different meaning and to section 204.

(4) Terms used in Chapter 3 of this Part and in the applied GDPR have the same meaning in Chapter 3 as they have in the applied GDPR.

(5) In subsection (4), the reference to a term's meaning in the applied GDPR is to its meaning in the GDPR read with any provision of Chapter 2 (as applied by Chapter 3) or Chapter 3 which modifiesthe term's meaning for the purposes of the applied GDPR.

(6) Subsection (4) is subject to any provision in Chapter 2 (as applied by Chapter 3) or Chapter 3 which provides expressly for the term to have a different meaning.

(7) A reference in Chapter 2 or Chapter 3 of this Part to the processing of personal data is to processing to which the Chapter applies.

(8) Sections 3 and 205 include definitions of other expressions used in this PAriticle

Ref. code: 25646301033624ADV

CHAPTER 2

THE GDPR

Meaning of certain terms used in the GDPR

6 Meaning of "controller"

(1) The definition of "controller" in Article 4(7) of the GDPR has effect subject to—

(a) subsection (2),

(b) section 209, and

(c) section 210.

(2) For the purposes of the GDPR, where personal data is processed only—

(a) for purposes for which it is required by an enactment to be processed, and

(b) by means by which it is required by an enactment to be processed,

the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

7 Meaning of "public authority" and "public body"

(1) For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom—

(a) a public authority as defined by the Freedom of Information Act 2000,

(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), and

(c) an authority or body specified or described by the Secretary of State in regulations, subject to subsections (2), (3) and (4).

(2) An authority or body that falls within subsection (1) is only a "public authority" or "public body" for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it.

(3) The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (asp 13) do not include any of the following that fall within those definitions—

(a) a parish council in England;

Ref. code: 25646301033624ADV

(b) a community council in Wales;

(c) a community council in Scotland;

(d) a parish meeting constituted under section 13 of the Local Government Act 1972;

(e) a community meeting constituted under section 27 of that Act;

(f) charter trustees constituted—

(i) under section 246 of that Act,

(ii) under Part 1 of the Local Government and Public Involvement in Health Act 2007, or

(iii) by the Charter Trustees Regulations 1996 (S.I. 1996/263)

(4) The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a "public authority" or "public body" for the purposes of the GDPR.

(5) Regulations under this section are subject to the affirmative resolution procedure

Lawfulness of processing

8 Lawfulness of processing: public interest etc

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for—

(a) the administration of justice,

(b) the exercise of a function of either House of Parliament,

(c) the exercise of a function conferred on a person by an enactment or rule of law,

(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or (e) an activity that supports or promotes democratic engagement.

Ref. code: 25646301033624ADV

9 Child's consent in relation to information society services

In Article 8(1) of the GDPR (conditions applicable to child's consent in relation to information society services)—

(a) references to "16 years" are to be read as references to "13 years", and

(b) the reference to "information society services" does not include preventive or counselling services

Special categories of personal data

10 Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health);

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

Ref. code: 25646301033624ADV

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

(i) by adding or varying conditions or safeguards, and

(ii) by omitting conditions or safeguards added by regulations under this section, and

(b) consequentially amend this section.

(7) Regulations under this section are subject to the affirmative resolution procedure.

11 Special categories of personal data etc: supplementary

(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the responsibility of a health professional or a social work professional, or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—

(a) the alleged commission of offences by the data subject, or

(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Rights of the data subject

12 Limits on fees that may be charged by controllers

(1) The Secretary of State may by regulations specify limits on the fees that a controller may charge in reliance on—

(a) Article 12(5) of the GDPR (reasonable fees when responding to manifestly unfounded or excessive requests), or

Ref. code: 25646301033624ADV

(b) Article 15(3) of the GDPR (reasonable fees for provision of further copies).

(2) The Secretary of State may by regulations—

(a) require controllers of a description specified in the regulations to produce and publish guidance about the fees that they charge in reliance on those provisions, and

(b) specify what the guidance must include.

(3) Regulations under this section are subject to the negative resolution procedure.

13 Obligations of credit reference agencies

(1) This section applies where a controller is a credit reference agency (within the meaning of section 145(8) of the Consumer Credit Act 1974).

(2) The controller's obligations under Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) are taken to apply only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention.

(3) Where the controller discloses personal data in pursuance of Article 15(1) to (3) of the GDPR, the disclosure must be accompanied by a statement informing the data subject of the data subject's rights under section 159 of the Consumer Credit Act 1974 (correction of wrong information).

14 Automated decision-making authorised by law: safeguards

(1) This section makes provision for the purposes of Article 22(2)(b) of the GDPR (exception from Article 22(1) of the GDPR for significant decisions based solely on automated processing that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests).

(2) A decision is a "significant decision" for the purposes of this section if, in relation to a data subject, it—

(a) produces legal effects concerning the data subject, or

(b) similarly significantly affects the data subject.

Ref. code: 25646301033624ADV

(3) A decision is a "qualifying significant decision" for the purposes of this section if—

(a) it is a significant decision in relation to a data subject,

(b) it is required or authorised by law, and

(c) it does not fall within Article 22(2)(a) or (c) of the GDPR (decisions necessary to a contract or made with the data subject's consent).

(4) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—

(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and

(b) the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

(ii) take a new decision that is not based solely on automated processing.

(5) If a request is made to a controller under subsection (4), the controller must, within the period described in Article 12(3) of the GDPR—

(a) consider the request, including any information provided by the data subject that is relevant to it,

(b) comply with the request, and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request, and

(ii) the outcome of complying with the request.

(6) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that apply in connection with Article 22 of the GDPR.

(7) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard

Ref. code: 25646301033624ADV

a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

(8) Regulations under subsection (7)—

(a) may amend this section, and

(b) are subject to the affirmative resolution procedure.

Restrictions on data subject's rights

15 Exemptions etc

(1) Schedules 2, 3 and 4 make provision for exemptions from, and restrictions and adaptations of the application of, rules of the GDPR.

(2) In Schedule 2—

(a) Part 1 makes provision adapting or restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 6(3) and Article 23(1) of the GDPR;

(b) Part 2 makes provision restricting the application of rules contained in Articles 13 to 21 and 34 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(c) Part 3 makes provision restricting the application of Article 15 of the GDPR where this is necessary to protect the rights of others, as allowed for by Article 23(1) of the GDPR;

(d) Part 4 makes provision restricting the application of rules contained in Articles 13 to 15 of the GDPR in specified circumstances, as allowed for by Article 23(1) of the GDPR;

(e) Part 5 makes provision containing exemptions or derogations from Chapters II, III, IV, V and VII of the GDPR for reasons relating to freedom of expression, as allowed for by Article 85(2) of the GDPR;

(f) Part 6 makes provision containing derogations from rights contained in Articles 15, 16, 18, 19, 20 and 21 of the GDPR for scientific or historical research purposes, statistical purposes and archiving purposes, as allowed for by Article 89(2) and (3) of the GDPR.

Ref. code: 25646301033624ADV

(3) Schedule 3 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to health, social work, education and child abuse data, as allowed for by Article 23(1) of the GDPR.

(4) Schedule 4 makes provision restricting the application of rules contained in Articles 13 to 21 of the GDPR to information the disclosure of which is prohibited or restricted by an enactment, as allowed for by Article 23(1) of the GDPR.

16 Power to make further exemptions etc by regulations

(1) The following powers to make provision altering the application of the GDPR may be exercised by way of regulations made by the Secretary of State under this section—

(a) the power in Article 6(3) for Member State law to lay down a legal basis containing specific provisions to adapt the application of rules of the GDPR where processing is necessary for compliance with a legal obligation, for the performance of a task in the public interest or in the exercise of official authority;

(b) the power in Article 23(1) to make a legislative measure restricting the scope of the obligations and rights mentioned in that Article where necessary and proportionate to safeguard certain objectives of general public interest;

(c) the power in Article 85(2) to provide for exemptions or derogations from certain Chapters of the GDPR where necessary to reconcile the protection of personal data with the freedom of expression and information.

(2) Regulations under this section may—

(a) amend Schedules 2 to 4—

(i) by adding or varying provisions, and

(ii) by omitting provisions added by regulations under this section, and

(b) consequentially amend section 15.

(3) Regulations under this section are subject to the affirmative resolution procedure.

Ref. code: 25646301033624ADV

Accreditation of certification providers

17 Accreditation of certification providers

(1) Accreditation of a person as a certification provider is only valid when carried out by—

(a) the Commissioner, or

(b) the national accreditation body.

(2) The Commissioner may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the Commissioner will carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(3) The national accreditation body may only accredit a person as a certification provider where the Commissioner—

(a) has published a statement that the body may carry out such accreditation, and

(b) has not published a notice withdrawing that statement.

(4) The publication of a notice undersubsection (2)(b) or (3)(b) does not affect the validity of any accreditation carried out before its publication.

(5) Schedule 5 makes provision about reviews of, and appeals from, a decision relating to accreditation of a person as a certification provider.

(6) The national accreditation body may charge a reasonable fee in connection with, or incidental to, the carrying out of the body's functions under this section, Schedule 5 and Article 43 of the GDPR.

(7) The national accreditation body must provide the Secretary of State with such information relating to its functions under this section, Schedule 5 and Article 43 of the GDPR as the Secretary of State may reasonably require.

(8) In this section—

"certification provider" means a person who issues certification for the purposes of Article 42 of the GDPR;

"the national accreditation body" means the national accreditation body for

Ref. code: 25646301033624ADV

the purposes of Article 4(1) of 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.

Transfers of personal data to third countries etc

18 Transfers of personal data to third countries etc

(1) The Secretary of State may by regulations specify, for the purposes of Article 49(1) (d) of the GDPR—

(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and

(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest.

(2) The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where—

(a) the transfer is not authorised by an adequacy decision under Article 45(3) of the GDPR, and

(b) the Secretary of State considers the restriction to be necessary for important reasons of public interest.

(3) Regulations under this section—

(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;

(b) are otherwise subject to the affirmative resolution procedure.

(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay.

Ref. code: 25646301033624ADV

Specific processing situations

19 Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

(a) processing of personal data that is necessary for archiving purposes in the public interest,

(b) processing of personal data that is necessary for scientific or historical research purposes, and

(c) processing of personal data that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(4) In this section—

"approved medical research" means medical research carried out by a person who has approval to carry out that research from—

(a) a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or

(b) a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—

(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;

(ii) a relevant NHS body;

(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;

Ref. code: 25646301033624ADV

(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);

"relevant NHS body" means—

(a) an NHS trust or NHS foundation trust in England,

(b) an NHS trust or Local Health Board in Wales,

(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,

(d) the Common Services Agency for the Scottish Health Service, or

(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).

(5) The Secretary of State may by regulations change the meaning of "approved medical research" for the purposes of this section, including by amending subsection (4).

(6) Regulations under subsection (5) are subject to the affirmative resolution procedure

Minor definition

20 Meaning of "court"

Section 5(1) (terms used in this Chapter to have the same meaning as in the GDPR) does not apply to referencesin this Chapter to a court and, accordingly, such references do not include a tribunal.

CHAPTER 3

OTHER GENERAL PROCESSING

Scope

21 Processing to which this Chapter applies

(1) This Chapter applies to the automated or structured processing of personal data in the course of—

(a) an activity which is outside the scope of European Union law, or

(b) an activity which falls within the scope of Article 2(2)(b) of the GDPR (common foreign and security policy activities), provided that the processing is not processing by a competent authority for any of the law enforcement purposes (as defined in Part 3) or processing to which Part 4 (intelligence services processing) applies.

(2) This Chapter also applies to the manual unstructured processing of personal data held by an FOI public authority.

(3) This Chapter does not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(4) In this section—

"the automated or structured processing of personal data" means—

(a) the processing of personal data wholly or partly by automated means, and

(b) the processing otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system;

" the manual unstructured processing of personal data" means the processing of personal data which is not the automated or structured processing of personal data.

(5) In this Chapter, "FOI public authority" means—

(a) a public authority as defined in the Freedom of Information Act 2000, or

(b) a Scottish public authority as defined in the Freedom of Information (Scotland) Act 2002 (asp 13).

(6) References in this Chapter to personal data "held" by an FOI public authority are to be interpreted—

(a) in relation to England and Wales and Northern Ireland, in accordance with section 3(2) of the Freedom of Information Act 2000, and

(b) in relation to Scotland, in accordance with section 3(2), (4) and (5) of the Freedom of Information (Scotland) Act 2002 (asp 13), but such references do not include information held by an intelligence service (as defined in section 82) on behalf of an FOI public authority.

(7) But personal data is not to be treated as "held" by an FOI public authority for the purposes of this Chapter, where—

Ref. code: 25646301033624ADV

(a) section 7 of the Freedom of Information Act 2000 prevents Parts 1 to 5 of that Act from applying to the personal data, or

(b) section 7(1) of the Freedom of Information (Scotland) Act 2002 (asp 13) prevents that Act from applying to the personal data

Application of the GDPR

22 Application of the GDPR to processing to which this Chapter applies

(1) The GDPR applies to the processing of personal data to which this Chapter applies but as if its Articles were part of an Act extending to England and Wales, Scotland and Northern Ireland.

(2) Chapter 2 of this Part applies for the purposes of the applied GDPR as it applies for the purposes of the GDPR.

(3) In this Chapter, "the applied Chapter 2 " means Chapter 2 of this Part as applied by this Chapter.

(4) Schedule 6 contains provision modifying—

(a) the GDPR as it applies by virtue of subsection (1) (see Part 1);

(b) Chapter 2 of this Part as it applies by virtue of subsection (2) (see Part 2).

(5) A question as to the meaning or effect of a provision of the applied GDPR, or the applied Chapter 2 , is to be determined consistently with the interpretation of the equivalent provision of the GDPR, or Chapter 2 of this Part, as it applies otherwise than by virtue of this Chapter, exceptso far as Schedule 6 requires a different interpretation.

23 Power to make provision in consequence of regulations related to the GDPR

(1) The Secretary of State may by regulations make provision in connection with the processing of personal data to which this Chapter applies which is equivalent to that made by GDPR regulations, subject to such modifications as the Secretary of State considers appropriate.

(2) In this section, "GDPR regulations" means regulations made under section 2(2) of the European Communities Act 1972 which make provision relating to the GDPR.

Ref. code: 25646301033624ADV

(3) Regulations under subsection (1) may apply a provision of GDPR regulations, with or without modification.

(4) Regulations under subsection (1) may amend or repeal a provision of—

(a) the applied GDPR;

(b) this Chapter;

(c) Parts 5 to 7, in so far as they apply in relation to the applied GDPR.

(5) Regulations under this section are subject to the affirmative resolution procedure.

Exemptions etc

24 Manual unstructured data held by FOI public authorities

(1) The provisions of the applied GDPR and this Act listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities).

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles)—

(i) Article 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle),

(ii) Article 6 (lawfulness),

(iii) Article 7 (conditions for consent),

(iv) Article 8(1) and (2) (child's consent),

(v) Article 9 (processing of special categories of personal data),

(vi) Article 10 (data relating to criminal convictions etc), and

(vii) Article 11(2) (processing not requiring identification);

(b) in Chapter III of the applied GDPR (rights of the data subject)—

(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(iii) Article 20 (right to data portability), and

Ref. code: 25646301033624ADV

(iv) Article 21(1) (objections to processing);

(c) in Chapter V of the applied GDPR, Articles 44 to 49 (transfers of personal data to third countries or international organisations);

(d) sections 170 and 171 of this Act; (see also paragraph 1(2) of Schedule 18).

(3) In addition, the provisions of the applied GDPR listed in subsection (4) do not apply to personal data to which this Chapter applies by virtue of section 21(2) where the personal data relates to appointments, removals, pay, discipline, superannuation or other personnel matters in relation to—

(a) service in any of the armed forces of the Crown;

(b) service in any office or employment under the Crown or under any public authority;

(c) service in any office or employment, or under any contract for services, in respect of which power to take action, or to determine or approve the action taken, in such matters is vested in—

(i) Her Majesty,

(ii) a Minister of the Crown,

(iii) the National Assembly for Wales,

(iv) the Welsh Ministers,

(v) a Northern Ireland Minister (within the meaning of the Freedom of Information Act 2000), or

(vi) an FOI public authority.

(4) Those provisions are—

(a) the remaining provisions of Chapters II and III (principles and rights of the data subject);

(b) Chapter IV (controller and processor);

(c) Chapter IX (specific processing situations).

(5) A controller is not obliged to comply with Article 15(1) to (3) of the applied GDPR (right of access by the data subject) in relation to personal data to which this Chapter applies by virtue of section 21(2) if—

Ref. code: 25646301033624ADV

(a) the request under that Article does not contain a description of the personal data, or

(b) the controller estimates that the cost of complying with the request so far as relating to the personal data would exceed the appropriate maximum.

(6) Subsection (5)(b) does not remove the controller's obligation to confirm whether or not personal data concerning the data subject is being processed unless the estimated cost of complying with that obligation alone in relation to the personal data would exceed the appropriate maximum.

(7) An estimate for the purposes of this section must be made in accordance with regulations under section 12(5) of the Freedom of Information Act 2000.

(8) In subsections (5) and (6), "the appropriate maximum" means the maximum amount specified by the Secretary of State by regulations.

(9) Regulations under subsection (8) are subject to the negative resolution procedure

25 Manual unstructured data used in longstanding historical research

(1) The provisions of the applied GDPR listed in subsection (2) do not apply to personal data to which this Chapter applies by virtue of section 21(2) (manual unstructured personal data held by FOI public authorities) at any time when—

(a) the personal data—

(i) is subject to processing which was already underway immediately before 24 October 1998, and

(ii) is processed only for the purposes of historical research, and

(b) the processing is not carried out—

(i) for the purposes of measures or decisions with respect to a particular data subject, or

(ii) in a way that causes, or is likely to cause, substantial damage or substantial distress to a data subject.

(2) Those provisions are—

(a) in Chapter II of the applied GDPR (principles), Article 5(1)(d) (the accuracy principle), and

(b) in Chapter III of the applied GDPR (rights of the data subject)—

(i) Article 16 (right to rectification), and

(ii) Article 17(1) and (2) (right to erasure).

(3) The exemptions in this section apply in addition to the exemptions in section 24.

26 National security and defence exemption

(1) A provision of the applied GDPR or this Act mentioned in subsection (2) does not apply to personal data to which this Chapter applies if exemption from the provision is required for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(2) The provisions are—

(a) Chapter II of the applied GDPR (principles) except for—

(i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful;

(ii) Article 6 (lawfulness of processing);

(iii) Article 9 (processing of special categories of personal data);

(b) Chapter III of the applied GDPR (rights of data subjects);

(c) in Chapter IV of the applied GDPR—

(i) Article 33 (notification of personal data breach to the Commissioner);

(ii) Article 34 (communication of personal data breach to the data subject);

(d) Chapter V of the applied GDPR (transfers of personal data to third countries or international organisations);

(e) in Chapter VI of the applied GDPR—

(i) Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations);

(ii) Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);

Ref. code: 25646301033624ADV

(f) Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for—

(i) Article 83 (general conditions for imposing administrative fines);

(ii) Article 84 (penalties);

(g) in Part 5 of this Act—

(i) in section 115 (general functions of the Commissioner), subsections (3) and (8);

(ii) in section 115, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR;

(iii) section 119 (inspection in accordance with international obligations);

(h) in Part 6 of this Act—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

(ii) sections 170 to 173 (offences relating to personal data); (i) in Part 7 of this Act, section 187 (representation of data subjects).

27 National security: certificate

(1) Subject to subsection (3), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions listed in section 26(2) is, or at any time was, required in relation to any personal data for the purpose of safeguarding national security is conclusive evidence of that fact

(2) A certificate under subsection (1)—

(a) may identify the personal data to which it applies by means of a general description, and

(b) may be expressed to have prospective effect.

(3) Any person directly affected by a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(4) If, on an appeal under subsection (3), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing a certificate, the Tribunal may—

Ref. code: 25646301033624ADV

(a) allow the appeal, and

(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of the applied GDPR or this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under subsection (1) is to be—

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

(9) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—

(a) in any legal proceedings, evidence of that certificate;

(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or

(b) the Attorney General or the Advocate General for Scotland.

28 National security and defence: modifications to Articles 9 and 32 of the applied GDPR

(1) Article 9(1) of the applied GDPR (prohibition on processing of special categories of personal data) does not prohibit the processing of personal data to which this Chapter applies to the extent that the processing is carried out—

Ref. code: 25646301033624ADV

(a) for the purpose of safeguarding national security or for defence purposes, and

(b) with appropriate safeguards for the rights and freedoms of data subjects.

(2) Article 32 of the applied GDPR (security of processing) does not apply to a controller or processor to the extent that the controller or the processor (as the case may be) is processing personal data to which this Chapter applies for—

(a) the purpose of safeguarding national security, or

(b) defence purposes.

(3) Where Article 32 of the applied GDPR does not apply, the controller or the processor must implement security measures appropriate to the risks arising from the processing of the personal data.

(4) For the purposes of subsection (3), where the processing of personal data is carried out wholly or partly by automated means, the controller or the processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with the processing,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

PART 3

LAW ENFORCEMENT PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

29 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by a competent authority of personal data wholly or partly by automated means, and

(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies.

(3) For the meaning of "competent authority", see section 30.

Definitions

30 Meaning of "competent authority"

(1) In this Part, "competent authority" means—

(a) a person specified or described in Schedule 7, and

(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

(2) But an intelligence service is not a competent authority within the meaning of this PAriticle

(3) The Secretary of State may by regulations amend Schedule 7—

(a) so as to add or remove a person or description of person;

(b) so as to reflect any change in the name of a person specified in the Schedule.

(4) Regulations under subsection (3) which make provision of the kind described in subsection (3)(a) may also make consequential amendments of section 73(4)(b).

(5) Regulations under subsection (3) which make provision of the kind described in subsection (3)(a), or which make provision of that kind and of the kind described in subsection (3)(b), are subject to the affirmative resolution procedure.

(6) Regulations under subsection (3) which make provision only of the kind described in subsection (3)(b) are subject to the negative resolution procedure.

(7) In this section—

"intelligence service" means—

Ref. code: 25646301033624ADV

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters;

"statutory function" means a function under or by virtue of an enactment.

31 "The law enforcement purposes"

For the purposes of this Part, "the law enforcement purposes" are 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.

32 Meaning of "controller" and "processor"

(1) In this Part, "controller" means the competent authority which, alone or jointly with others—

(a) determines the purposes and means of the processing of personal data, or

(b) is the controller by virtue of subsection (2).

(2) Where personal data is processed only—

(a) for purposes for which it is required by an enactment to be processed, and

(b) by means by which it is required by an enactment to be processed,

the competent authority on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

(3) In this Part, "processor" means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

33 Other definitions

(1) This section defines certain other expressions used in this PAriticle

(2) "Employee", in relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.

Ref. code: 25646301033624ADV

(3) “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.

(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 an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(5) “ Recipient”, in relation to any personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

(6) “Restriction of processing” means the marking of stored personal data with the aim of limiting its processing for the future.

(7) “Third country” means a country or territory other than a member State.

(8) Sections 3 and 205 include definitions of other expressions used in this Ariticle

CHAPTER 2

PRINCIPLES

34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

Ref. code: 25646301033624ADV

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

35 The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

Ref. code: 25646301033624ADV

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(6) The Secretary of State may by regulations amend Schedule 8—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8) In this section, "sensitive processing" means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual'ssex life orsexual orientation.

36 The second data protection principle

(1) The second data protection principle is that—

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—

Ref. code: 25646301033624ADV

(a) the controller is authorised by law to process the data for the other purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorized by law.

37 The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to theอpurpose for which it is processed.

38 The fourth data protection principle

(1) The fourth data protection principle is that—

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—

(a) persons suspected of having committed or being about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) persons who are or may be victims of a criminal offence;

(d) witnesses or other persons with information about offences.

Ref. code: 25646301033624ADV

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose—

(a) the quality of personal data must be verified before it is transmitted or made available,

(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

39 The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

40 The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage).

41 Safeguards: archiving

Ref. code: 25646301033624ADV

(1) This section applies in relation to the processing of personal data for a law enforcement purpose where the processing is necessary—

(a) for archiving purposes in the public interest,

(b) for scientific or historical research purposes, or

(c) for statistical purposes.

(2) The processing is not permitted if—

(a) it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject, or

(b) it is likely to cause substantial damage or substantial distress to a data subject.

42 Safeguards: sensitive processing

(1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8).

(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which—

(a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained

(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period—

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, and

Ref. code: 25646301033624ADV

(c) make it available to the Commissioner, on request, without charge.

(4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—

(a) whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, which condition in Schedule 8 is relied on,

(b) how the processing satisfies section 35 (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5) In this section, "relevant period", in relation to sensitive processing in reliance on the consent of the data subject or in reliance on a condition specified in Schedule 8, means a period which—

(a) begins when the controller starts to carry out the sensitive processing in reliance on the data subject's consent or (as the case may be) in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview and scope

43 Overview and scope

(1) This Chapter—

(a) imposes general duties on the controller to make information available (see section 44);

(b) confers a right of access by the data subject (see section 45);

Ref. code: 25646301033624ADV

(c) confers rights on the data subject with respect to the rectification of personal data and the erasure of personal data or the restriction of its processing (see sections 46 to 48);

(d) regulates automated decision-making (see sections 49 and 50);

(e) makes supplementary provision (see sections 51 to 54).

(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.

(3) But sections 44 to 48 do not apply in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty.

(4) In subsection (3), "relevant personal data" means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

(5) In this Chapter, "the controller", in relation to a data subject, means the controller in relation to personal data relating to the data subject.

Information: controller's general duties

44 Information: controller's general duties

(1) The controller must make available to data subjects the following information (whether by making the information generally available to the public or in any other way)—

(a) the identity and the contact details of the controller;

(b) where applicable, the contact details of the data protection officer (see sections 69 to 71);

(c) the purposes for which the controller processes personal data;

(d) the existence of the rights of data subjects to request from the controller—

(i) access to personal data (see section 45),

(ii) rectification of personal data (see section 46), and

(iii) erasure of personal data or the restriction of its processing (see section 47);

Ref. code: 25646301033624ADV

(e) the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.

(2) The controller must also, in specific cases for the purpose of enabling the exercise of a data subject's rights under this Part, give the data subject the following—

(a) information about the legal basis for the processing;

(b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;

(c) where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations);

(d) such further information as is necessary to enable the exercise of the data subject's rights under this PAriticle

(3) An example of where further information may be necessary as mentioned in subsection (2)(d) is where the personal data being processed was collected without the knowledge of the data subject.

(4) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (2) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(5) Where the provision of information to a data subject under subsection (2) is restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the provision of information has been restricted,

Ref. code: 25646301033624ADV

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 51,

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that complying with them would undermine the purpose of the restriction.

(7) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (2), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

Data subject's right of access

45 Right of access by the data subject

(1) A data subject is entitled to obtain from the controller—

(a) confirmation as to whether or not personal data concerning him or her is being processed, and

(b) where that is the case, access to the personal data and the information set out in subsection (2).

(2) That information is—

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);

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

(e) the existence of the data subject's rights to request from the controller—

(i) rectification of personal data (see section 46), and

Ref. code: 25646301033624ADV

(ii) erasure of personal data or the restriction of its processing (see section 47);

(f) the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) communication of the personal data undergoing processing and of any available information as to its origin.

(3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing —

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (as to which see section 54).

(4) The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 51,

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the

Ref. code: 25646301033624ADV

information would undermine the purpose of the restriction.

(7) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

Data subject's rights to rectification or erasure etc

46 Right to rectification

(1) The controller must, if so requested by a data subject, rectify without undue delay inaccurate personal data relating to the data subject.

(2) Where personal data is inaccurate because it is incomplete, the controller must, if so requested by a data subject, complete it.

(3) The duty under subsection (2) may, in appropriate cases, be fulfilled by the provision of a supplementary statement.

(4) Where the controller would be required to rectify personal data under this section but the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing.

47 Right to erasure or restriction of processing

(1) The controller must erase personal data without undue delay where—

(a) the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or

(b) the controller has a legal obligation to erase the data.

(2) Where the controller would be required to erase personal data under subsection (1) but the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.

(3) Where a data subject contests the accuracy of personal data (whether in making a request under this section or section 46 or in any other way), but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.

Ref. code: 25646301033624ADV

(4) A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller under this section apply whether or not such a request is made).

48 Rights under section 46 or 47: supplementary

(1) Where a data subject requests the rectification or erasure of personal data or the restriction of its processing, the controller must inform the data subject in writing—

(a) whether the request has been granted, and

(b) if it has been refused—

(i) of the reasons for the refusal,

(ii) of the data subject's right to make a request to the Commissioner under section 51,

(iii) of the data subject's right to lodge a complaint with the Commissioner, and

(iv) of the data subject's right to apply to a court under section 167.

(2) The controller must comply with the duty under subsection (1)—

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (see section 54).

(3) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1)(b)(i) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

Ref. code: 25646301033624ADV

(4) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to lodge a complaint with the Commissioner, and

(d) of the data subject's right to apply to a court under section 167.

(5) Subsection (4)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

(6) The controller must—

(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (1)(b)(i), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

(7) Where the controller rectifies personal data, it must notify the competent authority (if any) from which the inaccurate personal data originated.

(8) In subsection (7), the reference to a competent authority includes (in addition to a competent authority within the meaning of this Part) any person that is a competent authority for the purposes of the Law Enforcement Directive in a member State other than the United Kingdom.

(9) Where the controller rectifies, erases or restricts the processing of personal data which has been disclosed by the controller—

(a) the controller must notify the recipients, and

(b) the recipients must similarly rectify, erase or restrict the processing of the personal data (so far as they retain responsibility for it).

(10) Where processing is restricted in accordance with section 47(3), the controller must inform the data subject before lifting the restriction

Automated individual decision-making

49 Right not to be subject to automated decision-making

(1) A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.

(2) A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it—

(a) produces an adverse legal effect concerning the data subject, or

(b) significantly affects the data subject.

50 Automated decision-making authorised by law: safeguards

(1) A decision is a "qualifying significant decision" for the purposes of this section if—

(a) it is a significant decision in relation to a data subject, and

(b) it is required or authorised by law.

(2) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—

(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and

(b) the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to—

(i) reconsider the decision, or

(ii) take a new decision that is not based solely on automated processing.

(3) If a request is made to a controller under subsection (2), the controller must, before the end of the period of 1 month beginning with receipt of the request—

(a) consider the request, including any information provided by the data subject that is relevant to it,

(b) comply with the request, and

(c) by notice in writing inform the data subject of—

Ref. code: 25646301033624ADV

(i) the steps taken to comply with the request, and

(ii) the outcome of complying with the request.

(4) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

(5) Regulations under subsection (4)—

(a) may amend this section, and

(b) are subject to the affirmative resolution procedure.

(6) In this section "significant decision" has the meaning given by section 49(2).

Supplementary

51 Exercise of rights through the Commissioner

(1) This section applies where a controller—

(a) restricts under section 44(4) the information provided to the data subject under section 44(2) (duty of the controller to give the data subject additional information),

(b) restricts undersection 45(4) the data subject'srights undersection 45(1) (right of access), or

(c) refuses a request by the data subject for rectification under section 46 or for erasure or restriction of processing under section 47.

(2) The data subject may—

(a) where subsection (1)(a) or (b) applies, request the Commissioner to check that the restriction imposed by the controller was lawful;

(b) where subsection (1)(c) applies, request the Commissioner to check that the refusal of the data subject's request was lawful.

(3) The Commissioner must take such steps as appear to the Commissioner to be appropriate to respond to a request under subsection (2) (which may include the exercise of any of the powers conferred by sections 142 and 146).

(4) After taking those steps, the Commissioner must inform the data subject—

Ref. code: 25646301033624ADV

(a) where subsection (1)(a) or (b) applies, whether the Commissioner is satisfied that the restriction imposed by the controller was lawful;

(b) where subsection (1)(c) applies, whether the Commissioner is satisfied that the controller's refusal of the data subject's request was lawful.

(5) The Commissioner must also inform the data subject of the data subject's right to apply to a court under section 167.

(6) Where the Commissioner is not satisfied as mentioned in subsection (4)(a) or (b), the Commissioner may also inform the data subject of any further steps that the Commissioner is considering taking under Part 6 .

52 Form of provision of information etc

(1) The controller must take reasonable steps to ensure that any information that is required by this Chapter to be provided to the data subject is provided in a concise, intelligible and easily accessible form, using clear and plain language.

(2) Subject to subsection (3), the information may be provided in any form, including electronic form.

(3) Where information is provided in response to a request by the data subject under section 45, 46, 47 or 50, the controller must provide the information in the same form as the request where it is practicable to do so.

(4) Where the controller has reasonable doubts about the identity of an individual making a request under section 45, 46 or 47, the controller may—

(a) request the provision of additional information to enable the controller to confirm the identity, and

(b) delay dealing with the request until the identity is confirmed.

(5) Subject to section 53, any information that is required by this Chapter to be provided to the data subject must be provided free of charge.

(6) The controller must facilitate the exercise of the rights of the data subject under sections 45 to 50.

Ref. code: 25646301033624ADV

53 Manifestly unfounded or excessive requests by the data subject

(1) Where a request from a data subject under section 45, 46, 47 or 50 is manifestlyunfounded or excessive, the controller may—

(a) charge a reasonable fee for dealing with the request, or

(b) refuse to act on the request.

(2) An example of a request that may be excessive is one that merely repeats the substance of previous requests.

(3) In any proceedings where there is an issue as to whether a request under section 45, 46, 47 or 50 is manifestly unfounded or excessive, it is for the controller to show that it is.

(4) The Secretary of State may by regulations specify limits on the fees that a controller may charge in accordance with subsection (1)(a).

(5) Regulations under subsection (4) are subject to the negative resolution procedure.

54 Meaning of "applicable time period"

(1) This section defines "the applicable time period" for the purposes of sections 45(3) (b) and 48(2)(b)

(2) "The applicable time period" means the period of 1 month, or such longer period as may be specified in regulations, beginning with the relevant time.

(3) "The relevant time" means the latest of the following—

(a) when the controller receives the request in question;

(b) when the controller receives the information (if any) requested in connection with a request under section 52(4);

(c) when the fee (if any) charged in connection with the request under section 53 is paid.

(4) The power to make regulations under subsection (2) is exercisable by the Secretary of State.

(5) Regulations under subsection (2) may not specify a period which is longer than 3

Ref. code: 25646301033624ADV

months.

(6) Regulations under subsection (2) are subject to the negative resolution procedure.

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview and scope

55 Overview and scope

(1) This Chapter—

(a) sets out the general obligations of controllers and processors (see sections 56 to 65);

(b) sets out specific obligations of controllers and processors with respect to security (see section 66);

(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 67 and 68);

(d) makes provision for the designation, position and tasks of data protection officers (see sections 69 to 71).

(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.

(3) Where a controller is required by any provision of this Chapter to implement appropriate technical and organisational measures, the controller must (in deciding what measures are appropriate) take into account—

(a) the latest developments in technology,

(b) the cost of implementation,

(c) the nature, scope, context and purposes of processing, and

(d) the risks for the rights and freedoms of individuals arising from the processing.

Ref. code: 25646301033624ADV

General obligations

56 General obligations of the controller

(1) Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this PAriticle

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Data protection by design and default

(1) Each controller must implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner, and

(b) to integrate into the processing itself the safeguards necessary for that purpose.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.

(3) Each controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

(4) The duty under subsection (3) applies to—

(a) the amount of personal data collected,

(b) the extent of its processing,

(c) the period of its storage, and

(d) its accessibility.

(5) In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

Ref. code: 25646301033624ADV

58 Joint controllers

(1) Where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this PAriticle

(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.

(3) The arrangement must designate the controller which is to be the contact point for data subjects.

59 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.

(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—

(a) meet the requirements of this Part, and

(b) ensure the protection of the rights of the data subject.

(3) The processor used by the controller may not engage another processor ("a sub-processor") without the prior written authorisation of the controller, which may be specific or general.

(4) Where the controller gives a general written authorisation to a processor, the processor must inform the controller if the processor proposes to add to the number of sub-processors engaged by it or to replace any of them (so that the controller has the opportunity to object to the proposal).

(5) The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—

(a) the subject-matter and duration of the processing;

Ref. code: 25646301033624ADV

(b) the nature and purpose of the processing;

(c) the type of personal data and categories of data subjects involved;

(d) the obligations and rights of the controller and processor.

(6) The contract must, in particular, provide that the processor must—

(a) act only on instructions from the controller,

(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,

(c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part,

(d) at the end of the provision of services by the processor to the controller—

(i) either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and

(ii) delete copies of the personal data unless subject to a legal obligation to store the copies,

(e) make available to the controller all information necessary to demonstrate compliance with this section, and

(f) comply with the requirements of this section for engaging sub-processors.

(7) The terms included in the contract in accordance with subsection (6)(a) must provide that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to make the particular transfer.

(8) If a processor determines, in breach of this Part, the purposes and means of processing, the processor is to be treated for the purposes of this Part as a controller in respect of that processing.

60 Processing under the authority of the controller or processor

A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—

(a) on instructions from the controller, or

(b) to comply with a legal obligation.

Ref. code: 25646301033624ADV

61 Records of processing activities

(1) Each controller must maintain a record of all categories of processing activities for which the controller is responsible.

(2) The controller's record must contain the following information—

(a) the name and contact details of the controller;

(b) where applicable, the name and contact details of the joint controller;

(c) where applicable, the name and contact details of the data protection officer;

(d) the purposes of the processing;

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

(f) a description of the categories of—

(i) data subject, and

(ii) personal data;

(g) where applicable, details of the use of profiling;

(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;

(j) where possible, the envisaged time limitsfor erasure of the different categories of personal data;

(k) where possible, a general description of the technical and organisational security measures referred to in section 66.

(3) Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller.

(4) The processor's record must contain the following information—

(a) the name and contact details of the processor and of any other processors engaged by the processor in accordance with section 59(3);

(b) the name and contact details of the controller on behalf of which the processor is acting;

(c) where applicable, the name and contact details of the data protection officer;

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

(e) where applicable, details of transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(f) where possible, a general description of the technical and organisational security measures referred to in section 66.

(5) The controller and the processor must make the records kept under this section available to the Commissioner on request.

62 Logging

(1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems—

(a) collection;

(b) alteration;

(c) consultation;

(d) disclosure (including transfers);

(e) combination;

(f) erasure.

(2) The logs of consultation must make it possible to establish—

(a) the justification for, and date and time of, the consultation, and

(b) so far as possible, the identity of the person who consulted the data.

(3) The logs of disclosure must make it possible to establish—

(a) the justification for, and date and time of, the disclosure, and

(b) so far as possible—

Ref. code: 25646301033624ADV

(i) the identity of the person who disclosed the data, and

(ii) the identity of the recipients of the data.

(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—

(a) to verify the lawfulness of processing;

(b) to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings;

(c) to ensure the integrity and security of personal data;

(d) the purposes of criminal proceedings.

(5) The controller or (as the case may be) the processor must make the logs available to the Commissioner on request.

63 Co-operation with the Commissioner

Each controller and each processor must co-operate, on request, with the Commissioner in the performance of the Commissioner's tasks.

64 Data protection impact assessment

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Ref. code: 25646301033624ADV

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.

65 Prior consultation with the Commissioner

(1) This section applies where a controller intends to create a filing system and process personal data forming part of it.

(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—

(a) the data protection impact assessment prepared under section 64, and

(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this PAriticle

(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.

(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.

(6) The Commissioner may extend the period of 6 weeks by a further period of 1 month, taking into account the complexity of the intended processing.

(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—

(a) inform the controller and, where applicable, the processor of any such extension before the end of the period of 1 month beginning with receipt of the request for consultation, and

(b) provide reasons for the delay.

Obligations relating to security

66 Security of processing

(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data

(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

Obligations relating to personal data breaches

67 Notification of a personal data breach to the Commissioner

(1) If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner—

(a) without undue delay, and

(b) where feasible, not later than 72 hours after becoming aware of it.

(2) Subsection (1) does not apply if the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

(3) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.

(4) Subject to subsection (5), the notification must include—

Ref. code: 25646301033624ADV

(a) 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;

(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of 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.

(5) Where and to the extent that it is not possible to provide all the information mentioned in subsection (4) at the same time, the information may be provided in phases without undue further delay.

(6) The controller must record the following information in relation to a personal data breach—

(a) the facts relating to the breach,

(b) its effects, and

(c) the remedial action taken.

(7) The information mentioned in subsection (6) must be recorded in such a way as to enable the Commissioner to verify compliance with this section.

(8) Where a personal data breach involves personal data that has been transmitted by or to a person who is a controller under the law of another member State, the information mentioned in subsection (6) must be communicated to that person without undue delay.

(9) If a processor becomes aware of a personal data breach (in relation to personal data processed by the processor), the processor must notify the controller without undue delay.

Ref. code: 25646301033624ADV

68 Communication of a personal data breach to the data subject

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay.

(2) The information given to the data subject must include the following—

(a) a description of the nature of the breach;

(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of 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.

(3) The duty under subsection (1) does not apply where—

(a) the controller has implemented appropriate technological and organizational protection measures which were applied to the personal data affected by the breach,

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise, or

(c) it would involve a disproportionate effort.

(4) An example of a case which may fall within subsection (3)(a) is where measures that render personal data unintelligible to any person not authorised to access the data have been applied, such as encryption.

(5) In a case falling within subsection (3)(c) (but not within subsection (3)(a) or (b)), the information mentioned in subsection (2) must be made available to the data subject inanother equally effective way, for example, by means of a public communication.

(6) Where the controller has not informed the data subject of the breach the Commissioner,

Ref. code: 25646301033624ADV

on being notified under section 67 and after considering the likelihood of the breach resulting in a high risk, may—

(a) require the controller to notify the data subject of the breach, or

(b) decide that the controller is not required to do so because any of paragraphs (a) to (c) of subsection (3) applies.

(7) The controller may restrict, wholly or partly, the provision of information to the datasubject under subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(8) Subsection (6) does not apply where the controller's decision not to inform the data subject of the breach was made in reliance on subsection (7).

(9) The duties in section 52(1) and (2) apply in relation to information that the controller is required to provide to the data subject under this section as they apply in relation to information that the controller is required to provide to the data subject under.

Chapter 3

Data protection officers

69 Designation of a data protection officer

(1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.

(2) When designating a data protection officer, the controller must have regard to theprofessional qualities of the proposed officer, in particular—

Ref. code: 25646301033624ADV

(a) the proposed officer's expert knowledge of data protection law and practice, and

(b) the ability of the proposed officer to perform the tasks mentioned in section 71.

(3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.

(4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner.

70 Position of data protection officer

(1) The controller must 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 must provide the data protection officer with the necessary resources and access to personal data and processing operations to enable the data protection officer to—

(a) perform the tasks mentioned in section 71, and

(b) maintain his or her expert knowledge of data protection law and practice.

(3) The controller—

(a) must ensure that the data protection officer does not receive any instructions regarding the performance of the tasks mentioned in section 71;

(b) must ensure that the data protection officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;

(c) must not dismiss or penalise the data protection officer for performing the tasks mentioned in section 71.

(4) A data subject may contact the data protection officer with regard to all issues relating to—

(a) the processing of that data subject's personal data, or

(b) the exercise of that data subject's rights under this PAriticle

Ref. code: 25646301033624ADV

(5) The data protection officer, in the performance of this role, must report to the highest management level of the controller.

71 Tasks of data protection officer

(1) The controller must entrust the data protection officer with at least the following tasks—

(a) informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Part,

(b) providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,

(c) co-operating with the Commissioner,

(d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter,

(e) monitoring compliance with policies of the controller in relation to the protection of personal data, and

(f) monitoring compliance by the controller with this PAriticle

(2) In relation to the policies mentioned in subsection (1)(e), the data protection officer's tasks include—

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

(3) In performing the tasks set out in subsections (1) and (2), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Ref. code: 25646301033624ADV

CHAPTER 5

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC

Overview and interpretation

72 Overview and interpretation

(1) This Chapter deals with the transfer of personal data to third countries or international organisations, as follows—

(a) sections 73 to 76 set out the general conditions that apply;

(b) section 77 sets out the special conditions that apply where the intended recipient of personal data is not a relevant authority in a third country or an international organisation;

(c) section 78 makes special provision about subsequent transfers of personal data.

(2) In this Chapter, "relevant authority", in relation to a third country, means any person based in a third country that has (in that country) functions comparable to those of a competent authority.

General principles for transfers

73 General principles for transfers of personal data

(1) A controller may not transfer personal data to a third country or to an international organisation unless—

(a) the three conditions set out in subsections (2) to (4) are met, and

(b) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.

(2) Condition 1 is that the transfer is necessary for any of the law enforcement purposes.

(3) Condition 2 is that the transfer—

Ref. code: 25646301033624ADV

(a) is based on an adequacy decision (see section 74),

(b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76).

(4) Condition 3 is that—

(a) the intended recipient is a relevant authority in a third country or an international organisation that is a relevant international organisation, or

(b) in a case where the controller is a competent authority specified in any of paragraphs 5 to 17, 21, 24 to 28, 34 to 51, 54 and 56 of Schedule 7—

(i) the intended recipient is a person in a third country other than a relevant authority, and

(ii) the additional conditions in section 77 are met.

(5) Authorisation is not required as mentioned in subsection (1)(b) if—

(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and

(b) the authorisation cannot be obtained in good time.

(6) Where a transfer is made without the authorisation mentioned in subsection (1)(b), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay

(7) In this section, "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.

74 Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organisation is based on an adequacy decision where—

(a) the European Commission has decided, in accordance with Article 36 of the Law Enforcement Directive, that—

Ref. code: 25646301033624ADV

(i) the third country or a territory or one or more specified sectors within that third country, or

(ii) (as the case may be) the international organisation, ensures an adequate level of protection of personal data, and

(b) that decision has not been repealed or suspended, or amended in a way that demonstrates that the Commission no longer considers there to be an adequate level of protection of personal data.

75 Transfers on the basis of appropriate safeguards

(1) A transfer of personal data to a third country or an international organisation is based on there being appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data, or

(b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organisation, concludes that appropriate safeguards exist to protect the data.

(2) The controller must inform the Commissioner about the categories of data transfers that take place in reliance on subsection (1)(b).

(3) Where a transfer of data takes place in reliance on subsection (1)—

(a) the transfer must be documented,

(b) the documentation must be provided to the Commissioner on request, and

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the recipient,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

76 Transfers on the basis of special circumstances

(1) A transfer of personal data to a third country or international organisation is based on special circumstances where the transfer is necessary—

Ref. code: 25646301033624ADV

(a) to protect the vital interests of the data subject or another person,

(b) to safeguard the legitimate interests of the data subject,

(c) for the prevention of an immediate and serious threat to the public security of a member State or a third country,

(d) in individual cases for any of the law enforcement purposes, or

(e) in individual cases for a legal purpose.

(2) But subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.

(3) Where a transfer of data takes place in reliance on subsection (1)—

(a) the transfer must be documented,

(b) the documentation must be provided to the Commissioner on request, and

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the recipient,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

(4) For the purposes of this section, a transfer is necessary for a legal purpose if—

(a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes,

(b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or

(c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

Transfers to particular recipients

77 Transfers of personal data to persons other than relevant authorities

(1) The additional conditions referred to in section 73(4)(b)(ii) are the following four conditions.

Ref. code: 25646301033624ADV

(2) Condition 1 is that the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes.

(3) Condition 2 is that the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(4) Condition 3 is that the transferring controller considers that the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled).

(5) Condition 4 is that the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed.

(6) Where personal data is transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate.

(7) The transferring controller must—

(a) document any transfer to a recipient in a third country other than a relevant authority, and

(b) inform the Commissioner about the transfer.

(8) This section does not affect the operation of any international agreement in force between member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.

Subsequent transfers

78 Subsequent transfers

(1) Where personal data is transferred in accordance with section 73, the transferring controller must make it a condition of the transfer that the data is not to be further

Ref. code: 25646301033624ADV

transferred to a third country or international organisation without the authorisation of the transferring controller or another competent authority.

(2) A competent authority may give an authorisation under subsection (1) only where the further transfer is necessary for a law enforcement purpose.

(3) In deciding whether to give the authorisation, the competent authority must take into account (among any other relevant factors)—

(a) the seriousness of the circumstances leading to the request for authorisation,

(b) the purpose for which the personal data was originally transferred, and

(c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.

(4) In a case where the personal data was originally transmitted or otherwise made available to the transferring controller or another competent authority by a member State other than the United Kingdom, an authorisation may not be given under subsection (1) unless that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.

(5) Authorisation is not required as mentioned in subsection (4) if—

(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and

(b) the authorisation cannot be obtained in good time.

(6) Where a transfer is made without the authorisation mentioned in subsection (4), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.

Ref. code: 25646301033624ADV

CHAPTER 6

SUPPLEMENTARY

79 National security: certificate

(1) A Minister of the Crown may issue a certificate certifying, for the purposes of section 44(4), 45(4), 48(3) or 68(7), that a restriction is a necessary and proportionate measure to protect national security.

(2) The certificate may—

(a) relate to a specific restriction (described in the certificate) which a controller has imposed or is proposing to impose under section 44(4), 45(4), 48(3) or 68(7), or

(b) identify any restriction to which it relates by means of a general description.

(3) Subject to subsection (6), a certificate issued under subsection (1) is conclusive evidence that the specific restriction or (as the case may be) any restriction falling within the general description is, or at any time was, a necessary and proportionate measure to protect national security.

(4) A certificate issued under subsection (1) may be expressed to have prospective effect.

(5) Any person directly affected by the issuing of a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(6) If, on an appeal under subsection (5), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may —

(a) allow the appeal, and

(b) quash the certificate.

(7) Where in any proceedings under or by virtue of this Act, it is claimed by a controller that a restriction falls within a general description in a certificate issued under subsection (1), any other party to the proceedings may appeal to the Tribunal on the ground that the restriction does not fall within that description.

(8) But, subject to any determination under subsection (9), the restriction is to be conclusively presumed to fall within the general description.

Ref. code: 25646301033624ADV

(9) On an appeal under subsection (7), the Tribunal may determine that the certificate does not so apply.

(10) A document purporting to be a certificate under subsection (1) is to be—

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

(11) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—

(a) in any legal proceedings, evidence of that certificate, and

(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(12) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or

(b) the Attorney General or the Advocate General for Scotland.

(13) No power conferred by any provision of Part 6 may be exercised in relation to the imposition of—

(a) a specific restriction in a certificate under subsection (1), or

(b) a restriction falling within a general description in such a certificate.

80 Special processing restrictions

(1) Subsections (3) and (4) apply where, for a law enforcement purpose, a controller transmits or otherwise makes available personal data to an EU recipient or a non-EU recipient.

(2) In this section—

"EU recipient" means—

(a) a recipient in a member State other than the United Kingdom, or

(b) an agency, office or body established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union;

"non-EU recipient" means—

(a) a recipient in a third country, or

(b) an international organisation.

(3) The controller must consider whether, if the personal data had instead been transmitted or otherwise made available within the United Kingdom to another competent authority, processing of the data by the other competent authority would have been subject to any restrictions by virtue of any enactment or rule of law.

(4) Where that would be the case, the controller must inform the EU recipient or non-EU recipient that the data is transmitted or otherwise made available subject to compliance by that person with the same restrictions (which must be set out in the information given to that person).

(5) Except as provided by subsection (4), the controller may not impose restrictions on the processing of personal data transmitted or otherwise made available by the controller to an EU recipient.

(6) Subsection (7) applies where—

(a) a competent authority for the purposes of the Law Enforcement Directive in a member State other than the United Kingdom transmits or otherwise makes available personal data to a controller for a law enforcement purpose, and

(b) the competent authority in the other member State informs the controller, in accordance with any law of that member State which implements Article 9(3) and (4) of the Law Enforcement Directive, that the data is transmitted or otherwise made available subject to compliance by the controller with restrictions set out by the competent authority.

(7) The controller must comply with the restrictions.

81 Reporting of infringements

(1) Each controller must implement effective mechanisms to encourage the reporting of an infringement of this PAriticle

(2) The mechanisms implemented under subsection (1) must provide that an infringement may be reported to any of the following persons—

(a) the controller;

(b) the Commissioner.

(3) The mechanisms implemented under subsection (1) must include—

(a) raising awareness of the protections provided by Part 4A of the Employment Rights Act 1996 and Part 5A of the Employment Rights (Northern Ireland) Order 1996 (S.I. 1996/1919 (N.I. 16)), and

(b) such other protections for a person who reports an infringement of this Part as the controller considers appropriate.

(4) A person who reports an infringement of this Part does not breach—

(a) an obligation of confidence owed by the person, or

(b) any other restriction on the disclosure of information (however imposed).

(5) Subsection (4) does not apply if or to the extent that the report includes a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(6) Until the repeal of Part 1 of the Regulation of Investigatory Powers Act 2000 by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force, subsection (5) has effect as if it included a reference to that PAriticle

PART 4

INTELLIGENCE SERVICES PROCESSING

CHAPTER 1

SCOPE AND DEFINITIONS

Scope

82 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by an intelligence service of personal data wholly or partly byautomated means, and

(b) the processing by an intelligence service otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(2) In this Part, “intelligence service” means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) the Government Communications Headquarters.

(3) A reference in this Part to the processing of personal data is to processing to which this Part applies.

Definitions

83 Meaning of “controller” and “processor”

(1) In this Part, “controller” means the intelligence service which, alone or jointly with others—

(a) determines the purposes and means of the processing of personal data, or

(b) is the controller by virtue of subsection (2).

(2) Where personal data is processed only—

(a) for purposes for which it is required by an enactment to be processed, and

(b) by means by which it is required by an enactment to be processed,

the intelligence service on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.

(3) In this Part, “processor” means any person who processes personal data on behalf of

the controller (other than a person who is an employee of the controller).

84 Other definitions

(1) This section defines other expressions used in this PAriticle

(2) “Consent”, in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual’s wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

(3) “Employee”, in relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.

Ref. code: 25646301033624ADV

(4) “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.

(5) “Recipient”, in relation to any personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a person to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

(6) “Restriction of processing” means the marking of stored personal data with the aim of limiting its processing for the future.

(7) Sections 3 and 205 include definitions of other expressions used in this Ariticle.

CHAPTER 2
PRINCIPLES
Overview

85 Overview

(1) This Chapter sets out the six data protection principles as follows

(a) section 86 sets out the first data protection principle (requirement that processing be lawful, fair and transparent);

(b) section 87 sets out the second data protection principle (requirement that the purposes of processing be specified, explicit and legitimate);

(c) section 88 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 89 sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 90 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 91 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) Each of sections 86, 87 and 91 makes provision to supplement the principle to which it relates.

Ref. code: 25646301033624ADV

The data protection principles

86 The first data protection principle

(1) The first data protection principle is that the processing of personal data must be—

(a) lawful, and

(b) fair and transparent.

(2) The processing of personal data is lawful only if and to the extent that—

(a) at least one of the conditions in Schedule 9 is met, and

(b) in the case of sensitive processing, at least one of the conditions in Schedule 10 is also met.

(3) The Secretary of State may by regulations amend Schedule 10—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(4) Regulations under subsection (3) are subject to the affirmative resolution procedure.

(5) In determining whether the processing of personal data is fair and transparent, regard is to be had to the method by which it is obtained.

(6) For the purposes of subsection (5), data is to be treated as obtained fairly and transparently if it consists of information obtained from a person who—

(a) is authorised by an enactment to supply it, or

(b) is required to supply it by an enactment or by an international obligation of the United Kingdom.

(7) In this section, “sensitive processing” means—

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data for the purpose of uniquely identifying an individual;

(c) the processing of biometric data for the purpose of uniquely identifying an individual;

Ref. code: 25646301033624ADV

(d) the processing of data concerning health;

(e) the processing of data concerning an individual'ssex life orsexual orientation;

(f) the processing of personal data as to—

(i) the commission or alleged commission of an offence by an individual, or

(ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

87 The second data protection principle

(1) The second data protection principle is that—

(a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected by a controller for one purpose may be processed for any other purpose of the controller that collected the data or any purpose of another controller provided that—

(a) the controller is authorised by law to process the data for that purpose, and

(b) the processing is necessary and proportionate to that other purpose.

(4) Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing—

(a) consists of—

(i) processing for archiving purposes in the public interest,

(ii) processing for the purposes of scientific or historical research, or

(iii) processing for statistical purposes, and

(b) is subject to appropriate safeguards for the rights and freedoms of the data subject.

Ref. code: 25646301033624ADV

88 The third data protection principle

The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

89 The fourth data protection principle

The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

90 The fifth data protection principle

The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

91 The sixth data protection principle

(1) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

(2) The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

CHAPTER 3

RIGHTS OF THE DATA SUBJECT

Overview

92 Overview

(1) This Chapter sets out the rights of the data subject as follows—

(a) section 93 deals with the information to be made available to the data subject;

(b) sections 94 and 95 deal with the right of access by the data subject;

(c) sections 96 and 97 deal with rights in relation to automated processing;

(d) section 98 deals with the right to information about decision-making;

Ref. code: 25646301033624ADV

(e) section 99 deals with the right to object to processing;

(f) section 100 deals with rights to rectification and erasure of personal data.

(2) In this Chapter, "the controller", in relation to a data subject, means the controller in relation to personal data relating to the data subject.

Rights

93 Right to information

(1) The controller must give a data subject the following information—

(a) the identity and the contact details of the controller;

(b) the legal basis on which, and the purposes for which, the controller processes personal data;

(c) the categories of personal data relating to the data subject that are being processed;

(d) the recipients or the categories of recipients of the personal data (if applicable);

(e) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(f) how to exercise rights under this Chapter;

(g) any other information needed to secure that the personal data is processed fairly and transparently.

(2) The controller may comply with subsection (1) by making information generally available, where the controller considers it appropriate to do so.

(3) The controller is not required under subsection (1) to give a data subject information that the data subject already has.

(4) Where personal data relating to a data subject is collected by or on behalf of the controller from a person other than the data subject, the requirement in subsection (1) has effect, in relation to the personal data so collected, with the following exceptions—

(a) the requirement does not apply in relation to processing that is authorised by an enactment;

Ref. code: 25646301033624ADV

(b) the requirement does not apply in relation to the data subject if giving the information to the data subject would be impossible or involve disproportionate effort.

94 Right of access

(1) An individual is entitled to obtain from a controller—

(a) confirmation as to whether or not personal data concerning the individual is being processed, and

(b) where that is the case—

(i) communication, in intelligible form, of the personal data of which that individual is the data subject, and

(ii) the information set out in subsection (2).

(2) That information is—

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data has been disclosed;

(d) the period for which the personal data is to be preserved;

(e) the existence of a data subject's rights to rectification and erasure of personal data (see section 100);

(f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) any information about the origin of the personal data concerned.

(3) A controller is not obliged to provide information under this section unless the controller has received such reasonable fee as the controller may require, subject to subsection (4).

(4) The Secretary of State may by regulations—

(a) specify cases in which a controller may not charge a fee;

(b) specify the maximum amount of a fee.

(5) Where a controller—

Ref. code: 25646301033624ADV

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual making a request under subsection (1), or

(ii) to locate the information which that individual seeks, and

(b) has informed that individual of that requirement, the controller is not obliged to comply with the request unless the controller is supplied with that further information.

(6) Where a controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller is not obliged to comply with the request unless—

(a) the other individual has consented to the disclosure of the information to the individual making the request, or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(7) In subsection (6), the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request.

(8) Subsection (6) is not to be construed as excusing a controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(9) In determining for the purposes of subsection (6)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard must be had, in particular, to—

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the controller with a view to seeking the consent of the other individual,

(c) whether the other individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.

Ref. code: 25646301033624ADV

(10) Subject to subsection (6), a controller must comply with a request under subsection (1) —

(a) promptly, and

(b) in any event before the end of the applicable time period.

(11) If a court is satisfied on the application of an individual who has made a request under subsection (1) that the controller in question has failed to comply with the request in contravention of this section, the court may order the controller to comply with the request.

(12) A court may make an order under subsection (11) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

(13) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(14) In this section—

"the applicable time period" means—

(a) the period of 1 month, or

(b) such longer period, not exceeding 3 months, as may be specified in regulations made by the Secretary of State, beginning with the relevant time;

"the relevant time", in relation to a request under subsection (1), means the latest of the following—

(a) when the controller receives the request,

(b) when the fee (if any) is paid, and

(c) when the controller receives the information (if any) required under subsection (5) in connection with the request.

(15) Regulations under this section are subject to the negative resolution procedure.

95 Right of access: supplementary

(1) The controller must comply with the obligation imposed by section 94(1)(b)(i) by supplying the data subject with a copy of the information in writing unless—

Ref. code: 25646301033624ADV

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise; and where any of the information referred to in section 94(1)(b)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(2) Where a controller has previously complied with a request made under section 94 by an individual, the controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(3) In determining for the purposes of subsection (2) whether requests under section 94 are made at reasonable intervals, regard must be had to—

(a) the nature of the data,

(b) the purpose for which the data is processed, and

(c) the frequency with which the data is altered.

(4) The information to be supplied pursuant to a request under section 94 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(5) For the purposes of section 94(6) to (8), an individual can be identified from information to be disclosed to a data subject by a controller if the individual can be identified from—

(a) that information, or

(b) that and any other information that the controller reasonably believes the data subject making the request is likely to possess or obtain.

Ref. code: 25646301033624ADV

96 Right not to be subject to automated decision-making

(1) The controller may not take a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject.

(2) Subsection (1) does not prevent such a decision being made on that basis if—

(a) the decision is required or authorised by law,

(b) the data subject has given consent to the decision being made on that basis, or

(c) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

(3) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

97 Right to intervene in automated decision-making

(1) This section applies where—

(a) the controller takes a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject, and

(b) the decision is required or authorised by law.

(2) This section does not apply to such a decision if—

(a) the data subject has given consent to the decision being made on that basis, or

(b) the decision is a decision taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract.

Ref. code: 25646301033624ADV

(3) The controller must as soon as reasonably practicable notify the data subject that such a decision has been made.

(4) The data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller—

(a) to reconsider the decision, or

(b) to take a new decision that is not based solely on automated processing.

(5) If a request is made to the controller under subsection (4), the controller must, before the end of the period of 1 month beginning with receipt of the request—

(a) consider the request, including any information provided by the data subject that is relevant to it, and

(b) by notice in writing inform the data subject of the outcome of that consideration.

(6) For the purposes of this section, a decision that has legal effects as regards an individual is to be regarded as significantly affecting the individual.

98 Right to information about decision-making

(1) Where—

(a) the controller processes personal data relating to a data subject, and

(b) results produced by the processing are applied to the data subject, the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing.

(2) Where the data subject makes a request under subsection (1), the controller must comply with the request without undue delay.

99 Right to object to processing

(1) A data subject is entitled at any time, by notice given to the controller, to require the controller—

(a) not to process personal data relating to the data subject, or

(b) not to process such data for a specified purpose or in a specified manner,

on the ground that, for specified reasons relating to the situation of the data subject, the processing in question is an unwarranted interference with the interests or rights of the data subject.

(2) Where the controller—

(a) reasonably requires further information—

(i) in order that the controller be satisfied as to the identity of the individual giving notice under subsection (1), or

(ii) to locate the data to which the notice relates, and

(b) has informed that individual of that requirement, the controller is not obliged to comply with the notice unless the controller is supplied with that further information.

(3) The controller must, before the end of 21 days beginning with the relevant time, give a notice to the data subject—

(a) stating that the controller has complied or intends to comply with the notice under subsection (1), or

(b) stating the controller's reasons for not complying with the notice to any extent and the extent (if any) to which the controller has complied or intends to comply with the notice under subsection (1).

(4) If the controller does not comply with a notice under subsection (1) to any extent, the data subject may apply to a court for an order that the controller take steps for complying with the notice.

(5) If the court is satisfied that the controller should comply with the notice (or should comply to any extent), the court may order the controller to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.

(6) A court may make an order under subsection (5) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates.

Ref. code: 25646301033624ADV

(7) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

(8) In this section, "the relevant time", in relation to a notice under subsection (1), means—

(a) when the controller receives the notice, or

(b) if later, when the controller receives the information (if any) required under subsection (2) in connection with the notice

100 Rights to rectification and erasure

(1) If a court is satisfied on the application of a data subject that personal data relating to the data subject is inaccurate, the court may order the controller to rectify that data without undue delay.

(2) If a court is satisfied on the application of a data subject that the processing of personal data relating to the data subject would infringe any of sections 86 to 91, the court may order the controller to erase that data without undue delay.

(3) If personal data relating to the data subject must be maintained for the purposes of evidence, the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(4) If—

(a) the data subject contests the accuracy of personal data, and

(b) the court is satisfied that the controller is not able to ascertain whether the data is accurate or not, the court may (instead of ordering the controller to rectify or erase the personal data) order the controller to restrict its processing without undue delay.

(5) A court may make an order under this section in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for carrying out the rectification, erasure or restriction of processing that the court proposes to order.

(6) The jurisdiction conferred on a court by this section is exercisable by the High Court or, in Scotland, by the Court of Session.

CHAPTER 4

CONTROLLER AND PROCESSOR

Overview

101 Overview

This Chapter sets out—

(a) the general obligations of controllers and processors (see sections 102 to 106);

(b) specific obligations of controllers and processors with respect to security (see section 107);

(c) specific obligations of controllers and processors with respect to personal data breaches (see section 108).

General obligations

102 General obligations of the controller

Each controller must implement appropriate measures—

(a) to ensure, and

(b) to be able to demonstrate, in particular to the Commissioner, that the processing of personal data complies with the requirements of this Ariticle.

103 Data protection by design

(1) Where a controller proposes that a particular type of processing of personal data be carried out by or on behalf of the controller, the controller must, prior to the processing, consider the impact of the proposed processing on the rights and freedoms of data subjects.

(2) A controller must implement appropriate technical and organisational measures which are designed to ensure that—

(a) the data protection principles are implemented, and

(b) risks to the rights and freedoms of data subjects are minimised.

Ref. code: 25646301033624ADV

104 Joint controllers

(1) Where two or more intelligence services jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this PAriticle

(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.

(3) The arrangement must designate the controller which is to be the contact point for data subjects.

105 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.

(2) The controller may use only a processor who undertakes—

(a) to implement appropriate measures that are sufficient to secure that the processing complies with this Part;

(b) to provide to the controller such information as is necessary for demonstrating that the processing complies with this PAriticle

(3) If a processor determines, in breach of this Part, the purposes and means of processing, the processor is to be treated for the purposes of this Part as a controller in respect of that processing.

106 Processing under the authority of the controller or processor

A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—

(a) on instructions from the controller, or

(b) to comply with a legal obligation.

Ref. code: 25646301033624ADV

Obligations relating to security

107 Security of processing

(1) Each controller and each processor must implement security measures appropriate to the risks arising from the processing of personal data.

(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to—

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it,

(b) ensure that it is possible to establish the precise details of any processing that takes place,

(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and

(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

Obligations relating to personal data breaches

108 Communication of a personal data breach

(1) If a controller becomes aware of a serious personal data breach in relation to personal data for which the controller is responsible, the controller must notify the Commissioner of the breach without undue delay.

(2) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.

(3) Subject to subsection (4), the notification must include—

(a) 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;

(b) the name and contact details of the contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

Ref. code: 25646301033624ADV

(d) a description of 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 to the extent that it is not possible to provide all the information mentioned in subsection (3) at the same time, the information may be provided in phases without undue further delay.

(5) If a processor becomes aware of a personal data breach (in relation to data processed by the processor), the processor must notify the controller without undue delay.

(6) Subsection (1) does not apply in relation to a personal data breach if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016.

(7) For the purposes of this section, a personal data breach is serious if the breach seriously interferes with the rights and freedoms of a data subject.

CHAPTER 5

TRANSFERS OF PERSONAL DATA OUTSIDE THE UNITED KINGDOM

109 Transfers of personal data outside the United Kingdom

(1) A controller may not transfer personal data to—

(a) a country or territory outside the United Kingdom, or

(b) an international organisation, unless the transfer falls within subsection (2).

(2) A transfer of personal data falls within this subsection if the transfer is a necessary and proportionate measure carried out—

(a) for the purposes of the controller's statutory functions, or

(b) for other purposes provided for, in relation to the controller, in section 2(2)(a) of the Security Service Act 1989 or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994.

Ref. code: 25646301033624ADV

CHAPTER 6

EXEMPTIONS

110 National security

(1) A provision mentioned in subsection (2) does not apply to personal data to which this Part applies if exemption from the provision is required for the purpose of safeguarding national security.

(2) The provisions are—

(a) Chapter 2 (the data protection principles), except section 86(1)(a) and (2) and Schedules 9 and 10;

(b) Chapter 3 (rights of data subjects);

(c) in Chapter 4 , section 108 (communication of a personal data breach to the Commissioner);

(d) in Part 5—

(i) section 119 (inspection in accordance with international obligations);

(ii) in Schedule 13 (other general functions of the Commissioner), paragraphs 1(a) and (g) and 2;

(e) in Part 6—

(i) sections 142 to 154 and Schedule 15 (Commissioner's notices and powers of entry and inspection);

(ii) sections 170 to 173 (offences relating to personal data);

(iii) sections 174 to 176 (provision relating to the special purposes).

111 National security: certificate

(1) Subject to subsection (3), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in section 110(2) is, or at any time was, required for the purpose of safeguarding national security in respect of any personal data is conclusive evidence of that fact.

(2) A certificate under subsection (1)—

(a) may identify the personal data to which it applies by means of a general description, and

Ref. code: 25646301033624ADV

(b) may be expressed to have prospective effect.

(3) Any person directly affected by the issuing of a certificate under subsection (1) may appeal to the Tribunal against the certificate.

(4) If on an appeal under subsection (3), the Tribunal finds that, applying the principles applied by a court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the Tribunal may—

(a) allow the appeal, and

(b) quash the certificate.

(5) Where, in any proceedings under or by virtue of this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

(6) But, subject to any determination under subsection (7), the certificate is to be conclusively presumed so to apply.

(7) On an appeal under subsection (5), the Tribunal may determine that the certificate does not so apply.

(8) A document purporting to be a certificate under subsection (1) is to be—

(a) received in evidence, and

(b) deemed to be such a certificate unless the contrary is proved.

(9) A document which purports to be certified by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) is—

(a) in any legal proceedings, evidence of that certificate, and

(b) in any legal proceedings in Scotland, sufficient evidence of that certificate.

(10) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by—

(a) a Minister who is a member of the Cabinet, or

(b) the Attorney General or the Advocate General for Scotland.

Ref. code: 25646301033624ADV

112 Other exemptions

Schedule 11 provides for further exemptions.

113 Power to make further exemptions

(1) The Secretary of State may by regulations amend Schedule 11—

(a) by adding exemptions from any provision of this Part;

(b) by omitting exemptions added by regulations under paragraph (a).

(2) Regulations under this section are subject to the affirmative resolution procedure.

PART 5

THE INFORMATION COMMISSIONER

The Commissioner

114 The Information Commissioner

(1) There is to continue to be an Information Commissioner.

(2) Schedule 12 makes provision about the Commissioner.

General functions

115 General functions under the GDPR and safeguards

(1) The Commissioner is to be the supervisory authority in the United Kingdom for the purposes of Article 51 of the GDPR.

(2) General functions are conferred on the Commissioner by—

(a) Article 57 of the GDPR (tasks), and

(b) Article 58 of the GDPR (powers), (and see also the Commissioner's duty under section 2).

(3) The Commissioner's functions in relation to the processing of personal data to which the GDPR applies include—

(a) a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, and

Ref. code: 25646301033624ADV

(b) a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(4) The Commissioner's functions under Article 58 of the GDPR are subject to the safeguards in subsections (5) to (9).

(5) The Commissioner's power under Article 58(1)(a) of the GDPR (power to require a controller or processor to provide information that the Commissioner requires for the performance of the Commissioner's tasks under the GDPR) is exercisable only by giving an information notice under section 142.

(6) The Commissioner's power under Article 58(1)(b) of the GDPR (power to carry out data protection audits) is exercisable only in accordance with section 146.

(7) The Commissioner's powers under Article 58(1)(e) and (f) of the GDPR (power to obtain information from controllers and processors and access to their premises) are exercisable only—

(a) in accordance with Schedule 15 (see section 154), or

(b) to the extent that they are exercised in conjunction with the power under Article 58(1)(b) of the GDPR, in accordance with section 146.

(8) The following powers are exercisable only by giving an enforcement notice under section 149—

(a) the Commissioner's powers under Article 58(2)(c) to (g) and (j) of the GDPR (certain corrective powers);

(b) the Commissioner's powers under Article 58(2)(h) to order a certification body to withdraw, or not to issue, a certification under Articles 42 and 43 of the GDPR.

(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the GDPR (administrative fines) are exercisable only by giving a penalty notice under section 155.

(10) This section is without prejudice to other functions conferred on the Commissioner, whether by the GDPR, this Act or otherwise.

Ref. code: 25646301033624ADV

116 Other general functions

(1) The Commissioner—

(a) is to be the supervisory authority in the United Kingdom for the purposes of Article 41 of the Law Enforcement Directive, and

(b) is to continue to be the designated authority in the United Kingdom for the purposes of Article 13 of the Data Protection Convention.

(2) Schedule 13 confers general functions on the Commissioner in connection with processing to which the GDPR does not apply (and see also the Commissioner's duty under section 2).

(3) This section and Schedule 13 are without prejudice to other functions conferred on the Commissioner, whether by this Act or otherwise.

117 Competence in relation to courts etc

Nothing in this Act permits or requires the Commissioner to exercise functions in relation to the processing of personal data by—

(a) an individual acting in a judicial capacity, or

(b) a court or tribunal acting in its judicial capacity, (and see also Article 55(3) of the GDPR).

International role

118 Co-operation and mutual assistance

(1) Articles 60 to 62 of the GDPR confer functions on the Commissioner in relation to co-operation and mutual assistance between, and joint operations of, supervisory authorities under the GDPR.

(2) References to the GDPR in subsection (1) do not include the applied GDPR.

(3) Article 61 of the applied GDPR confers functions on the Commissioner in relation to co-operation with other supervisory authorities (as defined in Article 4(21) of the applied GDPR).

(4) Part 1 of Schedule 14 makes provision as to the functions to be carried out by the Commissioner for the purposes of Article 50 of the Law Enforcement Directive (mutual assistance).

Ref. code: 25646301033624ADV

(5) Part 2 of Schedule 14 makes provision as to the functions to be carried out by the Commissioner for the purposes of Article 13 of the Data Protection Convention (co-operation between parties).

119 Inspection of personal data in accordance with international obligations

(1) The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2).

(2) The power under subsection (1) is exercisable only if the personal data—

(a) is processed wholly or partly by automated means, or

(b) is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.

(3) The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data.

(4) Before exercising the power under subsection (1), the Commissioner must by written notice inform the controller and any processor that the Commissioner intends to do so.

(5) Subsection (4) does not apply if the Commissioner considers that the case is urgent.

(6) It is an offence—

(a) intentionally to obstruct a person exercising the power under subsection (1), or

(b) to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

(7) Paragraphs (c) and (d) of section 3(14) do not apply to references in this section to personal data, the processing of personal data, a controller or a processor.

120 Further international role

(1) The Commissioner must, in relation to third countries and international organisations, take appropriate steps to—

(a) develop international co-operation 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, 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 co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

(2) Subsection (1) applies only in connection with the processing of personal data to which the GDPR does not apply; for the equivalent duty in connection with the processing of personal data to which the GDPR applies, see Article 50 of the GDPR (international co-operation for the protection of personal data).

(3) The Commissioner must carry out data protection functions which the Secretary of State directs the Commissioner to carry out for the purpose of enabling Her Majesty's Government in the United Kingdom to give effect to an international obligation of the United Kingdom.

(4) The Commissioner may provide an authority carrying out data protection functions under the law of a British overseas territory with assistance in carrying out those functions.

(5) The Secretary of State may direct that assistance under subsection (4) is to be provided on terms, including terms as to payment, specified or approved by the Secretary of State.

(6) In this section—

"data protection functions" means functions relating to the protection of individuals with respect to the processing of personal data;

"mutual assistance in the enforcement of legislation for the protection of personal data" includes assistance in the form of notification, complaint

Ref. code: 25646301033624ADV

referral, investigative assistance and information exchange;

"third country" means a country or territory that is not a member State.

(7) Section 3(14)(c) does not apply to references to personal data and the processing of personal data in this section

Codes of practice

121 Data-sharing code

(1) The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section—

"good practice in the sharing of personal data" means such practice in the sharing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

"the sharing of personal data" means the disclosure of personal data by transmission, dissemination or otherwise making it available;

"trade association" includes a body representing controllers or processors.

122 Direct marketing code

(1) The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section—

"direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals;

"good practice in direct marketing" means such practice in direct marketing as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements mentioned in subsection (1)(a);

"trade association" includes a body representing controllers or processors.

Ref. code: 25646301033624ADV

123 Age-appropriate design code

(1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate, including—

(a) children,

(b) parents,

(c) persons who appear to the Commissioner to represent the interests of children,

(d) child development experts, and

(e) trade associations.

(4) In preparing a code or amendments under this section, the Commissioner must have regard—

(a) to the fact that children have different needs at different ages, and

(b) to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

(5) A code under this section may include transitional provision or savings.

(6) Any transitional provision included in the first code under this section must cease to have effect before the end of the period of 12 months beginning when the code comes into force.

(7) In this section—

"age-appropriate design" means the design of services so that they are appropriate for use by, and meet the development needs of, children;

"information society services" has the same meaning as in the GDPR, but does not include preventive or counselling services;

"relevant information society services" means information society services

which involve the processing of personal data to which the GDPR applies;

"standards of age-appropriate design of relevant information society services" means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children;

"trade association" includes a body representing controllers or processors;

"the United Nations Convention on the Rights of the Child" means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention which are in force in relation to the United Kingdom), subject to any reservations, objections or interpretative declarations by the United Kingdom for the time being in force.

124 Data protection and journalism code

(1) The Commissioner must prepare a code of practice which contains—

(a) practical guidance in relation to the processing of personal data for the purposes of journalism in accordance with the requirements of the data protection legislation, and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the processing of personal data for the purposes of journalism.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section—

"good practice in the processing of personal data for the purposes of journalism" means such practice in the processing of personal data for those purposes as appears to the Commissioner to be desirable having regard to—

(a) the interests of data subjects and others, including compliance with the requirements of the data protection legislation, and

(b) the special importance of the public interest in the freedom of expression and information;

"trade association" includes a body representing controllers or processors.

125 Approval of codes prepared under sections 121 to 124

(1) When a code is prepared under section 121, 122, 123 or 124—

(a) the Commissioner must submit the final version to the Secretary of State, and

(b) the Secretary of State must lay the code before Parliament.

(2) In relation to the first code under section 123—

(a) the Commissioner must prepare the code as soon as reasonably practicable and must submit it to the Secretary of State before the end of the period of 18 months beginning when this Act is passed, and

(b) the Secretary of State must lay it before Parliament as soon as reasonably practicable.

(3) If, within the 40-day period, either House of Parliament resolves not to approve a code prepared under section 121, 122, 123 or 124, the Commissioner must not issue the code.

(4) If no such resolution is made within that period—

(a) the Commissioner must issue the code, and

(b) the code comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(5) If, as a result of subsection (3), there is no code in force under section 121, 122, 123 or 124, the Commissioner must prepare another version of the code.

Ref. code: 25646301033624ADV

(6) Nothing in subsection (3) prevents another version of the code being laid before Parliament.

(7) In this section, "the 40-day period" means—

(a) if the code islaid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the code islaid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(8) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

(9) This section, other than subsections (2) and (5), applies in relation to amendments prepared under section 121, 122, 123 or 124 as it applies in relation to codes prepared under those sections.

126 Publication and review of codes issued under section 125(4)

(1) The Commissioner must publish a code issued under section 125(4).

(2) Where an amendment of a code is issued under section 125(4), the Commissioner must publish—

(a) the amendment, or

(b) the code as amended by it.

(3) The Commissioner must keep under review each code issued under section 125(4) for the time being in force.

(4) Where the Commissioner becomes aware that the terms of such a code could result in a breach of an international obligation of the United Kingdom, the Commissioner must exercise the power under section 121(2), 122(2), 123(2) or 124(2) with a view to remedying the situation.

127 Effect of codes issued under section 125(4)

(1) A failure by a person to act in accordance with a provision of a code issued under section 125(4) does not of itself make that person liable to legal proceedings in a court or tribunal.

(2) A code issued under section 125(4), including an amendment or replacement code, is admissible in evidence in legal proceedings.

(3) In any proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code issued under section 125(4) in determining a question arising in the proceedings if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the court or tribunal to be relevant to the question.

(4) Where the Commissioner is carrying out a function described in subsection (5), the Commissioner must take into account a provision of a code issued under section 125(4) in determining a question arising in connection with the carrying out of the function if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.

(5) Those functions are functions under—

(a) the data protection legislation, or

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426).

128 Other codes of practice

(1) The Secretary of State may by regulations require the Commissioner—

(a) to prepare appropriate codes of practice giving guidance as to good practice in the processing of personal data, and

(b) to make them available to such persons as the Commissioner considers appropriate.

(2) Before preparing such codes, the Commissioner must consult such of the following as the Commissioner considers appropriate—

(a) trade associations;

(b) data subjects;

(c) persons who appear to the Commissioner to represent the interests of data subjects.

(3) Regulations under this section—

(a) must describe the personal data or processing to which the code of practice is to relate, and

(b) may describe the persons or classes of person to whom it is to relate.

(4) Regulations under this section are subject to the negative resolution procedure.

(5) In this section—

"good practice in the processing of personal data" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

"trade association" includes a body representing controllers or processors.

Consensual audits

129 Consensual audits

(1) The Commissioner's functions under Article 58(1) of the GDPR and paragraph 1 of Schedule 13 include power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.

(2) The Commissioner must inform the controller or processor of the results of such an assessment.

(3) In this section, "good practice in the processing of personal data" has the same meaning as in section 128.

Records of national security certificates

130 Records of national security certificates

(1) A Minister of the Crown who issues a certificate under section 27, 79 or 111 must send a copy of the certificate to the Commissioner.

Ref. code: 25646301033624ADV

(2) If the Commissioner receives a copy of a certificate under subsection (1), the Commissioner must publish a record of the certificate.

(3) The record must contain—

(a) the name of the Minister who issued the certificate,

(b) the date on which the certificate was issued, and

(c) subject to subsection (4), the text of the certificate.

(4) The Commissioner must not publish the text, or a part of the text, of the certificate if—

(a) the Minister determines that publishing the text or that part of the text—

(i) would be against the interests of national security,

(ii) would be contrary to the public interest, or

(iii) might jeopardise the safety of any person, and

(b) the Minister has notified the Commissioner of that determination.

(5) The Commissioner must keep the record of the certificate available to the public while the certificate is in force.

(6) If a Minister of the Crown revokes a certificate issued under section 27, 79 or 111, the Minister must notify the Commissioner.

Information provided to the Commissioner

131 Disclosure of information to the Commissioner

(1) No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Commissioner with information necessary for the discharge of the Commissioner's functions.

(2) But this section does not authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

(3) Until the repeal of Part 1 of the Regulation of Investigatory Powers Act 2000 by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force, subsection (2) has effect as if it included a reference to that PAriticle

132 Confidentiality of information

Ref. code: 25646301033624ADV

(1) A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

(2) For the purposes of subsection (1), a disclosure is made with lawful authority only if and to the extent that—

(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,

(b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner),

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions,

(d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation,

(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising, or

(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.

(3) It is an offence for a person knowingly or recklessly to disclose information in contravention of subsection (1).

133 Guidance about privileged communications

(1) The Commissioner must produce and publish guidance about—

(a) how the Commissioner proposes to secure that privileged communications which the Commissioner obtains or has access to in the course of carrying out

Ref. code: 25646301033624ADV

the Commissioner's functions are used or disclosed only so far as necessary for carrying out those functions, and

(b) how the Commissioner proposes to comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment.

(2) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(3) The Commissioner must consult the Secretary of State before publishing guidance under this section (including altered or replacement guidance).

(4) The Commissioner must arrange for guidance under this section (including altered or replacement guidance) to be laid before Parliament.

(5) In this section, "privileged communications" means—

(a) communications made—

(i) between a professional legal adviser and the adviser's client, and

(ii) in connection with the giving of legal advice to the client with respect to legal obligations, liabilities or rights, and

(b) communications made—

(i) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(ii) in connection with or in contemplation of legal proceedings, and

(iii) for the purposes of such proceedings.

(6) In subsection (5)—

(a) references to the client of a professional legal adviser include references to a person acting on behalf of the client, and

(b) references to a communication include—

(i) a copy or other record of the communication, and

(ii) anything enclosed with or referred to in the communication if made as described in subsection (5)(a)(ii) or in subsection (5)(b)(ii) and (iii).

Ref. code: 25646301033624ADV

Fees

134 Fees for services

The Commissioner may require a person other than a data subject or a data protection officer to pay a reasonable fee for a service provided to the person, or at the person's request, which the Commissioner is required or authorised to provide under the data protection legislation.

135 Manifestly unfounded or excessive requests by data subjects etc

(1) Where a request to the Commissioner from a data subject or a data protection officer is manifestly unfounded or excessive, the Commissioner may—

(a) charge a reasonable fee for dealing with the request, or

(b) refuse to act on the request.

(2) An example of a request that may be excessive is one that merely repeats the substance of previous requests.

(3) In any proceedings where there is an issue as to whether a request described in subsection (1) is manifestly unfounded or excessive, it is for the Commissioner to show that it is.

(4) Subsections (1) and (3) apply only in cases in which the Commissioner does not already have such powers and obligations under Article 57(4) of the GDPR.

136 Guidance about fees

(1) The Commissioner must produce and publish guidance about the fees the Commissioner proposes to charge in accordance with—

(a) section 134 or 135, or

(b) Article 57(4) of the GDPR.

(2) Before publishing the guidance, the Commissioner must consult the Secretary of State.

Ref. code: 25646301033624ADV

Charges

137 Charges payable to the Commissioner by controllers

(1) The Secretary of State may by regulations require controllers to pay charges of an amount specified in the regulations to the Commissioner

(2) Regulations under subsection (1) may require a controller to pay a charge regardless of whether the Commissioner has provided, or proposes to provide, a service to the controller.

(3) Regulations under subsection (1) may—

(a) make provision about the time or times at which, or period or periods within which, a charge must be paid;

(b) make provision for cases in which a discounted charge is payable;

(c) make provision for cases in which no charge is payable;

(d) make provision for cases in which a charge which has been paid is to be refunded.

(4) In making regulations under subsection (1), the Secretary of State must have regard to the desirability of securing that the charges payable to the Commissioner under such regulations are sufficient to offset—

(a) expenses incurred by the Commissioner in discharging the Commissioner's functions—

(i) under the data protection legislation,

(ii) under the Data Protection Act 1998,

(iii) under or by virtue of sections 108 and 109 of the Digital Economy Act 2017, and

(iv) under or by virtue of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426),

(b) any expenses of the Secretary of State in respect of the Commissioner so far as attributable to those functions,

(c) to the extent that the Secretary of State considers appropriate, any deficit previously incurred (whether before or after the passing of this Act) in respect of the expenses mentioned in paragraph (a), and

Ref. code: 25646301033624ADV

(d) to the extent that the Secretary of State considers appropriate, expenses incurred by the Secretary of State in respect of the inclusion of any officers or staff of the Commissioner in any scheme under section 1 of the Superannuation Act 1972 or section 1 of the Public Service Pensions Act 2013.

(5) The Secretary of State may from time to time require the Commissioner to provide information about the expenses referred to in subsection (4)(a).

(6) The Secretary of State may by regulations make provision—

(a) requiring a controller to provide information to the Commissioner, or

(b) enabling the Commissioner to require a controller to provide information to the Commissioner, for either or both of the purposes mentioned in subsection (7).

(7) Those purposes are—

(a) determining whether a charge is payable by the controller under regulations under subsection (1);

(b) determining the amount of a charge payable by the controller.

(8) The provision that may be made under subsection (6)(a) includes provision requiring a controller to notify the Commissioner of a change in the controller's circumstances of a kind specified in the regulations.

138 Regulations under section 137: supplementary

(1) Before making regulations under section 137(1) or (6), the Secretary of State must consult such representatives of persons likely to be affected by the regulations as the Secretary of State thinks appropriate (and see also section 182).

(2) The Commissioner—

(a) must keep under review the working of regulations under section 137(1) or (6), and

(b) may from time to time submit proposals to the Secretary of State for amendments to be made to the regulations.

Ref. code: 25646301033624ADV

(3) The Secretary of State must review the working of regulations under section 137(1) or (6)—

(a) at the end of the period of 5 years beginning with the making of the first set of regulations under section 108 of the Digital Economy Act 2017, and

(b) at the end of each subsequent 5 year period.

(4) Regulations under section 137(1) are subject to the negative resolution procedure if—

(a) they only make provision increasing a charge for which provision is made by previous regulations under section 137(1) or section 108(1) of the Digital Economy Act 2017, and

(b) they do so to take account of an increase in the retail prices index since the previous regulations were made.

(5) Subject to subsection (4), regulations under section 137(1) or (6) are subject to the affirmative resolution procedure.

(6) In subsection (4), "the retail prices index" means—

(a) the general index of retail prices (for all items) published by the Statistics Board, or

(b) where that index is not published for a month, any substitute index or figures published by the Board.

(7) Regulations under section 137(1) or (6) may not apply to—

(a) Her Majesty in her private capacity,

(b) Her Majesty in right of the Duchy of Lancaster, or

(c) the Duke of Cornwall.

Reports etc

139 Reporting to Parliament

(1) The Commissioner must—

(a) produce a general report on the carrying out of the Commissioner's functions annually,

(b) arrange for it to be laid before Parliament, and

(c) publish it.

(2) The report must include the annual report required under Article 59 of the GDPR.

(3) The Commissioner may produce other reports relating to the carrying out of the Commissioner's functions and arrange for them to be laid before Parliament.

140 Publication by the Commissioner

A duty under this Act for the Commissioner to publish a document is a duty for the Commissioner to publish it, or to arrange for it to be published, in such form and manner as the Commissioner considers appropriate.

141 Notices from the Commissioner

(1) This section applies in relation to a notice authorised or required by this Act to be given to a person by the Commissioner.

(2) The notice may be given to an individual—

(a) by delivering it to the individual,

(b) by sending it to the individual by post addressed to the individual at his or her usual or last-known place of residence or business, or

(c) by leaving it for the individual at that place.

(3) The notice may be given to a body corporate or unincorporate—

(a) by sending it by post to the proper officer of the body at its principal office, or

(b) by addressing it to the proper officer of the body and leaving it at that office.

(4) The notice may be given to a partnership in Scotland—

(a) by sending it by post to the principal office of the partnership, or

(b) by addressing it to that partnership and leaving it at that office.

(5) The notice may be given to the person by other means, including by electronic means, with the person's consent.

(6) In this section—

"principal office", in relation to a registered company, means its registered office;

Ref. code: 25646301033624ADV

"proper officer", in relation to any body, means the secretary or other executive officer charged with the conduct of its general affairs;

"registered company" means a company registered under the enactments relating to companies for the time being in force in the United Kingdom.

(7) This section is without prejudice to any other lawful method of giving a notice.

PART 6

ENFORCEMENT

Information notices

142 Information notices

(1) The Commissioner may, by written notice (an "information notice")—

(a) require a controller or processor to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of carrying out the Commissioner's functions under the data protection legislation, or

(b) require any person to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of—

(i) investigating a suspected failure of a type described in section 149(2) or a suspected offence under this Act, or

(ii) determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.

(2) An information notice must state—

(a) whether it is given under subsection (1)(a), (b)(i) or (b)(ii), and

(b) why the Commissioner requires the information.

(3) An information notice—

(a) may specify or describe particular information or a category of information;

(b) may specify the form in which the information must be provided;

(c) may specify the time at which, or the period within which, the information must be provided;

(d) may specify the place where the information must be provided;

Ref. code: 25646301033624ADV

(but see the restrictions in subsections (5) to (7)).

(4) An information notice must provide information about—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(5) An information notice may not require a person to provide information before the end of the period within which an appeal can be brought against the notice.

(6) If an appeal is brought against an information notice, the information need not be provided pending the determination or withdrawal of the appeal.

(7) If an information notice—

(a) states that, in the Commissioner's opinion, the information is required urgently, and

(b) gives the Commissioner's reasons for reaching that opinion, subsections (5) and (6) do not apply but the notice must not require the information to be provided before the end of the period of 24 hours beginning when the notice is given.

(8) The Commissioner may cancel an information notice by written notice to the person to whom it was given.

(9) In subsection (1), in relation to a person who is a controller or processor for the purposes of the GDPR, the reference to a controller or processor includes a representative of a controller or processor designated under Article 27 of the GDPR (representatives of controllers or processors not established in the European Union).

(10) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (1)(b).

143 Information notices: restrictions

(1) The Commissioner may not give an information notice with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 with respect to the data or the processing has taken effect, or

(b) the Commissioner—

Ref. code: 25646301033624ADV

(i) has reasonable grounds for suspecting that such a determination could be made, and

(ii) the information is required for the purposes of making such a determination.

(2) An information notice does not require a person to give the Commissioner information to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

(3) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client, and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(4) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and

(c) for the purposes of such proceedings.

(5) In subsections (3) and (4), references to the client of a professional legal adviser include references to a person acting on behalf of the client.

(6) An information notice does not require a person to provide the Commissioner with information if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence.

(7) The reference to an offence in subsection (6) does not include an offence under—

(a) this Act;

(b) section 5 of the Perjury Act 1911 (false statements made otherwise than on oath);

(c) section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false

Ref. code: 25646301033624ADV

statements made otherwise than on oath);

(d) Article 10 of the Perjury (Northern Ireland) Order 1979 (S.I. 1979/1714 (N.I. 19)) (false statutory declarations and other false unsworn statements).

(8) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a prosecution for an offence under this Act (other than an offence under section 144) unless in the proceedings—

(a) in giving evidence the person provides information inconsistent with the statement, and

(b) evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(9) In subsection (6), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the GDPR, the reference to the person providing the information being exposed to proceedingsfor an offence includes a reference to the controller or processor being exposed to such proceedings.

144 False statements made in response to information notices

It is an offence for a person, in response to an information notice—

(a) to make a statement which the person knows to be false in a material respect, or

(b) recklessly to make a statement which is false in a material respect.

145 Information orders

(1) This section applies if, on an application by the Commissioner, a court is satisfied that a person has failed to comply with a requirement of an information notice.

(2) The court may make an order requiring the person to provide to the Commissioner some or all of the following—

(a) information referred to in the information notice;

(b) other information which the court is satisfied the Commissioner requires, having regard to the statement included in the notice in accordance with

Ref. code: 25646301033624ADV

section 142(2)(b).

(3) The order—

(a) may specify the form in which the information must be provided,

(b) must specify the time at which, or the period within which, the information must be provided, and

(c) may specify the place where the information must be provided.

Assessment notices 146 Assessment notices

(1) The Commissioner may by written notice (an "assessment notice") require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation.

(2) An assessment notice may require the controller or processor to do any of the following—

(a) permit the Commissioner to enter specified premises;

(b) direct the Commissioner to documents on the premises that are of a specified description;

(c) assist the Commissioner to view information of a specified description that is capable of being viewed using equipment on the premises;

(d) comply with a request from the Commissioner for a copy (in such form as may be requested) of—

(i) the documents to which the Commissioner is directed;

(ii) the information which the Commissioner is assisted to view;

(e) direct the Commissioner to equipment or other material on the premises which is of a specified description;

(f) permit the Commissioner to inspect or examine the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;

(g) provide the Commissioner with an explanation of such documents, information, equipment or material;

Ref. code: 25646301033624ADV

(h) permit the Commissioner to observe the processing of personal data that takes place on the premises;

(i) make available for interview by the Commissioner a specified number of people of a specified description who process personal data on behalf of the controller, not exceeding the number who are willing to be interviewed.

(3) In subsection (2), references to the Commissioner include references to the Commissioner's officers and staff.

(4) An assessment notice must, in relation to each requirement imposed by the notice, specify the time or times at which, or period or periods within which, the requirement must be complied with (but see the restrictions in subsections (6) to (9)).

(5) An assessment notice must provide information about—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(6) An assessment notice may not require a person to do anything before the end of the period within which an appeal can be brought against the notice.

(7) If an appeal is brought against an assessment notice, the controller or processor need not comply with a requirement in the notice pending the determination or withdrawal of the appeal.

(8) If an assessment notice—

(a) states that, in the Commissioner's opinion, it is necessary for the controller or processor to comply with a requirement in the notice urgently,

(b) gives the Commissioner's reasons for reaching that opinion, and

(c) does not meet the conditions in subsection (9)(a) to (d),

subsections (6) and (7) do not apply but the notice must not require the controller or processor to comply with the requirement before the end of the period of 7 days beginning when the notice is given.

(9) If an assessment notice—

Ref. code: 25646301033624ADV

(a) states that, in the Commissioner's opinion, there are reasonable grounds for suspecting that a controller or processor has failed or is failing as described in section 149(2) or that an offence under this Act has been or is being committed,

(b) indicates the nature of the suspected failure or offence,

(c) does not specify domestic premises,

(d) states that, in the Commissioner's opinion, it is necessary for the controller or processor to comply with a requirement in the notice in less than 7 days, and

(e) gives the Commissioner's reasons for reaching that opinion, subsections (6) and (7) do not apply.

(10) The Commissioner may cancel an assessment notice by written notice to the controller or processor to whom it was given.

(11) Where the Commissioner gives an assessment notice to a processor, the Commissioner must, so far as reasonably practicable, give a copy of the notice to each controller for whom the processor processes personal data.

(12) In this section—

"domestic premises" means premises, or a part of premises, used as a dwelling;

"specified" means specified in an assessment notice.

147 Assessment notices: restrictions

(1) An assessment notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.

(2) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—

(a) between a professional legal adviser and the adviser's client, and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(3) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—

Ref. code: 25646301033624ADV

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and

(c) for the purposes of such proceedings.

(4) In subsections (2) and (3)—

(a) references to the client of a professional legal adviser include references to a person acting on behalf of such a client, and

(b) references to a communication include—

(i) a copy or other record of the communication, and

(ii) anything enclosed with or referred to in the communication if made as described in subsection (2)(b) or in subsection (3)(b) and (c).

(5) The Commissioner may not give a controller or processor an assessment notice with respect to the processing of personal data for the special purposes.

(6) The Commissioner may not give an assessment notice to—

(a) a body specified in section 23(3) of the Freedom of Information Act 2000 (bodies dealing with security matters), or

(b) the Office for Standards in Education, Children's Services and Skills in so far as it is a controller or processor in respect of information processed for the purposes of functions exercisable by Her Majesty's Chief Inspector of Education, Children's Services and Skills by virtue of section 5(1)(a) of the Care Standards Act 2000.

Information notices and assessment notices: destruction of documents etc

148 Destroying or falsifying information and documents etc

(1) This section applies where a person—

(a) has been given an information notice requiring the person to provide the Commissioner with information, or

(b) has been given an assessment notice requiring the person to direct the Commissioner to a document, equipment or other material or to assist the

Ref. code: 25646301033624ADV

Commissioner to view information.

(2) It is an offence for the person—

(a) to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material, or

(b) to cause or permit the destruction, disposal, concealment, blocking or (where relevant) falsification of all or part of the information, document, equipment or material, with the intention of preventing the Commissioner from viewing, or being provided with or directed to, all or part of the information, document, equipment or material.

(3) It is a defence for a person charged with an offence under subsection (2) to prove that the destruction, disposal, concealment, blocking or falsification would have occurred in the absence of the person being given the notice.

Enforcement notices

149 Enforcement notices

(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice, or both (and see also sections 150 and 151).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

Ref. code: 25646301033624ADV

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

(3) The second type of failure is where a monitoring body has failed, or is failing, to comply with an obligation under Article 41 of the GDPR (monitoring of approved codes of conduct).

(4) The third type of failure is where a person who is a certification provider—

(a) does not meet the requirements for accreditation,

(b) has failed, or is failing, to comply with an obligation under Article 42 or 43 of the GDPR (certification of controllers and processors), or

(c) has failed, or is failing, to comply with any other provision of the GDPR (whether in the person's capacity as a certification provider or otherwise).

(5) The fourth type of failure is where a controller has failed, or is failing, to comply with regulations under section 137.

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure.

(7) An enforcement notice given in reliance on subsection (4) may only impose requirements which the Commissioner considers appropriate having regard to the failure (whether or not for the purpose of remedying the failure).

(8) The Secretary of State may by regulations confer power on the Commissioner to give an enforcement notice in respect of other failures to comply with the data protection legislation.

(9) Regulations under this section—

(a) may make provision about the giving of an enforcement notice in respect of the failure, including by amending this section and sections 150 to 152,

(b) may make provision about the giving of an information notice, an assessment notice or a penalty notice, or about powers of entry and inspection,

Ref. code: 25646301033624ADV

in connection with the failure, including by amending sections 142, 143, 146, 147 and 155 to 157 and Schedules 15 and 16, and

(c) are subject to the affirmative resolution procedure.

150 Enforcement notices: supplementary

(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).

(5) An enforcement notice must provide information about—

(a) the consequences of failure to comply with it, and

(b) the rights under sections 162 and 164 (appeals etc).

(6) An enforcement notice must not specify a time for compliance with a requirement in the notice which falls before the end of the period within which an appeal can be brought against the notice.

Ref. code: 25646301033624ADV

(7) If an appeal is brought against an enforcement notice, a requirement in the notice need not be complied with pending the determination or withdrawal of the appeal.

(8) If an enforcement notice—

(a) states that, in the Commissioner's opinion, it is necessary for a requirement to be complied with urgently, and

(b) gives the Commissioner's reasons for reaching that opinion,

subsections (6) and (7) do not apply but the notice must not require the requirement to be complied with before the end of the period of 24 hours beginning when the notice is given.

(9) In this section, "specified" means specified in an enforcement notice.

151 Enforcement notices: rectification and erasure of personal data etc

(1) Subsections (2) and (3) apply where an enforcement notice is given in respect of a failure by a controller or processor—

(a) to comply with a data protection principle relating to accuracy, or

(b) to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 46, 47 or 100 of this Act.

(2) If the enforcement notice requires the controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any other data which—

(a) is held by the controller or processor, and

(b) contains an expression of opinion which appears to the Commissioner to be based on the inaccurate personal data.

(3) Where a controller or processor has accurately recorded personal data provided by the data subject or a third party but the data is inaccurate, the enforcement notice may require the controller or processor—

(a) to take steps specified in the notice to ensure the accuracy of the data,

Ref. code: 25646301033624ADV

(b) if relevant, to secure that the data indicates the data subject's view that the data is inaccurate, and

(c) to supplement the data with a statement of the true facts relating to the matters dealt with by the data that is approved by the Commissioner,

(as well as imposing requirements under subsection (2)).

(4) When deciding what steps it is reasonable to specify under subsection (3)(a), the Commissioner must have regard to the purpose for which the data was obtained and further processed.

(5) Subsections (6) and (7) apply where—

(a) an enforcement notice requires a controller or processor to rectify or erase personal data, or

(b) the Commissioner is satisfied that the processing of personal data which has been rectified or erased by the controller or processor involved a failure described in subsection (1).

(6) An enforcement notice may, if reasonably practicable, require the controller or processor to notify third parties to whom the data has been disclosed of the rectification or erasure.

(7) In determining whether it is reasonably practicable to require such notification, the Commissioner must have regard, in particular, to the number of people who would have to be notified.

(8) In this section, "data protection principle relating to accuracy" means the principle in—

(a) Article 5(1)(d) of the GDPR,

(b) section 38(1) of this Act, or

(c) section 89 of this Act.

152 Enforcement notices: restrictions

(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 with respect to the data or the processing has taken effect, and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—

(a) the Commissioner has reason to suspect a failure described in section 149(2) which is of substantial public importance, and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) An enforcement notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.

(4) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller an enforcement notice in reliance on section 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

153 Enforcement notices: cancellation and variation

(1) The Commissioner may cancel or vary an enforcement notice by giving written notice to the person to whom it was given.

(2) A person to whom an enforcement notice is given may apply in writing to the Commissioner for the cancellation or variation of the notice.

(3) An application under subsection (2) may be made only—

(a) after the end of the period within which an appeal can be brought against the notice, and

(b) on the ground that, by reason of a change of circumstances, one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.

Ref. code: 25646301033624ADV

Powers of entry and inspection

154 Powers of entry and inspection

Schedule 15 makes provision about powers of entry and inspection.

Penalties

155 Penalty notices

(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2), (3), (4) or (5), or

(b) has failed to comply with an information notice, an assessment notice or an enforcement notice, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(3) Those matters are—

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 57, 66, 103 or 107;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

Ref. code: 25646301033624ADV

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Commissioner, including whether, and ifso to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) whether the penalty would be effective, proportionate and dissuasive.

(4) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 149(5).

(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

(6) The Secretary of State may by regulations—

(a) confer power on the Commissioner to give a penalty notice in respect of other failures to comply with the data protection legislation, and

(b) provide for the maximum penalty that may be imposed in relation to such failures to be either the standard maximum amount or the higher maximum amount.

(7) Regulations under this section—

(a) may make provision about the giving of penalty notices in respect of the failure,

(b) may amend this section and sections 156 to 158, and

(c) are subject to the affirmative resolution procedure.

(8) In this section, “higher maximum amount” and “standard maximum amount” have the same meaning as in section 157.

Ref. code: 25646301033624ADV

156 Penalty notices: restrictions

(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 with respect to the data or the processing has taken effect, and

(b) a court has granted leave for the notice to be given.

(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—

(a) the Commissioner has reason to suspect a failure described in section 149(2) which is of substantial public importance, and

(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.

(3) The Commissioner may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either House of Parliament.

(4) The Commissioner may not give a penalty notice to—

(a) the Crown Estate Commissioners, or

(b) a person who is a controller by virtue of section 209(4) (controller for the Royal Household etc).

(5) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller a penalty notice in reliance on section 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.

157 Maximum amount of penalty

(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) the amount specified in Article 83 of the GDPR, or

Ref. code: 25646301033624ADV

(b) if an amount is not specified there, the standard maximum amount.

(2) In relation to an infringement of a provision of Part 3 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 35, 36, 37, 38(1), 39(1), 40, 44, 45, 46, 47, 48, 49, 52, 53, 73, 74, 75, 76, 77 or 78, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(3) In relation to an infringement of a provision of Part 4 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—

(a) in relation to a failure to comply with section 86, 87, 88, 89, 90, 91, 93, 94, 100 or 109, the higher maximum amount, and

(b) otherwise, the standard maximum amount.

(4) In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.

(5) The "higher maximum amount" is—

(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 20 million Euros.

(6) The "standard maximum amount" is—

(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or

(b) in any other case, 10 million Euros.

(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

158 Fixed penalties for non-compliance with charges regulations

(1) The Commissioner must produce and publish a document specifying the amount of the penalty for a failure to comply with regulations made under section 137.

(2) The Commissioner may specify different amounts for different types of failure.

(3) The maximum amount that may be specified is 150% of the highest charge payable by a controller in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.

(4) The Commissioner—

(a) may alter or replace the document, and

(b) must publish any altered or replacement document.

(5) Before publishing a document under this section (including any altered or replacement document), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Commissioner considers appropriate.

(6) The Commissioner must arrange for a document published under this section (including any altered or replacement document) to be laid before Parliament.

159 Amount of penalties: supplementary

(1) For the purposes of Article 83 of the GDPR and section 157, the Secretary of State may by regulations—

(a) provide that a person of a description specified in the regulations is or is not an undertaking, and

(b) make provision about how an undertaking's turnover is to be determined.

(2) For the purposes of Article 83 of the GDPR, section 157 and section 158, the Secretary of State may by regulations provide that a period is or is not a financial year.

(3) Regulations under this section are subject to the affirmative resolution procedure.

Ref. code: 25646301033624ADV

Guidance

160 Guidance about regulatory action

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's functions in connection with—

(a) information notices,

(b) assessment notices,

(c) enforcement notices, and

(d) penalty notices.

(2) The Commissioner may produce and publish guidance about how the Commissioner proposes to exercise the Commissioner's other functions under this PAriticle

(3) In relation to information notices, the guidance must include—

(a) provision specifying factors to be considered in determining the time at which, or the period within which, information is to be required to be provided;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an information notice to a person in reliance on section 142(7) (urgent cases);

(c) provision about how the Commissioner will determine how to proceed if a person does not comply with an information notice.

(4) In relation to assessment notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an assessment notice to a person;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an assessment notice in reliance on section 146(8) or (9) (urgent cases);

(c) provision specifying descriptions of documents or information that—

(i) are not to be examined or inspected in accordance with an assessment notice, or

Ref. code: 25646301033624ADV

(ii) are to be so examined or inspected only by a person of a description specified in the guidance;

(d) provision about the nature of inspections and examinations carried out in accordance with an assessment notice;

(e) provision about the nature of interviews carried out in accordance with an assessment notice;

(f) provision about the preparation, issuing and publication by the Commissioner of assessment reports in respect of controllers and processors that have been given assessment notices;

(g) provision about how the Commissioner will determine how to proceed if a person does not comply with an assessment notice.

(5) The guidance produced in accordance with subsection (4)(c) must include provisions that relate to—

(a) documents and information concerning an individual's physical or mental health;

(b) documents and information concerning the provision of social care for an individual.

(6) In relation to enforcement notices, the guidance must include—

(a) provision specifying factors to be considered in determining whether to give an enforcement notice to a person;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to give an enforcement notice to a person in reliance on section 150(8) (urgent cases);

(c) provision about how the Commissioner will determine how to proceed if a person does not comply with an enforcement notice.

(7) In relation to penalty notices, the guidance must include—

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

Ref. code: 25646301033624ADV

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties;

(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.

(8) The Commissioner—

(a) may alter or replace guidance produced under this section, and

(b) must publish any altered or replacement guidance.

(9) Before producing guidance under this section (including any altered or replacement guidance), the Commissioner must consult—

(a) the Secretary of State, and

(b) such other persons as the Commissioner considers appropriate.

(10) Section 161 applies in relation to the first guidance under subsection (1).

(11) The Commissioner must arrange for other guidance under this section (including any altered or replacement guidance) to be laid before Parliament.

(12) In this section, "social care" has the same meaning as in Part 1 of the Health and Social Care Act 2008 (see section 9(3) of that Act).

161 Approval of first guidance about regulatory action

(1) When the first guidance is produced under section 160(1)—

(a) the Commissioner must submit the final version to the Secretary of State, and

(b) the Secretary of State must lay the guidance before Parliament.

(2) If, within the 40-day period, either House of Parliament resolves not to approve the guidance—

(a) the Commissioner must not issue the guidance, and

(b) the Commissioner must produce another version of the guidance (and this section applies to that version).

Ref. code: 25646301033624ADV

(3) If, within the 40-day period, no such resolution is made—

(a) the Commissioner must issue the guidance, and

(b) the guidance comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(4) Nothing in subsection (2)(a) prevents another version of the guidance being laid before Parliament.

(5) In this section, "the 40-day period" means—

(a) if the guidance is laid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the guidance is laid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(6) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

Appeals etc

162 Rights of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal—

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(2) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under section 153 for the cancellation or variation of the notice.

(3) A person who is given a penalty notice or a penalty variation notice may appeal to the Tribunal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

Ref. code: 25646301033624ADV

(4) Where a determination is made under section 174 in respect of the processing of personal data, the controller or processor may appeal to the Tribunal against the determination.

163 Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 162(1) or (3).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers—

(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently, the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

(5) On an appeal under section 162(2), if the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice.

(6) On an appeal under section 162(4), the Tribunal may cancel the Commissioner's determination.

164 Applications in respect of urgent notices

(1) This section applies where an information notice, an assessment notice or an enforcement notice given to a person contains an urgency statement.

(2) The person may apply to the court for either or both of the following—

(a) the disapplication of the urgency statement in relation to some or all of the requirements of the notice;

Ref. code: 25646301033624ADV

(b) a change to the time at which, or the period within which, a requirement of the notice must be complied with.

(3) On an application under subsection (2), the court may do any of the following—

(a) direct that the notice is to have effect as if it did not contain the urgency statement;

(b) direct that the inclusion of the urgency statement is not to have effect in relation to a requirement of the notice;

(c) vary the notice by changing the time at which, or the period within which, a requirement of the notice must be complied with;

(d) vary the notice by making other changes required to give effect to a direction under paragraph (a) or (b) or in consequence of a variation under paragraph (c).

(4) The decision of the court on an application under this section is final.

(5) In this section, "urgency statement" means—

(a) in relation to an information notice, a statement under section 142(7)(a),

(b) in relation to an assessment notice, a statement under section 146(8)(a) or (9) (d), and

(c) in relation to an enforcement notice, a statement under section 150(8)(a).

Complaints

165 Complaints by data subjects

(1) Articles 57(1)(f) and (2) and 77 of the GDPR (data subject'sright to lodge a complaint) confer rights on data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the GDPR.

(2) A data subject may make a complaint to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of Part 3 or 4 of this Act.

Ref. code: 25646301033624ADV

(3) The Commissioner must facilitate the making of complaints under subsection (2) by taking steps such as providing a complaint form which can be completed electronically and by other means.

(4) If the Commissioner receives a complaint under subsection (2), the Commissioner must—

(a) take appropriate steps to respond to the complaint,

(b) inform the complainant of the outcome of the complaint,

(c) inform the complainant of the rights under section 166, and

(d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps in response to a complaint includes—

(a) investigating the subject matter of the complaint, to the extent appropriate, and

(b) informing the complainant about progress on the complaint, including about whether further investigation or co-ordination with another supervisory authority or foreign designated authority is necessary.

(6) If the Commissioner receives a complaint relating to the infringement of a data subject's rights under provisions adopted by a member State other than the United Kingdom pursuant to the Law Enforcement Directive, the Commissioner must—

(a) send the complaint to the relevant supervisory authority for the purposes of that Directive,

(b) inform the complainant that the Commissioner has done so, and

(c) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(7) In this section—

"foreign designated authority" means an authority designated for the purposes of Article 13 of the Data Protection Convention by a party, other than the United Kingdom, which is bound by that Convention;

"supervisory authority" means a supervisory authority for the purposes of

Ref. code: 25646301033624ADV

Article 51 of the GDPR or Article 41 of the Law Enforcement Directive in a member State other than the United Kingdom.

166 Orders to progress complaints

(1) This section applies where, after a data subject makes a complaint under section 165 or Article 77 of the GDPR, the Commissioner—

(a) fails to take appropriate steps to respond to the complaint,

(b) fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning when the Commissioner received the complaint, or

(c) if the Commissioner's consideration of the complaint is not concluded during that period, fails to provide the complainant with such information during a subsequent period of 3 months.

(2) The Tribunal may, on an application by the data subject, make an order requiring the Commissioner—

(a) to take appropriate steps to respond to the complaint, or

(b) to inform the complainant of progress on the complaint, or of the outcome of the complaint, within a period specified in the order.

(3) An order under subsection (2)(a) may require the Commissioner—

(a) to take steps specified in the order;

(b) to conclude an investigation, or take a specified step, within a period specified in the order.

(4) Section 165(5) applies for the purposes of subsections (1)(a) and (2)(a) as it appliesfor the purposes of section 165(4)(a).

Remedies in the court

167 Compliance orders

(1) This section applies if, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation.

Ref. code: 25646301033624ADV

(2) A court may make an order for the purposes of securing compliance with the data protection legislation which requires the controller in respect of the processing, or a processor acting on behalf of that controller—

(a) to take steps specified in the order, or

(b) to refrain from taking steps specified in the order.

(3) The order may, in relation to each step, specify the time at which, or the period within which, it must be taken.

(4) In subsection (1)—

(a) the reference to an application by a data subject includes an application made in exercise of the right under Article 79(1) of the GDPR (right to an effective remedy against a controller or processor);

(b) the reference to the data protection legislation does not include Part 4 of this Act or regulations made under that PAriticle

(5) In relation to a joint controller in respect of the processing of personal data to which Part 3 applies whose responsibilities are determined in an arrangement under section 58, a court may only make an order under this section if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

168 Compensation for contravention of the GDPR

(1) In Article 82 of the GDPR (right to compensation for material or non-material damage), “non-material damage” includes distress.

(2) Subsection (3) applies where—

(a) in accordance with rules of court, proceedings under Article 82 of the GDPR are brought by a representative body on behalf of a person, and

(b) a court orders the payment of compensation.

(3) The court may make an order providing for the compensation to be paid on behalf of the person to—

(a) the representative body, or

(b) such other person as the court thinks fit.

Ref. code: 25646301033624ADV

169 Compensation for contravention of other data protection legislation

(1) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3).

(2) Under subsection (1)—

(a) a controller involved in processing of personal data is liable for any damage caused by the processing, and

(b) a processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the data protection legislation specifically directed at processors, or

(ii) has acted outside, or contrary to, the controller's lawful instructions.

(3) A controller or processor is not liable as described in subsection (2) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

(4) A joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities are determined in an arrangement under section 58 or 104 is only liable as described in subsection (2) if the controller is responsible for compliance with the provision of the data protection legislation that is contravened.

(5) In this section, "damage" includes financial loss and damage not involving financial loss, such as distress. Offences relating to personal data

170 Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly—

(a) to obtain or disclose personal data without the consent of the controller,

(b) to procure the disclosure of personal data to another person without the consent of the controller, or

Ref. code: 25646301033624ADV

(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining—

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(3) It is also a defence for a person charged with an offence under subsection (1) to prove that—

(a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,

(b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or

(c) the person acted—

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.

(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.

(5) It is an offence for a person to offer to sell personal data if the person—

(a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or

(b) subsequently obtains the data in such circumstances.

Ref. code: 25646301033624ADV

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

(7) In this section—

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);

(b) where there is more than one controller, such references are references to the consent of one or more of them.

171 Re-identification of de-identified personal data

(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

(2) For the purposes of this section and section 172—

(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).

(3) It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification—

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(4) It is also a defence for a person charged with an offence under subsection (1) to prove that—

(a) the person acted in the reasonable belief that the person—

(i) is the data subject to whom the information relates,

Ref. code: 25646301033624ADV

(ii) had the consent of that data subject, or

(iii) would have had such consent if the data subject had known about the re-identification and the circumstances of it,

(b) the person acted in the reasonable belief that the person—

(i) is the controller responsible for de-identifying the personal data,

(ii) had the consent of that controller, or

(iii) would have had such consent if that controller had known about the re-identification and the circumstances of it,

(c) the person acted—

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest, or

(d) the effectiveness testing conditions were met (see section 172).

(5) It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so—

(a) without the consent of the controller responsible for de-identifying the personal data, and

(b) in circumstances in which the re-identification was an offence under subsection (1).

(6) It is a defence for a person charged with an offence under subsection (5) to prove that the processing—

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(7) It is also a defence for a person charged with an offence under subsection (5) to prove that—

(a) the person acted in the reasonable belief that the processing was lawful,

Ref. code: 25646301033624ADV

(b) the person acted in the reasonable belief that the person—

(i) had the consent of the controller responsible for de-identifying the personal data, or

(ii) would have had such consent if that controller had known about the processing and the circumstances of it, or

(c) the person acted—

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the processing was justified as being in the public interest.

(8) In this section—

(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);

(b) where there is more than one controller, such references are references to the consent of one or more of them.

172 Re-identification: effectiveness testing conditions

(1) For the purposes of section 171, in relation to a person who re-identifies information that is de-identified personal data, "the effectiveness testing conditions" means the conditions in subsections (2) and (3).

(2) The first condition is that the person acted—

(a) with a view to testing the effectiveness of the de-identification of personal data,

(b) without intending to cause, or threaten to cause, damage or distress to a person, and

(c) in the reasonable belief that, in the particular circumstances, re-identifying the information was justified as being in the public interest.

Ref. code: 25646301033624ADV

(3) The second condition is that the person notified the Commissioner or the controller responsible for de-identifying the personal data about the re-identification—

(a) without undue delay, and

(b) where feasible, not later than 72 hours after becoming aware of it.

(4) Where there is more than one controller responsible for de-identifying personal data, the requirement in subsection (3) is satisfied if one or more of them is notified.

173 Alteration etc of personal data to prevent disclosure to data subject

(1) Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

(2) In this section, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).

(3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

(4) Those persons are—

(a) the controller, and

(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

(5) It is a defence for a person charged with an offence undersubsection (3) to prove that—

Ref. code: 25646301033624ADV

(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right, or

(b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request

The special purposes

174 The special purposes

(1) In this Part, "the special purposes" means one or more of the following—

(a) the purposes of journalism;

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

(2) In this Part, "special purposes proceedings" means legal proceedings against a controller or processor which relate, wholly or partly, to personal data processed for the special purposes and which are—

(a) proceedings under section 167 (including proceedings on an application under Article 79 of the GDPR), or

(b) proceedings under Article 82 of the GDPR or section 169.

(3) The Commissioner may make a written determination, in relation to the processing of personal data, that—

(a) the personal data is not being processed only for the special purposes;

(b) the personal data is not being processed with a view to the publication by a person of journalistic, academic, artistic or literary material which has not previously been published by the controller.

(4) The Commissioner must give written notice of the determination to the controller and the processor.

(5) The notice must provide information about the rights of appeal under section 162.

(6) The determination does not take effect until one of the following conditions is

Ref. code: 25646301033624ADV

satisfied—

(a) the period for the controller or the processor to appeal against the determination has ended without an appeal having been brought, or

(b) an appeal has been brought against the determination and—

(i) the appeal and any further appeal in relation to the determination has been decided or has otherwise ended, and

(ii) the time for appealing against the result of the appeal or further appeal has ended without another appeal having been brought.

175 Provision of assistance in special purposes proceedings

(1) An individual who is a party, or prospective party, to special purposes proceedings may apply to the Commissioner for assistance in those proceedings.

(2) As soon as reasonably practicable after receiving an application under subsection (1), the Commissioner must decide whether, and to what extent, to grant it.

(3) The Commissioner must not grant the application unless, in the Commissioner's opinion, the case involves a matter of substantial public importance.

(4) If the Commissioner decides not to provide assistance, the Commissioner must, as soon as reasonably practicable, notify the applicant of the decision, giving reasons for the decision.

(5) If the Commissioner decides to provide assistance, the Commissioner must—

(a) as soon as reasonably practicable, notify the applicant of the decision, stating the extent of the assistance to be provided, and

(b) secure that the person against whom the proceedings are, or are to be, brought is informed that the Commissioner is providing assistance.

(6) The assistance that may be provided by the Commissioner includes—

(a) paying costs in connection with the proceedings, and

(b) indemnifying the applicant in respect of liability to pay costs, expenses or damages in connection with the proceedings.

(7) In England and Wales or Northern Ireland, the recovery of expenses incurred by the Commissioner in providing an applicant with assistance under this section (as

Ref. code: 25646301033624ADV

taxed or assessed in accordance with rules of court) is to constitute a first charge for the benefit of the Commissioner—

(a) on any costs which, by virtue of any judgment or order of the court, are payable to the applicant by any other person in respect of the matter in connection with which the assistance is provided, and

(b) on any sum payable to the applicant under a compromise or settlement arrived at in connection with that matter to avoid, or bring to an end, any proceedings.

(8) In Scotland, the recovery of such expenses (as taxed or assessed in accordance with rules of court) is to be paid to the Commissioner, in priority to other debts—

(a) out of any expenses which, by virtue of any judgment or order of the court, are payable to the applicant by any other person in respect of the matter in connection with which the assistance is provided, and

(b) out of any sum payable to the applicant under a compromise or settlement arrived at in connection with that matter to avoid, or bring to an end, any proceedings.

176 Staying special purposes proceedings

(1) In any special purposes proceedings before a court, if the controller or processor claims, or it appears to the court, that any personal data to which the proceedings relate—

(a) is being processed only for the special purposes,

(b) is being processed with a view to the publication by any person of journalistic, academic, artistic or literary material, and

(c) has not previously been published by the controller, the court must stay or, in Scotland, sist the proceedings.

(2) In considering, for the purposes of subsection (1)(c), whether material has previously been published, publication in the immediately preceding 24 hours is to be ignored.

Ref. code: 25646301033624ADV

(3) Under subsection (1), the court must stay or sist the proceedings until either of the following conditions is met—

(a) a determination of the Commissioner under section 174 with respect to the personal data or the processing takes effect;

(b) where the proceedings were stayed or sisted on the making of a claim, the claim is withdrawn.

177 Guidance about how to seek redress against media organisations

(1) The Commissioner must produce and publish guidance about the steps that may be taken where an individual considers that a media organisation is failing or has failed to comply with the data protection legislation.

(2) In this section, "media organisation" means a body or other organisation whose activities consist of or include journalism.

(3) The guidance must include provision about relevant complaints procedures, including—

(a) who runs them,

(b) what can be complained about, and

(c) how to make a complaint.

(4) For the purposes of subsection (3), relevant complaints procedures include procedures for making complaints to the Commissioner, the Office of Communications, the British Broadcasting Corporation and other persons who produce or enforce codes of practice for media organisations.

(5) The guidance must also include provision about—

(a) the powers available to the Commissioner in relation to a failure to comply with the data protection legislation,

(b) when a claim in respect of such a failure may be made before a court and how to make such a claim,

(c) alternative dispute resolution procedures,

(d) the rights of bodies and other organisations to make complaints and claims on behalf of data subjects, and

Ref. code: 25646301033624ADV

(e) the Commissioner's power to provide assistance in special purpose proceedings.

(6) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(7) The Commissioner must produce and publish the first guidance under this section before the end of the period of 1 year beginning when this Act is passed.

178 Review of processing of personal data for the purposes of journalism

(1) The Commissioner must—

(a) review the extent to which, during each review period, the processing of personal data for the purposes of journalism complied with—

(i) the data protection legislation, and

(ii) good practice in the processing of personal data for the purposes of journalism,

(b) prepare a report of the review, and

(c) submit the report to the Secretary of State.

(2) In this section—

"good practice in the processing of personal data for the purposes of journalism" has the same meaning as in section 124;

"review period" means—

(a) the period of 4 years beginning with the day on which Chapter 2 of Part 2 of this Act comes into force, and

(b) each subsequent period of 5 years beginning with the day after the day on which the previous review period ended.

(3) The Commissioner must start a review under this section, in respect of a review period, within the period of 6 months beginning when the review period ends.

(4) The Commissioner must submit the report of a review under this section to the Secretary of State—

(a) in the case of the first review, before the end of the period of 18 months

Ref. code: 25646301033624ADV

beginning when the Commissioner started the review, and

(b) in the case of each subsequent review, before the end of the period of 12 months beginning when the Commissioner started the review.

(5) The report must include consideration of the extent of compliance (as described in subsection (1)(a)) in each part of the United Kingdom.

(6) The Secretary of State must—

(a) lay the report before Parliament, and

(b) send a copy of the report to—

(i) the Scottish Ministers,

(ii) the Welsh Ministers, and

(iii) the Executive Office in Northern Ireland.

(7) Schedule 17 makes further provision for the purposes of a review under this section.

179 Effectiveness of the media's dispute resolution procedures

(1) The Secretary of State must, before the end of each review period, lay before Parliament a report produced by the Secretary of State or an appropriate person on—

(a) the use of relevant alternative dispute resolution procedures, during that period, in cases involving a failure, or alleged failure, by a relevant media organisation to comply with the data protection legislation, and

(b) the effectiveness of those procedures in such cases.

(2) In this section—

"appropriate person" means a person who the Secretary of State considers has appropriate experience and skills to produce a report described in subsection (1);

"relevant alternative dispute resolution procedures" means alternative dispute resolution procedures provided by persons who produce or enforce codes of practice for relevant media organisations;

"relevant media organisation" means a body or other organisation whose

Ref. code: 25646301033624ADV

activities consist of or include journalism, other than a broadcaster;

"review period" means—

(a) the period of 3 years beginning when this Act is passed, and

(b) each subsequent period of 3 years.

(3) The Secretary of State must send a copy of the report to—

(a) the Scottish Ministers

(b) the Welsh Ministers, and

(c) the Executive Office in Northern Ireland.

Jurisdiction of courts

180 Jurisdiction

(1) The jurisdiction conferred on a court by the provisions listed in subsection (2) is exercisable—

(a) in England and Wales, by the High Court or the county court,

(b) in Northern Ireland, by the High Court or a county court, and

(c) in Scotland, by the Court of Session or the sheriff,

subject to subsections (3) and (4).

(2) Those provisions are—

(a) section 145 (information orders);

(b) section 152 (enforcement notices and processing for the special purposes);

(c) section 156 (penalty notices and processing for the special purposes);

(d) section 167 and Article 79 of the GDPR (compliance orders);

(e) sections 168 and 169 and Article 82 of the GDPR (compensation).

(3) In relation to the processing of personal data to which Part 4 applies, the jurisdiction conferred by the provisions listed in subsection (2) is exercisable only by the High Court or, in Scotland, the Court of Session.

(4) In relation to an information notice which contains a statement under section 142(7), the jurisdiction conferred on a court by section 145 is exercisable only by the High Court or, in Scotland, the Court of Session.

Ref. code: 25646301033624ADV

(5) The jurisdiction conferred on a court by section 164 (applications in respect of urgent notices) is exercisable only by the High Court or, in Scotland, the Court of Session.

Definitions

181 Interpretation of Part 6

In this Part—

"assessment notice" has the meaning given in section 146;

"certification provider" has the meaning given in section 17;

"enforcement notice" has the meaning given in section 149;

"information notice" has the meaning given in section 142;

"penalty notice" has the meaning given in section 155;

"penalty variation notice" has the meaning given in Schedule 16;

"representative", in relation to a controller or processor, means a person designated by the controller or processor under Article 27 of the GDPR to represent the controller or processor with regard to the controller's or processor's obligations under the GDPR.

PART 7

SUPPLEMENTARY AND FINAL PROVISION

Regulations under this Act

182 Regulations and consultation

(1) Regulations under this Act are to be made by statutory instrument.

(2) Before making regulations under this Act, the Secretary of State must consult—

(a) the Commissioner, and

(b) such other persons as the Secretary of State considers appropriate.

(3) Subsection (2) does not apply to regulations made under—

(a) section 23;

(b) section 30;

(c) section 211;

(d) section 212;

(e) section 213;

(f) paragraph 15 of Schedule 2.

(4) Subsection (2) does not apply to regulations made under section 18 where the Secretary of State has made an urgency statement in respect of them.

(5) Regulations under this Act may—

(a) make different provision for different purposes;

(b) include consequential, supplementary, incidental, transitional, transitory or saving provision.

(6) Where regulations under this Act are subject to "the negative resolution procedure" the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of either House of Parliament.

(7) Where regulations under this Act are subject to "the affirmative resolution procedure" the regulations may not be made unless a draft of the statutory instrument containing them has been laid before Parliament and approved by a resolution of each House of Parliament.

(8) Where regulations under this Act are subject to "the made affirmative resolution procedure"—

(a) the statutory instrument containing the regulations must be laid before Parliament after being made, together with the urgency statement in respect of them, and

(b) the regulations cease to have effect at the end of the period of 120 days beginning with the day on which the instrument is made, unless within that period the instrument is approved by a resolution of each House of Parliament.

(9) In calculating the period of 120 days, no account is to be taken of any time during which—

(a) Parliament is dissolved or prorogued, or

(b) both Houses of Parliament are adjourned for more than 4 days.

(10) Where regulations cease to have effect as a result of subsection (8), that does not—

Ref. code: 25646301033624ADV

(a) affect anything previously done under the regulations, or

(b) prevent the making of new regulations.

(11) Any provision that may be included in regulations under this Act subject to the negative resolution procedure may be made by regulations subject to the affirmative resolution procedure or the made affirmative resolution procedure.

(12) If a draft of a statutory instrument containing regulations under section 7 would, apart from this subsection, be treated for the purposes of the standing orders of either House of Parliament as a hybrid instrument, it is to proceed in that House as if it were not such an instrument.

(13) A requirement under a provision of this Act to consult may be satisfied by consultation before, as well as by consultation after, the provision comes into force.

(14) In this section, "urgency statement" has the meaning given in section 18(4).

Changes to the Data Protection Convention

183 Power to reflect changes to the Data Protection Convention

(1) The Secretary of State may by regulations make such provision as the Secretary of State considers necessary or appropriate in connection with an amendment of, or an instrument replacing, the Data Protection Convention which has effect, or is expected to have effect, in the United Kingdom.

(2) The power under subsection (1) includes power—

(a) to amend or replace the definition of "the Data Protection Convention" in section 3;

(b) to amend Chapter 3 of Part 2 of this Act;

(c) to amend Part 4 of this Act;

(d) to make provision about the functions of the Commissioner, courts or tribunals in connection with processing of personal data to which Chapter 3 of Part 2 or Part 4 of this Act applies, including provision amending Parts 5 to 7 of this Act;

Ref. code: 25646301033624ADV

(e) to make provision about the functions of the Commissioner in connection with the Data Protection Convention or an instrument replacing that Convention, including provision amending Parts 5 to 7 of this Act;

(f) to consequentially amend this Act.

(3) Regulations under this section are subject to the affirmative resolution procedure.

(4) Regulations under this section may not be made after the end of the period of 3 years beginning with the day on which this Act is passed. Rights of the data subject

184 Prohibition of requirement to produce relevant records

(1) It is an offence for a person ("P1") to require another person to provide P1 with, or give P1 access to, a relevant record in connection with—

(a) the recruitment of an employee by P1,

(b) the continued employment of a person by P1, or

(c) a contract for the provision of services to P1.

(2) It is an offence for a person ("P2") to require another person to provide P2 with, or give P2 access to, a relevant record if—

(a) P2 is involved in the provision of goods, facilities or services to the public or a section of the public, and

(b) the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or to a third party.

(3) It is a defence for a person charged with an offence undersubsection (1) or (2) to prove that imposing the requirement—

(a) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(b) in the particular circumstances, was justified as being in the public interest.

(4) The imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc).

Ref. code: 25646301033624ADV

(5) In subsections (1) and (2), the references to a person who requires another person to provide or give access to a relevant record include a person who asks another person to do so—

(a) knowing that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request, or

(b) being reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request, and the references to a "requirement" in subsections (3) and (4) are to be interpreted accordingly.

(6) In this section—

"employment" means any employment, including—

(a) work under a contract for services or as an office-holder,

(b) work under an apprenticeship,

(c) work experience as part of a training course or in the course of training for employment, and

(d) voluntary work, and "employee" is to be interpreted accordingly;

" relevant record" has the meaning given in Schedule 18 and references to a relevant record include—

(a) a part of such a record, and

(b) a copy of, or of part of, such a record.

185 Avoidance of certain contractual terms relating to health records

(1) A term or condition of a contract is void in so far as it purports to require an individual to supply another person with a record which—

(a) consists of the information contained in a health record, and (b) has been or is to be obtained by a data subject in the exercise of a data subject access right.

(2) A term or condition of a contract is also void in so far as it purports to require an individual to produce such a record to another person.

Ref. code: 25646301033624ADV

(3) The references in subsections (1) and (2) to a record include a part of a record and a copy of all or part of a record.

(4) In this section, "data subject access right" means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).

186 Data subject's rights and other prohibitions and restrictions

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).

(2) The provisions providing obligations and rights are—

(a) Chapter III of the GDPR (rights of the data subject),

(b) Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and

(c) Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are—

(a) in Chapter 2 of Part 2 of this Act, sections 15 and 16 and Schedules 2, 3 and 4,

(b) in Chapter 3 of Part 2 of this Act, sections 23, 24, 25 and 26,

(c) in Part 3 of this Act, sections 44(4), 45(4) and 48(3), and

(d) in Part 4 of this Act, Chapter 6 .

Ref. code: 25646301033624ADV

Representation of data subjects

187 Representation of data subjects with their authority

(1) In relation to the processing of personal data to which the GDPR applies—

(a) Article 80(1) of the GDPR (representation of data subjects) enables a data subject to authorise a body or other organisation which meets the conditions set out in that Article to exercise the data subject's rights under Articles 77, 78 and 79 of the GDPR (rights to lodge complaints and to an effective judicial remedy) on the data subject's behalf, and

(b) a data subject may also authorise such a body or organisation to exercise the data subject's rights under Article 82 of the GDPR (right to compensation).

(2) In relation to the processing of personal data to which the GDPR does not apply, a body or other organisation which meets the conditions in subsections (3) and (4), if authorised to do so by a data subject, may exercise some or all of the following rights of a data subject on the data subject's behalf—

(a) rights under section 165(2), (4)(d) and (6)(c) (complaints to the Commissioner);

(b) rights under section 166(2) (orders for the Commissioner to progress complaints);

(c) rights under section 167(1) (compliance orders);

(d) the right to bring judicial review proceedings against the Commissioner.

(3) The first condition is that the body or organisation, by virtue of its constitution or an enactment—

(a) is required (after payment of outgoings) to apply the whole of its income and any capital it expends for charitable or public purposes,

(b) is prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and

(c) has objectives which are in the public interest.

(4) The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data.

Ref. code: 25646301033624ADV

(5) In this Act, references to a "representative body", in relation to a right of a data subject, are to a body or other organisation authorised to exercise the right on the data subject's behalf under Article 80 of the GDPR or this section.

188 Representation of data subjects with their authority: collective proceedings

(1) The Secretary of State may by regulations make provision for representative bodies to bring proceedings before a court or tribunal in England and Wales or Northern Ireland combining two or more relevant claims.

(2) In this section, "relevant claim", in relation to a representative body, means a claim in respect of a right of a data subject which the representative body is authorised to exercise on the data subject's behalf under Article 80(1) of the GDPR or section 187.

(3) The power under subsection (1) includes power—

(a) to make provision about the proceedings;

(b) to confer functions on a person, including functions involving the exercise of a discretion;

(c) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(4) The provision mentioned in subsection (3)(a) includes provision about—

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

(5) Regulations under this section are subject to the negative resolution procedure.

189 Duty to review provision for representation of data subjects

(1) Before the end of the review period, the Secretary of State must—

Ref. code: 25646301033624ADV

(a) review the matters listed in subsection (2) in relation to England and Wales and Northern Ireland,

(b) prepare a report of the review, and

(c) lay a copy of the report before Parliament.

(2) Those matters are—

(a) the operation of Article 80(1) of the GDPR,

(b) the operation of section 187,

(c) the merits of exercising the power under Article 80(2) of the GDPR (power to enable a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise some or all of a data subject's rights under Articles 77, 78 and 79 of the GDPR without being authorised to do so by the data subject),

(d) the merits of making equivalent provision in relation to data subjects' rights under Article 82 of the GDPR (right to compensation), and

(e) the merits of making provision for a children's rights organisation to exercise some or all of a data subject's rights under Articles 77, 78, 79 and 82 of the GDPR on behalf of a data subject who is a child, with or without being authorised to do so by the data subject.

(3) "The review period" is the period of 30 months beginning when section 187 comes into force.

(4) In carrying out the review, the Secretary of State must—

(a) consider the particular needs of children separately from the needs of adults,

(b) have regard to the fact that children have different needs at different stages of development,

(c) carry out an analysis of the particular challenges that children face in authorising, and deciding whether to authorise, other persons to act on their behalf under Article 80(1) of the GDPR or section 187,

(d) consider the support and advice available to children in connection with the exercise of their rights under Articles 77, 78, 79 and 82 of the GDPR by

Ref. code: 25646301033624ADV

another person on their behalf and the merits of making available other support or advice, and

(e) have regard to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

(5) Before preparing the report under subsection (1), the Secretary of State must consult the Commissioner and such other persons as the Secretary of State considers appropriate, including—

(a) persons active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data,

(b) children and parents,

(c) children's rights organisations and other persons who appear to the Secretary of State to represent the interests of children,

(d) child development experts, and

(e) trade associations.

(6) In this section—

"children's rights organisation" means a body or other organisation which—

(a) is active in representing the interests of children, and

(b) has objectives which are in the public interest;

"trade association" includes a body representing controllers or processors;

"the United Nations Convention on the Rights of the Child" means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention which are in force in relation to the United Kingdom), subject to any reservations, objections or interpretative declarations by the United Kingdom for the time being in force.

190 Post-review powers to make provision about representation of data subjects

(1) After the report under section 189(1) is laid before Parliament, the Secretary of State may by regulations—

Ref. code: 25646301033624ADV

(a) exercise the powers under Article 80(2) of the GDPR in relation to England and Wales and Northern Ireland,

(b) make provision enabling a body or other organisation which meets the conditions in Article 80(1) of the GDPR to exercise a data subject's rights under Article 82 of the GDPR in England and Wales and Northern Ireland without being authorised to do so by the data subject, and

(c) make provision described in section 189(2)(e) in relation to the exercise in England and Wales and Northern Ireland of the rights of a data subject who is a child.

(2) The powers under subsection (1) include power—

(a) to make provision enabling a data subject to prevent a body or other organisation from exercising, or continuing to exercise, the data subject's rights;

(b) to make provision about proceedings before a court or tribunal where a body or organisation exercises a data subject's rights;

(c) to make provision for bodies or other organisations to bring proceedings before a court or tribunal combining two or more claims in respect of a right of a data subject;

(d) to confer functions on a person, including functions involving the exercise of a discretion;

(e) to amend sections 166 to 168, 180, 187, 203, 205 and 206;

(f) to insert new sections and Schedules into Part 6 or 7 ;

(g) to make different provision in relation to England and Wales and in relation to Northern Ireland.

(3) The powers under subsection (1)(a) and (b) include power to make provision in relation to data subjects who are children or data subjects who are not children or both.

(4) The provision mentioned in subsection (2)(b) and (c) includes provision about—

(a) the effect of judgments and orders;

(b) agreements to settle claims;

(c) the assessment of the amount of compensation;

(d) the persons to whom compensation may or must be paid, including compensation not claimed by the data subject;

(e) costs.

(5) Regulations under this section are subject to the affirmative resolution procedure. Framework for Data Processing by Government

191 Framework for Data Processing by Government

(1) The Secretary of State may prepare a document, called the Framework for Data Processing by Government, which contains guidance about the processing of personal data in connection with the exercise of functions of—

(a) the Crown, a Minister of the Crown or a United Kingdom government department, and

(b) a person with functions of a public nature who is specified or described in regulations made by the Secretary of State.

(2) The document may make provision relating to all of those functions or only to particular functions or persons.

(3) The document may not make provision relating to, or to the functions of, a part of the Scottish Administration, the Welsh Government, a Northern Ireland Minister or a Northern Ireland department.

(4) The Secretary of State may from time to time prepare amendments of the document or a replacement document.

(5) Before preparing a document or amendments under this section, the Secretary of State must consult—

(a) the Commissioner, and

(b) any other person the Secretary of State considers it appropriate to consult.

(6) Regulations under subsection (1)(b) are subject to the negative resolution procedure.

(7) In this section, “Northern Ireland Minister” includes the First Minister and deputy

Ref. code: 25646301033624ADV

First Minister in Northern Ireland.

192 Approval of the Framework

(1) Before issuing a document prepared under section 191, the Secretary of State must lay it before Parliament.

(2) If, within the 40-day period, either House of Parliament resolves not to approve the document, the Secretary of State must not issue it.

(3) If no such resolution is made within that period—

(a) the Secretary of State must issue the document, and

(b) the document comes into force at the end of the period of 21 days beginning with the day on which it is issued.

(4) Nothing in subsection (2) prevents another version of the document being laid before Parliament.

(5) In this section, "the 40-day period" means—

(a) if the document is laid before both Houses of Parliament on the same day, the period of 40 days beginning with that day, or

(b) if the document is laid before the Houses of Parliament on different days, the period of 40 days beginning with the later of those days.

(6) In calculating the 40-day period, no account is to be taken of any period during which Parliament is dissolved or prorogued or during which both Houses of Parliament are adjourned for more than 4 days.

(7) This section applies in relation to amendments prepared under section 191 as it applies in relation to a document prepared under that section.

193 Publication and review of the Framework

(1) The Secretary of State must publish a document issued under section 192(3).

(2) Where an amendment of a document is issued under section 192(3), the Secretary of State must publish—

(a) the amendment, or

(b) the document as amended by it.

(3) The Secretary of State must keep under review the document issued under

Ref. code: 25646301033624ADV

section 192(3) for the time being in force.

(4) Where the Secretary of State becomes aware that the terms of such a document could result in a breach of an international obligation of the United Kingdom, the Secretary of State must exercise the power under section 191(4) with a view to remedying the situation.

194 Effect of the Framework

(1) When carrying out processing of personal data which is the subject of a document issued under section 192(3) which is for the time being in force, a person must have regard to the document.

(2) A failure to act in accordance with a provision of such a document does not of itself make a person liable to legal proceedings in a court or tribunal.

(3) A document issued under section 192(3), including an amendment or replacement document, is admissible in evidence in legal proceedings.

(4) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of any document issued under section 192(3) in determining a question arising in the proceedings if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the court or tribunal to be relevant to the question.

(5) In determining a question arising in connection with the carrying out of any of the Commissioner's functions, the Commissioner must take into account a provision of a document issued under section 192(3) if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.

Data-sharing: HMRC and reserve forces

195 Reserve forces: data-sharing by HMRC

(1) The Reserve Forces Act 1996 is amended as follows.

(2) After section 125 insert—

"**125A Supply of contact details by HMRC**

Ref. code: 25646301033624ADV

(1) This subsection applies to contact details for—

(a) a member of an ex-regular reserve force, or

(b) a person to whom section 66 (officers and former servicemen liable to recall) applies, which are held by HMRC in connection with a function of HMRC.

(2) HMRC may supply contact details to which subsection (1) applies to the Secretary of State for the purpose of enabling the Secretary of State—

(a) to contact a member of an ex-regular reserve force in connection with the person's liability, or potential liability, to be called out for service under Part 6;

(b) to contact a person to whom section 66 applies in connection with the person's liability, or potential liability, to be recalled for service under Part 7.

(3) Where a person's contact details are supplied under subsection (2) for a purpose described in that subsection, they may also be used for defence purposes connected with the person's service (whether past, present or future) in the reserve forces or regular services.

(4) In this section, "HMRC" means Her Majesty's Revenue and Customs.

125B Prohibition on disclosure of contact details supplied undersection 125A

(1) A person who receives information supplied under section 125A may not disclose it except with the consent of the Commissioners for Her Majesty's Revenue and Customs (which may be general or specific).

(2) A person who contravenes subsection (1) is guilty of an offence.

(3) It is a defence for a person charged with an offence under this section to prove that the person reasonably believed—

(a) that the disclosure was lawful, or

(b) that the information had already lawfully been made available to the public.

(4) Subsections (4) to (7) of section 19 of the Commissioners for Revenue and Customs Act 2005 apply to an offence under this section as they apply to an

Ref. code: 25646301033624ADV

offence under that section.

(5) Nothing in section 107 or 108 (institution of proceedings and evidence) applies in relation to an offence under this section.

125C Data protection

(1) Nothing in section 125A or 125B authorises the making of a disclosure which contravenes the data protection legislation.

(2) In this section, "the data protection legislation" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act)."

Offences

196 Penalties for offences

(1) A person who commits an offence under section 119 or 173 or paragraph 15 of Schedule 15 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding level 5 on the standard scale.

(2) A person who commits an offence under section 132, 144, 148, 170, 171 or 184 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to a fine.

(3) Subsections (4) and (5) apply where a person is convicted of an offence under section 170 or 184.

(4) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if—

(a) it has been used in connection with the processing of personal data, and

(b) it appears to the court to be connected with the commission of the offence, subject to subsection (5).

Ref. code: 25646301033624ADV

(5) If a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court must not make an order under subsection (4) without giving the person an opportunity to show why the order should not be made.

197 Prosecution

(1) In England and Wales, proceedings for an offence under this Act may be instituted only—

(a) by the Commissioner, or

(b) by or with the consent of the Director of Public Prosecutions.

(2) In Northern Ireland, proceedingsfor an offence under this Act may be instituted only—

(a) by the Commissioner, or

(b) by or with the consent of the Director of Public Prosecutions for Northern Ireland

(3) Subject to subsection (4), summary proceedings for an offence under section 173 (alteration etc of personal data to prevent disclosure) may be brought within the period of 6 months beginning with the day on which the prosecutor first knew of evidence that, in the prosecutor's opinion, was sufficient to bring the proceedings.

(4) Such proceedings may not be brought after the end of the period of 3 years beginning with the day on which the offence was committed.

(5) A certificate signed by or on behalf of the prosecutor and stating the day on which the 6 month period described in subsection (3) began is conclusive evidence of that fact.

(6) A certificate purporting to be signed as described in subsection (5) is to be treated as so signed unless the contrary is proved.

(7) In relation to proceedings in Scotland, section 136(3) of the Criminal Procedure (Scotland) Act 1995 (deemed date of commencement of proceedings) applies for the purposes of this section as it applies for the purposes of that section.

Ref. code: 25646301033624ADV

198 Liability of directors etc

(1) Subsection (2) applies where—

(a) an offence under this Act has been committed by a body corporate, and

(b) it is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of—

(i) a director, manager, secretary or similar officer of the body corporate, or

(ii) a person who was purporting to act in such a capacity.

(2) The director, manager, secretary, officer or person, as well as the body corporate, is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) Where the affairs of a body corporate are managed by its members, subsections (1) and (2) apply in relation to the acts and omissions of a member in connection with the member's management functions in relation to the body as if the member were a director of the body corporate.

(4) Subsection (5) applies where—

(a) an offence under this Act has been committed by a Scottish partnership, and

(b) the contravention in question is proved to have occurred with the consent or connivance of, or to be attributable to any neglect on the part of, a partner.

(5) The partner, as well as the partnership, is guilty of the offence and liable to be proceeded against and punished accordingly.

199 Recordable offences

(1) The National Police Records (Recordable Offences) Regulations 2000 (S.I. 2000/1139) have effect as if the offences under the following provisions were listed in the Schedule to the Regulations—

(a) section 119;

(b) section 132;

(c) section 144;

(d) section 148;

Ref. code: 25646301033624ADV

(e) section 170;

(f) section 171;

(g) section 173;

(h) section 184;

(i) paragraph 15 of Schedule 15.

(2) Regulations under section 27(4) of the Police and Criminal Evidence Act 1984 (recordable offences) may repeal subsection (1).

200 Guidance about PACE codes of practice

(1) The Commissioner must produce and publish guidance about how the Commissioner proposes to perform the duty under section 67(9) of the Police and Criminal Evidence Act 1984 (duty to have regard to codes of practice under that Act when investigating offences and charging offenders) in connection with offences under this Act.

(2) The Commissioner—

(a) may alter or replace the guidance, and

(b) must publish any altered or replacement guidance.

(3) The Commissioner must consult the Secretary of State before publishing guidance under this section (including any altered or replacement guidance).

(4) The Commissioner must arrange for guidance under this section (including any altered or replacement guidance) to be laid before Parliament.

The Tribunal

201 Disclosure of information to the Tribunal

(1) No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the First-tier Tribunal or the Upper Tribunal with information necessary for the discharge of—

(a) its functions under the data protection legislation, or

(b) its other functions relating to the Commissioner's acts and omissions.

(2) But this section does not authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

Ref. code: 25646301033624ADV

(3) Until the repeal of Part 1 of the Regulation of Investigatory Powers Act 2000 by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force, subsection (2) has effect as if it included a reference to that PAriticle

202 Proceedings in the First-tier Tribunal: contempt

(1) This section applies where—

(a) a person does something, or fails to do something, in relation to proceedings before the First-tier Tribunal—

(i) on an appeal under section 27, 79, 111 or 162, or

(ii) for an order under section 166, and

(b) if those proceedings were proceedings before a court having power to commit for contempt, the act or omission would constitute contempt of court.

(2) The First-tier Tribunal may certify the offence to the Upper Tribunal.

(3) Where an offence is certified under subsection (2), the Upper Tribunal may—

(a) inquire into the matter, and

(b) deal with the person charged with the offence in any manner in which it could deal with the person if the offence had been committed in relation to the Upper Tribunal.

(4) Before exercising the power under subsection (3)(b), the Upper Tribunal must—

(a) hear any witness who may be produced against or on behalf of the person charged with the offence, and

(b) hear any statement that may be offered in defence.

203 Tribunal Procedure Rules

(1) Tribunal Procedure Rules may make provision for regulating—

(a) the exercise of the rights of appeal conferred by section 27, 79, 111 or 162, and

(b) the exercise of the rights of data subjects under section 166, including their exercise by a representative body.

Ref. code: 25646301033624ADV

(2) In relation to proceedings involving the exercise of those rights, Tribunal Procedure Rules may make provision about—

(a) securing the production of material used for the processing of personal data, and

(b) the inspection, examination, operation and testing of equipment or material used in connection with the processing of personal data.

Interpretation

204 Meaning of "health professional" and "social work professional"

(1) In this Act, "health professional" means any of the following—

(a) a registered medical practitioner;

(b) a registered nurse or midwife;

(c) a registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);

(d) a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);

(e) a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);

(f) a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);

(g) a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England;

(h) a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 (S.I. 2010/231) (see article 3 of that Order);

(i) a registered person within the meaning of the Pharmacy (Northern Ireland) Order 1976 (S.I. 1976/1213 (N.I. 22)) (see Article 2 of that Order);

(j) a child psychotherapist;

(k) a scientist employed by a health service body as head of a department.

Ref. code: 25646301033624ADV

(2) In this Act, “social work professional” means any of the following—

(a) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);

(b) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);

(c) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (asp 8);

(d) a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.)).

(3) In subsection (1)(a) “registered medical practitioner” includes a person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section.

(4) In subsection (1)(k) “health service body” means any of the following—

(a) the Secretary of State in relation to the exercise of functions under section 2A or 2B of, or paragraph 7C, 8 or 12 of Schedule 1 to, the National Health Service Act 2006;

(b) a local authority in relation to the exercise of functions under section 2B or 111 of, or any of paragraphs 1 to 7B or 13 of Schedule 1 to, the National Health Service Act 2006;

(c) a National Health Service trust first established under section 25 of the National Health Service Act 2006;

(d) a Special Health Authority established under section 28 of the National Health Service Act 2006;

(e) an NHS foundation trust;

(f) the National Institute for Health and Care Excellence;

(g) the Health and Social Care Information Centre;

Ref. code: 25646301033624ADV

(h) a National Health Service trust first established under section 5 of the National Health Service and Community Care Act 1990;

(i) a Local Health Board established under section 11 of the National Health Service (Wales) Act 2006;

(j) a National Health Service trust first established under section 18 of the National Health Service (Wales) Act 2006;

(k) a Special Health Authority established under section 22 of the National Health Service (Wales) Act 2006;

(l) a Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(m) a Special Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(n) a National Health Service trust first established under section 12A of the National Health Service (Scotland) Act 1978;

(o) the managers of a State Hospital provided under section 102 of the National Health Service (Scotland) Act 1978;

(p) the Regional Health and Social Care Board established under section 7 of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I));

(q) a special health and social care agency established under the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 (S.I. 1990/247 (N.I. 3));

(r) a Health and Social Care trust established under Article 10 of the Health and Personal Social Services (Northern Ireland) Order 1991 (S.I. 1991/194 (N.I. 1)).

205 General interpretation

(1) In this Act—

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique

Ref. code: 25646301033624ADV

identification of that individual, such as facial images or dactyloscopic data;
"data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status;
"enactment" includes—

(a) an enactment passed or made after this Act,

(b) an enactment comprised in subordinate legislation,

(c) an enactment comprised in, or in an instrument made under, a Measure or Act of the National Assembly for Wales,

(d) an enactment comprised in, or in an instrument made under, an Act of the Scottish Parliament, and

(e) an enactment comprised in, or in an instrument made under, Northern Ireland legislation;

"genetic data" means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question;
"government department" includes the following (except in the expression "United Kingdom government department")—

(a) a part of the Scottish Administration;

(b) a Northern Ireland department;

(c) the Welsh Government;

(d) a body or authority exercising statutory functions on behalf of the Crown;

"health record" means a record which—

(a) consists of data concerning health, and

(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

"inaccurate", in relation to personal data, means incorrect or misleading as

Ref. code: 25646301033624ADV

to any matter of fact;

“international obligation of the United Kingdom” includes—

(a) an EU obligation, and

(b) an obligation that arises under an international agreement or arrangement to which the United Kingdom is a party;

“international organisation” means an organisation and its subordinate bodies governed by international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

“Minister of the Crown” has the same meaning as in the Ministers of the Crown Act 1975;

“publish” means make available to the public or a section of the public (and related expressions are to be read accordingly);

“subordinate legislation” has the meaning given in the Interpretation Act 1978;

“tribunal” means any tribunal in which legal proceedings may be brought;

“the Tribunal”, in relation to an application or appeal under this Act, means—

(a) the Upper Tribunal, in any case where it is determined by or under Tribunal Procedure Rules that the Upper Tribunal is to hear the application or appeal, or

(b) the First-tier Tribunal, in any other case.

(2) References in this Act to a period expressed in hours, days, weeks, months or years

are to be interpreted in accordance with Article 3 of Regulation (EEC, Euratom) No. 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods,

dates and time limits, except in—

(a) section 125(4), (7) and (8);

(b) section 161(3), (5) and (6);

(c) section 176(2);

Ref. code: 25646301033624ADV

(d) section 178(2);

(e) section 182(8) and (9);

(f) section 183(4);

(g) section 192(3), (5) and (6);

(h) section 197(3) and (4);

(i) paragraph 23(4) and (5) of Schedule 1;

(j) paragraphs 5(4) and 6(4) of Schedule 3;

(k) Schedule 5;

(l) paragraph 11(5) of Schedule 12;

(m) Schedule 15;

(and the references in section 5 to terms used in Chapter 2 or 3 of Part 2 do not include references to a period expressed in hours, days, weeks, months or years).

(3) Section 3(14)(b) (interpretation of references to Chapter 2 of Part 2 in Parts 5 to 7) and the amendments in Schedule 19 which make equivalent provision are not to be treated as implying a contrary intention for the purposes of section 20(2) of the Interpretation Act 1978, or any similar provision in another enactment, as it applies to other references to, or to a provision of, Chapter 2 of Part 2 of this Act.

206 Index of defined expressions

The Table below lists provisions which define or otherwise explain terms defined for this Act, for a Part of this Act or for Chapter 2 or 3 of Part 2 of this Act.

the affirmative resolution procedure	section 182
the applied Chapter 2 (in Chapter 3 of Part 2)	section 22
the applied GDPR	section 3
assessment notice (in Part 6)	section 181
biometric data	section 205
certification provider (in Part 6)	section 181
the Commissioner	section 3
competent authority (in Part 3)	section 30
consent (in Part 4)	section 84

Ref. code: 25646301033624ADV

controller	section 3
data concerning health	section 205
the Data Protection Convention	section 3
the data protection legislation	section 3
data subject	section 3
employee (in Parts 3 and 4)	sections 33 and 84
enactment	section 205
enforcement notice (in Part 6)	section 181
filing system	section 3
FOI public authority (in Chapter 3 of Part 2)	section 21
the GDPR	section 3
genetic data	section 205
government department	section 205
health professional	section 204
health record	section 205
identifiable living individual	section 3
inaccurate	section 205
information notice (in Part 6)	section 181
intelligence service (in Part 4)	section 82
international obligation of the United Kingdom	section 205
international organisation	section 205
the Law Enforcement Directive	section 3
the law enforcement purposes (in Part 3)	section 31
the made affirmative resolution procedure	section 182
Minister of the Crown	section 205
the negative resolution procedure	section 182
penalty notice (in Part 6)	section 181
penalty variation notice (in Part 6)	section 181
personal data	section 3
personal data breach (in Parts 3 and 4)	sections 33 and 84

Ref. code: 25646301033624ADV

processing	section 3
processor	section 3
profiling (in Part 3)	section 33
public authority (in the GDPR and Part 2)	section 7
public body (in the GDPR and Part 2)	section 7
publish	section 205
recipient (in Parts 3 and 4)	sections 33 and 84
representative (in Part 6)	section 181
representative body (in relation to a right of a data subject)	section 187
restriction of processing (in Parts 3 and 4)	sections 33 and 84
social work professional	section 204
the special purposes (in Part 6)	section 174
special purposes proceedings (in Part 6)	section 174
subordinate legislation	section 205
third country (in Part 3)	section 3
tribunal	section 205
the Tribunal	section 205

Territorial application

207 Territorial application of this Act

(1) This Act applies only to processing of personal data described in subsections (2) and(3).

(2) It applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the United Kingdom, whether or not the processing takes place in the United Kingdom.

(3) It also applies to the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—

(a) the processing is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a member State,

Ref. code: 25646301033624ADV

whether or not the processing takes place in such a country or territory,

(b) the personal data relates to a data subject who is in the United Kingdom when the processing takes place, and

(c) the processing activities are related to—

(i) the offering of goods or services to data subjects in the United Kingdom, whether or not for payment, or

(ii) the monitoring of data subjects' behaviour in the United Kingdom.

(4) Subsections(1) to (3) have effectsubject to any provision in or made undersection 120 providing for the Commissioner to carry out functions in relation to other processing of personal data.

(5) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (2).

(6) The reference in subsection (3) to Chapter 2 of Part 2 (the GDPR) does not include that Chapter as applied by Chapter 3 of Part 2 (the applied GDPR).

(7) In this section, references to a person who has an establishment in the United Kingdom include the following—

(a) an individual who is ordinarily resident in the United Kingdom,

(b) a body incorporated under the law of the United Kingdom or a part of the United Kingdom,

(c) a partnership or other unincorporated association formed under the law of the United Kingdom or a part of the United Kingdom, and

(d) a person not within paragraph (a), (b) or (c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangements in the United Kingdom, and references to a person who has an establishment in another country or territory have a corresponding meaning.

General

208 Children in Scotland

(1) Subsections (2) and (3) apply where a question falls to be determined in Scotland as to the legal capacity of a person aged under 16 to—

(a) exercise a right conferred by the data protection legislation, or

(b) give consent for the purposes of the data protection legislation.

(2) The person is to be taken to have that capacity where the person has a general understanding of what it means to exercise the right or give such consent.

(3) A person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown.

209 Application to the Crown

(1) This Act binds the Crown.

(2) For the purposes of the GDPR and this Act, each government department is to be treated as a person separate from the other government departments (to the extent that is not already the case).

(3) Where government departments are not able to enter into contracts with each other, a provision of the GDPR or this Act that would require relations between them to be governed by a contract (or other binding legal act) in writing is to be treated as satisfied if the relations are the subject of a memorandum of understanding between them.

(4) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by a person acting on behalf of the Royal Household, the Duchy of Lancaster or the Duchy of Cornwall, the controller in respect of that data for the purposes of the GDPR and this Act is—

(a) in relation to the Royal Household, the Keeper of the Privy Purse,

(b) in relation to the Duchy of Lancaster, such person as the Chancellor of the Duchy appoints, and

(c) in relation to the Duchy of Cornwall, such person as the Duke of Cornwall, or the possessor for the time being of the Duchy of Cornwall, appoints.

(5) Different persons may be appointed under subsection (4)(b) or (c) for different purposes.

(6) As regards criminal liability—

(a) a government department is not liable to prosecution under this Act;

Ref. code: 25646301033624ADV

(b) nothing in subsection (4) makes a person who is a controller by virtue of that subsection liable to prosecution under this Act;

(c) a person in the service of the Crown is liable to prosecution under the provisions of this Act listed in subsection (7).

(7) Those provisions are—

(a) section 119;

(b) section 170;

(c) section 171;

(d) section 173;

(e) paragraph 15 of Schedule 15.

210 Application to Parliament

(1) Parts 1, 2 and 5 to 7 of this Act apply to the processing of personal data by or on behalf of either House of Parliament.

(2) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Commons, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(3) Where the purposes for which and the manner in which personal data is, or is to be, processed are determined by or on behalf of the House of Lords, the controller in respect of that data for the purposes of the GDPR and this Act is the Corporate Officer of that House.

(4) Subsections (2) and (3) do not apply where the purposes for which and the manner in which the personal data is, or is to be, processed are determined by or on behalf of the Intelligence and Security Committee of Parliament.

(5) As regards criminal liability—

(a) nothing in subsection (2) or (3) makes the Corporate Officer of the House of Commons or the Corporate Officer of the House of Lordsliable to prosecution under this Act;

Ref. code: 25646301033624ADV

(b) a person acting on behalf of either House of Parliament is liable to prosecution under the provisions of this Act listed in subsection (6).

(6) Those provisions are—

(a) section 170;

(b) section 171;

(c) section 173;

(d) paragraph 15 of Schedule 15.

211 Minor and consequential provision

(1) In Schedule 19—

(a) Part 1 contains minor and consequential amendments of primary legislation;

(b) Part 2 contains minor and consequential amendments of other legislation;

(c) Part 3 contains consequential modifications of legislation;

(d) Part 4 contains supplementary provision.

(2) The Secretary of State may by regulations make provision that is consequential on any provision made by this Act.

(3) Regulations under subsection (2)—

(a) may include transitional, transitory or saving provision;

(b) may amend, repeal or revoke an enactment.

(4) The reference to an enactment in subsection (3)(b) does not include an enactment passed or made after the end of the Session in which this Act is passed.

(5) Regulations under this section that amend, repeal or revoke primary legislation are subject to the affirmative resolution procedure.

(6) Any other regulations under this section are subject to the negative resolution procedure.

(7) In this section, “primary legislation” means—

(a) an Act;

(b) an Act of the Scottish Parliament;

(c) a Measure or Act of the National Assembly for Wales;

(d) Northern Ireland legislation.

Ref. code: 25646301033624ADV

Final

212 Commencement

(1) Except as provided by subsections (2) and (3), this Act comes into force on such day as the Secretary of State may by regulations appoint.

(2) This section and the following provisions come into force on the day on which this Act is passed—

(a) sections 1 and 3;

(b) section 182;

(c) sections 204, 205 and 206;

(d) sections 209 and 210;

(e) sections 213(2), 214 and 215;

(f) any other provision of this Act so far as it confers power to make regulations or Tribunal Procedure Rules or is otherwise necessary for enabling the exercise of such a power on or after the day on which this Act is passed.

(3) The following provisions come into force at the end of the period of 2 months beginning when this Act is passed—

(a) section 124;

(b) sections 125, 126 and 127, so far as they relate to a code prepared under section 124;

(c) section 177;

(d) section 178 and Schedule 17;

(e) section 179.

(4) Regulations under this section may make different provision for different areas.

213 Transitional provision

(1) Schedule 20 contains transitional, transitory and saving provision.

(2) The Secretary of State may by regulations make transitional, transitory or saving provision in connection with the coming into force of any provision of this Act or with the GDPR beginning to apply, including provision amending or repealing a provision of Schedule 20.

Ref. code: 25646301033624ADV

(3) Regulations under this section that amend or repeal a provision of Schedule 20 are subject to the negative resolution procedure.

214 Extent

(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject to—

(a) subsections (2) to (5), and

(b) paragraph 12 of Schedule 12.

(2) Section 199 extends to England and Wales only.

(3) Sections 188, 189 and 190 extend to England and Wales and Northern Ireland only.

(4) An amendment, repeal or revocation made by this Act has the same extent in the United Kingdom as the enactment amended, repealed or revoked.

(5) This subsection and the following provisions also extend to the Isle of Man—

(a) paragraphs 332 and 434 of Schedule 19;

(b) sections 211(1), 212(1) and 213(2), so far as relating to those paragraphs.

(6) Where there is a power to extend a part of an Act by Order in Council to any of the Channel Islands, the Isle of Man or any of the British overseas territories, the power may be exercised in relation to an amendment or repeal of that part which is made by or under this Act.

215 Short title

This Act may be cited as the Data Protection Act 2018.

Ref. code: 25646301033624ADV

SCHEDULES

SCHEDULE 1

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA

PART 1

CONDITIONS RELATING TO EMPLOYMENT, HEALTH AND RESEARCH ETC

Employment, social security and social protection

1 (1) This condition is met if—

(a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and

(b) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

(3) In this paragraph—

"social security" includes any of the branches of social security listed in Article 3(1) of Regulation (EC) No. 883/2004 of the European Parliament and of the Council on the co-ordination of social security systems (asamended from time to time);

"social protection" includes an intervention described in Article 2(b) of Regulation (EC) 458/2007 of the European Parliament and of the Council of 25 April 2007 on the European system of integrated social protection statistics (ESSPROS) (as amended from time to time).

Health or social care purposes

2 (1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of—

(a) preventive or occupational medicine,

(b) the assessment of the working capacity of an employee,

(c) medical diagnosis,

Ref. code: 25646301033624ADV

(d) the provision of health care or treatment,

(e) the provision of social care, or

(f) the management of health care systems or services or social care systems or services

(3) See also the conditions and safeguards in Article 9(3) of the GDPR (obligations of secrecy) and section 11(1).

Public health

3 This condition is met if the processing—

(a) is necessary for reasons of public interest in the area of public health, and

(b) is carried out—

(i) by or under the responsibility of a health professional, or

(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

Research etc

4 This condition is met if the processing—

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes,

(b) is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and

(c) is in the public interest.

PART 2

SUBSTANTIAL PUBLIC INTEREST CONDITIONS

Requirement for an appropriate policy document when relying on conditions in this Part 5

(1) Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

Statutory etc and government purposes

Ref. code: 25646301033624ADV

6 (1) This condition is met if the processing—

(a) is necessary for a purpose listed in sub-paragraph (2), and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

(a) the exercise of a function conferred on a person by an enactment or rule of law;

(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

Administration of justice and parliamentary purposes

7 This condition is met if the processing is necessary—

(a) for the administration of justice, or

(b) for the exercise of a function of either House of Parliament.

Equality of opportunity or treatment

8 (1) This condition is met if the processing—

(a) is of a specified category of personal data, and

(b) is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained, subject to the exceptions in sub-paragraphs (3) to (5).

(2) In sub-paragraph (1), "specified" means specified in the following table—

Category of personal data	Groups of people (in relation to a category of personal data)
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health

Ref. code: 25646301033624ADV

Personal data concerning an individual's sexual orientation	People of different sexual orientation

(3) Processing does not meet the condition in sub-paragraph (1) if it is carried out for the purposes of measures or decisions with respect to a particular data subject.

(4) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(5) Processing does not meet the condition in sub-paragraph (1) if—

(a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),

(b) the notice gave the controller a reasonable period in which to stop processing such data, and

(c) that period has ended

Racial and ethnic diversity at senior levels of organisations

9 (1) This condition is met if the processing—

(a) is of personal data revealing racial or ethnic origin,

(b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally,

(c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and

(d) can reasonably be carried out without the consent of the data subject, subject to the exception in sub-paragraph (3).

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

Ref. code: 25646301033624ADV

(b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual—

(a) holds a position listed in sub-paragraph (5), or

(b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are—

(a) a director, secretary or other similar officer of a body corporate;

(b) a member of a limited liability partnership;

(c) a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6) In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in—

(a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised, or

(b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Preventing or detecting unlawful acts

10 (1) This condition is met if the processing—

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-

Ref. code: 25646301033624ADV

paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph—

"act" includes a failure to act;

"competent authority" has the same meaning as in Part 3 of this Act (see section 30).

Protecting the public against dishonesty etc

11 (1) This condition is met if the processing—

(a) is necessary for the exercise of a protective function,

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and

(c) is necessary for reasons of substantial public interest.

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against—

(a) dishonesty, malpractice or other seriously improper conduct,

(b) unfitness or incompetence,

(c) mismanagement in the administration of a body or association, or

(d) failures in services provided by a body or association.

Regulatory requirements relating to unlawful acts and dishonesty etc

12 (1) This condition is met if—

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or otherseriously improper conduct,

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

(c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph—

Ref. code: 25646301033624ADV

"act" includes a failure to act;

"regulatory requirement" means—

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or

(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

Journalism etc in connection with unlawful acts and dishonesty etc

13 (1) This condition is met if—

(a) the processing consists of the disclosure of personal data for the special purposes,

(b) it is carried out in connection with a matter described in sub-paragraph (2),

(c) it is necessary for reasons of substantial public interest,

(d) it is carried out with a view to the publication of the personal data by any person, and

(e) the controller reasonably believes that publication of the personal data would be in the public interest.

(2) The matters mentioned in sub-paragraph (1)(b) are any of the following (whether alleged or established)—

(a) the commission of an unlawful act by a person;

(b) dishonesty, malpractice or other seriously improper conduct of a person;

(c) unfitness or incompetence of a person;

(d) mismanagement in the administration of a body or association;

(e) a failure in services provided by a body or association.

(3) The condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(4) In this paragraph—

"act" includes a failure to act;

"the special purposes" means—

(a) the purposes of journalism;

Ref. code: 25646301033624ADV

(b) academic purposes;

(c) artistic purposes;

(d) literary purposes.

Preventing fraud

14 (1) This condition is met if the processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of—

(i) the disclosure of personal data by a person as a member of an anti-fraud organisation,

(ii) the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation, or

(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

Suspicion of terrorist financing or money laundering

15 This condition is met if the processing is necessary for the purposes of making adisclosure in good faith under either of the following—

(a) section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property);

(b) section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to suspicion of money laundering).

Support for individuals with a particular disability or medical condition

16 (1) This condition is met if the processing—

(a) is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,

(b) is of a type of personal data falling within sub-paragraph (2) which relates to an individual falling within sub-paragraph (3),

Ref. code: 25646301033624ADV

(c) is necessary for the purposes of—

(i) raising awareness of the disability or medical condition, or

(ii) providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other,

(d) can reasonably be carried out without the consent of the data subject, and

(e) is necessary for reasons of substantial public interest.

(2) The following types of personal data fall within this sub-paragraph—

(a) personal data revealing racial or ethnic origin;

(b) genetic data or biometric data;

(c) data concerning health;

(d) personal data concerning an individual's sex life or sexual orientation.

(3) An individual falls within this sub-paragraph if the individual is or has been a member of the body mentioned in sub-paragraph (1)(a) and—

(a) has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or

(b) is a relative or carer of an individual who satisfies paragraph (a) of this sub-paragraph.

(4) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

"carer" means an individual who provides or intends to provide care for another individual other than—

(a) under or by virtue of a contract, or

(b) as voluntary work;

"disability" has the same meaning as in the Equality Act 2010 (see section 6 of, and Schedule 1 to, that Act).

Ref. code: 25646301033624ADV

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Counselling etc

17 (1) This condition is met if the processing—

(a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially,

(b) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(c) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(b) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the service mentioned in sub-paragraph (1)(a).

Safeguarding of children and of individuals at risk

18 (1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

Ref. code: 25646301033624ADV

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Safeguarding of economic well-being of certain individuals

19 (1) This condition is met if the processing—

(a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over,

(b) is of data concerning health,

(c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

Ref. code: 25646301033624ADV

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) In this paragraph, "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

Insurance

20 (1) This condition is met if the processing—

(a) is necessary for an insurance purpose,

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

(c) is necessary for reasons of substantial public interest, subject to sub-paragraphs (2) and (3).

(2) Sub-paragraph (3) applies where—

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

(b) the data subject does not have and is not expected to acquire—

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or

(ii) other rights or obligations in connection with such a contract.

(3) Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

Ref. code: 25646301033624ADV

"insurance contract" means a contract of general insurance or long-term insurance;

"insurance purpose" means—

(a) advising on, arranging, underwriting or administering an insurance contract,

(b) administering a claim under an insurance contract, or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of "insurance contract" in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.

Occupational pensions

21 (1) This condition is met if the processing—

(a) is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme,

(b) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme,

(c) is not carried out for the purposes of measures or decisions with respect to the data subject, and

(d) can reasonably be carried out without the consent of the data subject.

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(3) In this paragraph—

"occupational pension scheme" has the meaning given in section 1 of the Pension Schemes Act 1993;

Ref. code: 25646301033624ADV

"member", in relation to a scheme, includes an individual who is seeking to become a member of the scheme.

(4) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Political parties

22 (1) This condition is met if the processing—

(a) is of personal data revealing political opinions,

(b) is carried out by a person or organisation included in the register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000, and

(c) is necessary for the purposes of the person's or organisation's political activities, subject to the exceptions in sub-paragraphs (2) and (3).

(2) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to a person.

(3) Processing does not meet the condition in sub-paragraph (1) if—

(a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),

(b) the notice gave the controller a reasonable period in which to stop processing such data, and

(c) that period has ended.

(4) In this paragraph, "political activities" include campaigning, fund-raising, political surveys and case-work.

Elected representatives responding to requests

23 (1) This condition is met if—

(a) the processing is carried out—

(i) by an elected representative or a person acting with the authority of such a representative,

Ref. code: 25646301033624ADV

(ii) in connection with the discharge of the elected representative's functions, and

(iii) in response to a request by an individual that the elected representative take action on behalf of the individual, and

(b) the processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative in response to that request, subject to sub-paragraph (2).

(2) Where the request is made by an individual other than the data subject, the condition in sub-paragraph (1) is met only if the processing must be carried out without the consent of the data subject for one of the following reasons—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

(3) In this paragraph, "elected representative" means—

(a) a member of the House of Commons;

(b) a member of the National Assembly for Wales;

(c) a member of the Scottish Parliament;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected in the United Kingdom;

(f) an elected member of a local authority within the meaning of section 270(1) of the Local Government Act 1972, namely—

(i) in England, a county council, a district council, a London borough council or a parish council;

(ii) in Wales, a county council, a county borough council or a community council;

Ref. code: 25646301033624ADV

(g) an elected mayor of a local authority within the meaning of Part 1A or 2 of the Local Government Act 2000;

(h) a mayor for the area of a combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009;

(i) the Mayor of London or an elected member of the London Assembly;

(j) an elected member of—

(i) the Common Council of the City of London, or

(ii) the Council of the Isles of Scilly;

(k) an elected member of a council constituted under section 2 of the Local Government etc (Scotland) Act 1994;

(l) an elected member of a district council within the meaning of the Local Government Act (Northern Ireland) 1972 (c. 9 (N.I.));

(m) a police and crime commissioner.

(4) For the purposes of sub-paragraph (3), a person who is—

(a) a member of the House of Commons immediately before Parliament is dissolved,

(b) a member of the National Assembly for Wales immediately before that Assembly is dissolved,

(c) a member of the Scottish Parliament immediately before that Parliament is dissolved, or

(d) a member of the Northern Ireland Assembly immediately before that Assembly is dissolved, is to be treated as if the person were such a member until the end of the fourth day after the day on which the subsequent general election in relation to that Parliament or Assembly is held.

(5) For the purposes of sub-paragraph (3), a person who is an elected member of the Common Council of the City of London and whose term of office comes to an end at the end of the day preceding the annual Wardmotes is to be treated as if he or she were such a member until the end of the fourth day after the day on which those Wardmotes are held.

Disclosure to elected representatives

24 (1) This condition is met if—

(a) the processing consists of the disclosure of personal data—

(i) to an elected representative or a person acting with the authority of such a representative, and

(ii) in response to a communication to the controller from that representative or person which was made in response to a request from an individual,

(b) the personal data is relevant to the subject matter of that communication, and

(c) the disclosure is necessary for the purpose of responding to that communication, subject to sub-paragraph (2).

(2) Where the request to the elected representative came from an individual other than the data subject, the condition in sub-paragraph (1) is met only if the disclosure must be made without the consent of the data subject for one of the following reasons—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) obtaining the consent of the data subject would prejudice the action taken by the elected representative;

(d) the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

(3) In this paragraph, "elected representative" has the same meaning as in paragraph 23.

Informing elected representatives about prisoners

25 (1) This condition is met if—

(a) the processing consists of the processing of personal data about a prisoner for the purpose of informing a member of the House of Commons, a member of the National Assembly for Wales or a member of the Scottish Parliament about the prisoner, and

Ref. code: 25646301033624ADV

(b) the member is under an obligation not to further disclose the personal data.

(2) The references in sub-paragraph (1) to personal data about, and to informing someone about, a prisoner include personal data about, and informing someone about, arrangements for the prisoner's release.

(3) In this paragraph—

"prison" includes a young offender institution, a remand centre, a secure training centre or a secure college;

"prisoner" means a person detained in a prison.

Publication of legal judgments

26 This condition is met if the processing—

(a) consists of the publication of a judgment or other decision of a court or tribunal, or

(b) is necessary for the purposes of publishing such a judgment or decision.

Anti-doping in sport

27 (1) This condition is met if the processing is necessary—

(a) for the purposes of measures designed to eliminate doping which are undertaken by or under the responsibility of a body or association that is responsible for eliminating doping in a sport, at a sporting event or in sport generally, or

(b) for the purposes of providing information about doping, or suspected doping, to such a body or association.

(2) The reference in sub-paragraph (1)(a) to measures designed to eliminate doping includes measures designed to identify or prevent doping.

(3) If the processing consists of the disclosure of personal data to a body or association described in sub-paragraph (1)(a), or is carried out in preparation for such disclosure,

the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule)

Standards of behaviour in sport

Ref. code: 25646301033624ADV

28 (1) This condition is met if the processing—

(a) is necessary for the purposes of measures designed to protect the integrity of a sport or a sporting event,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) In sub-paragraph (1)(a), the reference to measures designed to protect the integrity of a sport or a sporting event is a reference to measures designed to protect a sport or a sporting event against—

(a) dishonesty, malpractice or other seriously improper conduct, or

(b) failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or event.

PART 3

ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

Consent

29 This condition is met if the data subject has given consent to the processing.

Protecting individual's vital interests

30 This condition is met if—

(a) the processing is necessary to protect the vital interests of an individual, and

(b) the data subject is physically or legally incapable of giving consent. Processing by not-for-profit bodies

31 This condition is met if the processing is carried out—

(a) in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, and

(b) on condition that—

Ref. code: 25646301033624ADV

(i) 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

(ii) the personal data is not disclosed outside that body without the consent of the data subjects

Personal data in the public domain

32 This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Legal claims

33 This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Judicial acts

34 This condition is met if the processing is necessary when a court or tribunal is acting

in its judicial capacity. Administration of accounts used in commission of indecency offences involving children

35 (1) This condition is met if—

(a) the processing is of personal data about a conviction or caution for an offence listed in sub-paragraph (2),

(b) the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card, and

(c) when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) Those offences are an offence under—

Ref. code: 25646301033624ADV

(a) section 1 of the Protection of Children Act 1978 (indecent photographs of children),

(b) Article 3 of the Protection of Children (Northern Ireland) Order 1978 (S.I. 1978/1047 (N.I. 17)) (indecent photographs of children),

(c) section 52 of the Civic Government (Scotland) Act 1982 (indecent photographs etc of children),

(d) section 160 of the Criminal Justice Act 1988 (possession of indecent photograph of child),

(e) Article 15 of the Criminal Justice (Evidence etc) (Northern Ireland) Order 1988 (S.I. 1988/1847 (N.I. 17)) (possession of indecent photograph of child),

or

(f) section 62 of the Coroners and Justice Act 2009 (possession of prohibited images of children), or incitement to commit an offence under any of those provisions.

(3) See also the additional safeguards in Part 4 of this Schedule.

(4) In this paragraph—

"caution" means a caution given to a person in England and Wales or Northern Ireland in respect of an offence which, at the time when the caution is given, is admitted;

"conviction" has the same meaning as in the Rehabilitation of Offenders Act 1974 or the Rehabilitation of Offenders (Northern Ireland) Order 1978 (S.I. 1978/1908 (N.I. 27));

"payment card" includes a credit card, a charge card and a debit card. Extension of conditions in Part 2 of this Schedule referring to substantial public interest 36 This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.

Extension of insurance conditions

37 This condition is met if the processing—

(a) would meet the condition in paragraph 20 in Part 2 of this Schedule (the "insurance condition"), or

Ref. code: 25646301033624ADV

(b) would meet the condition in paragraph 36 by virtue of the insurance condition, but for the requirement for the processing to be processing of a category of personal data specified in paragraph 20(1)(b).

PART 4

APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

Application of this Part of this Schedule

38 This Part of this Schedule makes provision about the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of this Schedule which requires the controller to have an appropriate policy document in place when the processing is carried out.

Requirement to have an appropriate policy document in place

39 The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition described in paragraph 38 if the controller has produced a document which—

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained. Additional safeguard: retention of appropriate policy document

40 (1) Where personal data is processed in reliance on a condition described in paragraph 38, the controller must during the relevant period—

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, and

(c) make it available to the Commissioner, on request, without charge.

(2) "Relevant period", in relation to the processing of personal data in reliance on a condition described in paragraph 38, means a period which—

Ref. code: 25646301033624ADV

(a) begins when the controller starts to carry out processing of personal data in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out such processing.

Additional safeguard: record of processing

41 A record maintained by the controller, or the controller's representative, under Article 30 of the GDPR in respect of the processing of personal data in reliance on a condition described in paragraph 38 must include the following information—

(a) which condition is relied on,

(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in paragraph 39(b) and, if it is not, the reasons for not following those policies.

Ref. code: 25646301033624ADV

ภาคผนวก ค

PERSONAL DATA PROTECTION ACT 2012

PART 1

PRELIMINARY

Short title

1. This Act is the Personal Data Protection Act 2012.

Interpretation

2.—(1) In this Act, unless the context otherwise requires —

"advisory committee" means an advisory committee appointed under section 7;

" Appeal Committee" means a Data Protection Appeal Committee constituted under section 48P(4), read with the Seventh Schedule;

"Appeal Panel" means the Data Protection Appeal Panel established by section 48P(1);

" authorised officer", in relation to the exercise of any power or performance of any function or duty under any provision of this Act, means a person to whom the exercise of that power or performance of that function or duty under that provision has been delegated under section 38 of the Info-communications Media Development Authority Act 2016;

" Authority" means the Info-communications Media Development Authority established by section 3 of the Info-communications Media Development Authority Act 2016;

" benefit plan" means an insurance policy, a pension plan, an annuity, a provident fund plan or other similar plan;

" business" includes the activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his or her personal or domestic capacity;

" business contact information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes;

Ref. code: 25646301033624ADV

“Chief Executive”, in relation to the Authority, means the Chief Executive of the Authority appointed under section 40(2) of the Info-communications Media Development Authority Act 2016, and includes any individual acting in that capacity;

“Commission” means the person designated as the Personal Data Protection Commission under section 5 to be responsible for the administration of this Act;

“Commissioner” means the Commissioner for Personal Data Protection appointed under section 8(1)(a), and includes any Deputy Commissioner for Personal Data Protection or Assistant Commissioner for Personal Data Protection appointed under section 8(1)(b);

“credit bureau” means an organisation which —

(a) provides credit reports for gain or profit; or

(b) provides credit reports on a routine, non-profit basis as an ancillary part of a business carried on for gain or profit;

“credit report” means a communication, whether in written, oral or other form, provided to an organisation to assess the creditworthiness of an individual in relation to a transaction between the organisation and the individual;

“data intermediary” means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;

“derived personal data” —

(a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but

(b) does not include personal data derived by the organisation using any prescribed means or method;

“document” includes information recorded in any form;

“domestic” means related to home or family;

“education institution” means an organisation that provides education, including instruction, training or teaching, whether by itself or in association or collaboration with, or by affiliation with, any other person;

“employee” includes a volunteer;

Ref. code: 25646301033624ADV

“employment” includes working under an unpaid volunteer work relationship;

“evaluative purpose” means —

(a) the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates —

(i) for employment or for appointment to office;

(ii) for promotion in employment or office or for continuance in employment or office;

(iii) for removal from employment or office;

(iv) for admission to an education institution;

(v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits;

(vi) for selection for an athletic or artistic purpose; or

(vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;

(b) the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;

(c) the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or

(d) such other similar purposes as the Minister may prescribe;

“individual” means a natural person, whether living or deceased;

“inspector” means an individual appointed as an inspector under section 8(1)(b);

“investigation” means an investigation relating to —

(a) a breach of an agreement;

(b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a circumstance or conduct that may result in a remedy or relief being available under any law;

Ref. code: 25646301033624ADV

“national interest” includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs;

“organisation” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not —

(a) formed or recognised under the law of Singapore; or

(b) resident, or having an office or a place of business, in Singapore;

“personal data” means data, whether true or not, about an individual who can be identified —

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access;

“prescribed healthcare body” means a healthcare body prescribed for the purposes of the Second Schedule by the Minister charged with the responsibility for health;

“prescribed law enforcement agency” means an authority charged with the duty of investigating offences or charging offenders under written law, prescribed for the purposes of sections 21(4) and 26D(6) and the Second Schedule by the Minister charged with the responsibility for that authority;

“private trust” means a trust for the benefit of one or more designated individuals who are the settlor’s friends or family members;

“proceedings” means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —

(a) a breach of an agreement;

(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a wrong or a breach of a duty for which a remedy is claimed under any law;

“processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

(a) recording;

(b) holding;

Ref. code: 25646301033624ADV

(c) organisation, adaptation or alteration;

(d) retrieval;

(e) combination;

(f) transmission;

(g) erasure or destruction;

"public agency" includes —

(a) the Government, including any ministry, department, agency, or organ of State;

(b) any tribunal appointed under any written law; or

(c) any statutory body specified under subsection (2);

"publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event —

(a) at which the individual appears; and

(b) that is open to the public;

"relevant body" means the Commission, the Appeal Panel or any Appeal Committee;

" tribunal" includes a judicial or quasi-judicial body or a disciplinary, an arbitral or a mediatory body;

" user activity data", in relation to an organisation, means personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation;

"user-provided data", in relation to an organisation, means personal data provided by an individual to the organisation.

(2) The Minister may, by notification in the Gazette, specify any statutory body established under a public Act for a public function to be a public agency for the purposes of this Act.

Purpose

3. The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to

Ref. code: 25646301033624ADV

protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

Application of Act

4.—(1) Parts 3, 4, 5, 6, 6A and 6B do not impose any obligation on —

(a) any individual acting in a personal or domestic capacity;

(b) any employee acting in the course of his or her employment with an organisation;

(c) any public agency; or

(d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision.

(2) Parts 3, 4, 5, 6 (except sections 24 and 25), 6A (except sections 26C(3)(a) and 26E) and 6B do not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

(3) An organisation has the same obligation under this Act in respect of personal data processed on its behalf and for its purposes. by a data intermediary as if the personal data were processed by the organisation itself.

(4) This Act does not apply in respect of — (a) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or (b) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) apply in respect of personal data about an individual who has been dead for 10 years or less.

(5) Except where business contact information is expressly mentioned, Parts 3, 4, 5, 6 and 6A do not apply to business contact information

(6) Unless otherwise expressly provided in this Act — (a) nothing in Parts 3, 4, 5, 6, 6A and 6B affects any authority, right, privilege or immunity conferred, or obligation

Ref. code: 25646301033624ADV

or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation is not an excuse for contravening this Act; and (b) the provisions of other written law prevail to the extent that any provision of Parts 3, 4, 5, 6, 6A and 6B is inconsistent with the provisions of that other written law.

PART 2

PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION

Personal Data Protection Commission

5.—(1) The Info-communications Media Development Authority is designated as the Personal Data Protection Commission.

(2) The Personal Data Protection Commission is responsible for the administration of this Act.

Functions of Commission

6. The functions of the Commission are —

(a) to promote awareness of data protection in Singapore;

(b) to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection;

(c) to advise the Government on all matters relating to data protection;

(d) to represent the Government internationally on matters relating to data protection;

(e) to conduct research and studies and promote educational activities relating to data protection, including organizing and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;

(f) to manage technical cooperation and exchange in the area of data protection with other organisations, including foreign data protection

Ref. code: 25646301033624ADV

authorities and international or inter-governmental organisations, on its own behalf or on behalf of the Government;

(g) to administer and enforce this Act;

(h) to carry out functions conferred on the Commission under any other written law; and

(i) to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order in the Gazette.

Advisory committees

7.—(1) The Minister may appoint one or more advisory committees to provide advice to the Commission with regard to the performance of any of its functions under this Act.

(2) The Commission may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Act but is not bound by such consultation.

Delegation

8.—(1) The Commission may appoint, by name or office, from among public officers and the employees of the Authority —

(a) the Commissioner for Personal Data Protection; and

(b) such number of Deputy Commissioners for Personal Data Protection, Assistant Commissioners for Personal Data Protection and inspectors, as the Commission considers necessary.

(2) Where any function, duty or power of the Commission under this Act is delegated to the Commissioner under section 38 of the Info-communications Media Development Authority Act 2016 —

(a) the Commissioner must perform that function or duty, or exercise that power, in his or her name;

(b) the Commission must not perform that function or duty, or exercise that power, during the period when the delegation is in force; and

Ref. code: 25646301033624ADV

(c) the Commission must, as soon as practicable after the delegation, publish a notice of the delegation in the Gazette.

(3) In exercising any of the powers of enforcement under this Act, an authorised officer must on demand produce to the person against whom he or she is acting the authority issued to him or her by the Commission.

Conduct of proceedings

9.—(1) An individual appointed under section 8(1) or an employee of the Authority, who is authorised in writing by the Chief Executive of the Authority for the purpose of this section, may conduct, with the authorisation of the Public Prosecutor, proceedings in respect of an offence under this Act.

(2) A legal counsel of the Commission who is an advocate and solicitor may —

(a) appear in any civil proceedings involving the performance of any function or duty, or the exercise of any power, of the Commission under any written law; and

(b) make all applications and do all acts in respect of the civil proceedings on behalf of the Commission or an authorized officer.

Cooperation agreements

10.—(1) For the purposes of section 59, a cooperation agreement is an agreement for the purposes of —

(a) facilitating cooperation between the Commission and another regulatory authority in the performance of their respective functions in so far as those functions relate to data protection; and

(b) avoiding duplication of activities by the Commission and another regulatory authority, being activities involving the enforcement of data protection laws.

(2) A cooperation agreement may include provisions —

(a) to enable the Commission and the other regulatory authority to provide to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;

Ref. code: 25646301033624ADV

(b) to provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and

(c) to enable the Commission and the other regulatory authority to forbear to perform any of their respective functions in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

(3) The Commission must not provide any information to a foreign data protection body pursuant to a cooperation agreement unless it requires of, and obtains from, that body an undertaking in writing by it that it will comply with terms specified in that requirement, including terms that correspond to the provisions of any written law concerning the disclosure of that information by the Commission.

(4) The Commission may give an undertaking to a foreign data protection body that it will comply with terms specified in a requirement made of the Commission by the foreign data protection body to give such an undertaking where —

(a) those terms correspond to the provisions of any law in force in the country or territory in which the foreign data protection body is established, being provisions which concern the disclosure by the foreign data protection body of the information mentioned in paragraph (b); and

(b) compliance with the requirement is a condition imposed by the foreign data protection body for providing information in its possession to the Commission pursuant to a cooperation agreement.

(5) In this section —

"foreign data protection body" means a body in whom there are vested functions under the law of another country or territory with respect to the enforcement or the administration of provisions of law of that country or territory concerning data protection;

"regulatory authority" includes the Commission and any foreign data protection body

Ref. code: 25646301033624ADV

PART 3

GENERAL RULES WITH RESPECT TO PROTECTION OF AND ACCOUNTABILITY FOR PERSONAL DATA

Compliance with Act

11.—(1) In meeting its responsibilities under this Act, anorganisation must consider what a reasonable person would consider appropriate in the circumstances.

(2) An organisation is responsible for personal data in its possession or under its control.

(3) An organisation must designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation.

(5) An organisation must make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4).

(5A) Without limiting subsection (5), an organisation is deemed to have satisfied that subsection if the organisation makes available the business contact information of any individual mentioned in subsection (3) in any prescribed manner.

(6) The designation of an individual by an organisation under subsection (3) does not relieve the organisation of any of its obligations under this Act.

Policies and practices

12. An organisation must —

(a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;

(c) communicate to its staff information about the organisation's policies and practices mentioned in paragraph (a); and

Ref. code: 25646301033624ADV

(d) make information available on request about —

(i) the policies and practices mentioned in paragraph (a); and

(ii) the complaint process mentioned in paragraph (b)

PART 4

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Consent required

13. An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless —

(a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or

(b) the collection, use or disclosure (as the case may be) without the individual's consent is required or authorized under this Act or any other written law.

Provision of consent

14.—(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless —

(a) the individual has been provided with the information required under section 20; and

(b) the individual provided his or her consent for that purpose in accordance with this Act.

(2) An organisation must not —

(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or

(b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the

Ref. code: 25646301033624ADV

collection, use or disclosure of the personal data, or using deceptive or misleading practices.

(3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act.

(4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual include consent given, or deemed to have been given, by any person validly acting on that individual's behalf for the collection, use or disclosure of such personal data.

Deemed consent

15.—(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organization for a purpose if —

(a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and

(b) it is reasonable that the individual would voluntarily provide the data.

(2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organization to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.

(3) Without limiting subsection (2) and subject to subsection (9), an individual (P) who provides personal data to an organisation (A) with a view to P entering into a contract with A is deemed to consent to the following where reasonably necessary for the conclusion of the contract between P and A: (a) the disclosure of that personal data by A to another organisation (B); (b) the collection and use of that personal data by B; (c) the disclosure of that personal data by B to another organisation.

(4) Where an organisation collects personal data disclosed to it by B under subsection (3)(c), subsection (3)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (3)(a).

Ref. code: 25646301033624ADV

(5) Subsections (3) and (4) apply to personal data provided before 1 February 2021 by an individual to an organisation with a view to the individual entering into a contract with the organisation —

(a) on or after 1 February 2021; or

(b) which contract was entered into before 1 February 2021 and remains in force on that date, as if subsections (3) and (4) —

(c) were in force when the personal data was so provided; and

(d) had continued in force until 1 February 2021.

(6) Without limiting subsection (2) and subject to subsection (9), an individual (P) who enters into a contract with an organisation (A) and provides personal data to A pursuant or in relation to that contract is deemed to consent to the following:

(a) the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary —

(i) for the performance of the contract between P and A; or

(ii) for the conclusion or performance of a contract between A and B which is entered into at P's request, or which a reasonable person would consider to be in P's interest;

(b) the collection and use of that personal data by B, where the collection and use are reasonably necessary for any purpose mentioned in paragraph (a);

(c) the disclosure of that personal data by B to another organisation, where the disclosure is reasonably necessary for any purpose mentioned in paragraph (a).

(7) Where an organisation collects personal data disclosed to it by B under subsection (6)(c), subsection (6)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (6)(a).

(8) Subsections (6) and (7) apply to personal data provided before 1 February 2021 by an individual to an organisation in relation to a contract that the individual entered into before that date with the organisation, and which remains in force on that date, as if subsections (6) and (7) —

(a) were in force when the personal data was so provided; and

(b) had continued in force until 1 February 2021.

Ref. code: 25646301033624ADV

(9) Subsections (3), (4), (5), (6), (7) and (8) do not affect any obligation under the contract between P and A that specifies or restricts —

(a) the personal data provided by P that A may disclose to another organisation; or

(b) the purposes for which A may disclose the personal data provided by P to another organisation.

Deemed consent by notification

15A.—(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021.

(2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if —

(a) the organisation satisfies the requirements in subsection (4); and

(b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation.

(3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose.

(4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual —

(a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual;

(b) take reasonable steps to bring the following information to the attention of the individual:

(i) the organisation's intention to collect, use or disclose the personal data;

(ii) the purpose for which the personal data will be collected, used or disclosed;

(iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and

(c) satisfy any other prescribed requirements.

(5) The organisation must, in respect of the assessment mentioned in subsection (4)(a) —

(a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual;

(b) identify and implement reasonable measures to —

(i) eliminate the adverse effect;

(ii) reduce the likelihood that the adverse effect will occur; or

(iii) mitigate the adverse effect; and

(c) comply with any other prescribed requirements.

Withdrawal of consent

16.—(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his or her consent.

(3) An organisation must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal data about the individual, but this section does not affect any legal consequences arising from such withdrawal.

(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation must cease (and cause its data intermediaries and agents

Ref. code: 25646301033624ADV

to cease) collecting, using or disclosing the personal data (as the case may be) unless such collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or other written law.

Collection, use and disclosure without consent

17.—(1) An organisation may —

(a) collect personal data about an individual, without the individual's consent or from a source other than the individual, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 1 of the Second Schedule;

(b) use personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 2 of the Second Schedule; or

(c) disclose personal data about an individual without the individual's consent, in the circumstances or for the purposes, and subject to any condition, in the First Schedule or Part 3 of the Second Schedule.

(2) Unless otherwise provided under this Act, an organization may —

(a) collect personal data about an individual that the organisation receives by way of a disclosure to the organisation —

(i) on or after 1 February 2021 in accordance with subsection (1)(c); or

(ii) before 1 February 2021 in accordance with section 17(3) as in force before that date, for purposes consistent with the purpose of that disclosure, or for any purpose permitted by subsection (1)(a); or

(b) use or disclose personal data about an individual that —

(i) is collected by the organisation on or after 1 February 2021 in accordance with subsection (1)(a); or

(ii) was collected by the organisation before 1 February 2021 in accordance with section 17(1) as in force before that date, for purposes consistent with the purpose of that collection, or for any purpose permitted by subsection (1)(b) or (c), as the case may be.

Ref. code: 25646301033624ADV

Division 2 — Purpose

Limitation of purpose and extent

18. An organisation may collect, use or disclose personal data about an individual only for purposes —

(a) that a reasonable person would consider appropriate in the circumstances; and

(b) that the individual has been informed of under section 20, if applicable.

Personal data collected before 2 July 2014

19. Despite the other provisions in this Part, an organisation may use personal data about an individual collected before 2 July 2014 for the purposes for which the personal data was collected unless —

(a) consent for such use is withdrawn in accordance with section 16; or

(b) the individual, whether before, on or after 2 July 2014, has otherwise indicated to the organisation that he or she does not consent to the use of the personal data.

Notification of purpose

20.—(1) For the purposes of sections 14(1)(a) and 18(b), an organisation must inform the individual of —

(a) the purposes for the collection, use or disclosure of the personal data (as the case may be) on or before collecting the personal data;

(b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and

(c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

(2) An organisation, on or before collecting personal data about an individual from another organisation without the individual's consent, must provide the other

Ref. code: 25646301033624ADV

organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act.

(3) Subsection (1) does not apply if —

(a) the individual is deemed to have consented to the collection, use or disclosure (as the case may be) under section 15 or 15A; or

(b) the organisation collects, uses or discloses the personal data without the individual's consent in accordance with section 17.

(4) Despite subsection (3), an organisation must comply with subsection (5) on or before collecting, using or disclosing personal data about an individual for the purpose of or in relation to the organisation —

(a) entering into an employment relationship with the individual or appointing the individual to any office; or

(b) managing or terminating the employment relationship with or appointment of the individual.

(5) For the purposes of subsection (4), the organisation must inform the individual of the following:

(a) the purpose for which the organisation is collecting, using or disclosing (as the case may be) the personal data about the individual;

(b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure (as the case may be) on behalf of the organisation.

PART 5

ACCESS TO AND CORRECTION OF PERSONAL DATA

Access to personal data

21.—(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation must, as soon as reasonably possible, provide the individual with —

(a) personal data about the individual that is in the possession or under the control of the organisation; and

(b) information about the ways in which the personal data mentioned in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.

(3) Subject to subsection (3A), an organisation must not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information (as the case may be) could reasonably be expected to —

(a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

(b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

(c) reveal personal data about another individual;

(d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or

(e) be contrary to the national interest.

(3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.

(4) An organisation must not inform any individual under subsection (1)(b) that the organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made under this Act or any other written law without the individual's consent.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation must provide the individual with access to the personal data and

Ref. code: 25646301033624ADV

other information without the personal data or other information excluded under subsections (2), (3) and (4).

(6) Where —

(a) an individual makes a request under subsection (1) to an organisation on or after 1 February 2021; and

(b) the organisation, by reason of subsection (2) or (3), does not provide an individual with the individual's personal data or other information requested under subsection (1), the organisation must, within the prescribed time and in accordance with the prescribed requirements, notify the individual of the rejection.

(7) Where —

(a) an individual makes a request under subsection (1) to an organisation on or after 1 February 2021; and

(b) the organisation provides the individual, in accordance with subsection (5), with the individual's personal data or other information requested under subsection (1), the organisation must notify the individual of the exclusion, under subsection (2) or (3), of any of the personal data or other information so requested.

Correction of personal data

22.—(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation.

(2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation must —

(a) correct the personal data as soon as practicable; and

(b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organization does not need the corrected personal data for any legal or business purpose.

Ref. code: 25646301033624ADV

(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made.

(4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation must correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made.

(5) If no correction is made under subsection (2)(a) or (4), the organisation must annotate the personal data in its possession or under its control with the correction that was requested but not made.

(6) Nothing in this section requires an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion.

(7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule.

Preservation of copies of personal data

22A.—(1) Where —

(a) an individual, on or after 1 February 2021, makes a request under section 21(1)(a) to an organisation to provide personal data about the individual that is in the possession or under the control of the organisation; and

(b) the organisation refuses to provide that personal data, the organisation must preserve, for not less than the prescribed period, a copy of the personal data concerned.

(2) The organisation must ensure that the copy of the personal data it preserves for the purposes of subsection (1) is a complete and accurate copy of the personal data concerned

Ref. code: 25646301033624ADV

PART 6

CARE OF PERSONAL DATA

Accuracy of personal data

23. An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data —

(a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

(b) is likely to be disclosed by the organisation to another organisation.

Protection of personal data

24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent —

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

Retention of personal data

25. An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —

(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

Transfer of personal data outside Singapore

26.—(1) An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

Ref. code: 25646301033624ADV

(2) The Commission may, on the application of any organisation, by written notice exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) — (a) may be granted subject to such conditions as the Commission may specify in writing; and (b) need not be published in the Gazette and may be revoked at any time by the Commission. (4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

PART 6A

NOTIFICATION OF DATA BREACHES

Interpretation of this Part

26A. In this Part, unless the context otherwise requires —

"affected individual" means any individual to whom any personal data affected by a data breach relates;

"data breach", in relation to personal data, means —

(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or

(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Notifiable data breaches

26B.—(1) A data breach is a notifiable data breach if the data breach —

(a) results in, or is likely to result in, significant harm to an affected individual; or

(b) is, or is likely to be, of a significant scale.

(2) Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual —

(a) if the data breach is in relation to any prescribed personal

data or class of personal data relating to the individual; or

(b) in other prescribed circumstances.

(3) Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale —

(a) if the data breach affects not fewer than the prescribed number of affected individuals; or

(b) in other prescribed circumstances.

(4) Despite subsections (1), (2) and (3), a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach.

Duty to conduct assessment of data breach

26C.—(1) This section applies to a data breach that occurs on or after 1 February 2021.

(2) Subject to subsection (3), where an organisation has reason tobelieve that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

(3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation —

(a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and

(b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach.

(4) The organisation must carry out the assessment mentioned insubsection (2) or (3)(b) in accordance with any prescribed requirements.

Ref. code: 25646301033624ADV

Duty to notify occurrence of notifiable data breach

26D.—(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment.

(2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances.

(3) The notification under subsection (1) or (2) must contain, to the best of the knowledge and belief of the organisation at the time it notifies the Commission or affected individual (as the case may be), all the information that is prescribed for this purpose.

(4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Commission.

(5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation —

(a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or

(b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

(6) An organisation must not notify any affected individual in accordance with subsection (2) if —

(a) a prescribed law enforcement agency so instructs; or

(b) the Commission so directs.

Ref. code: 25646301033624ADV

(7) The Commission may, on the written application of an organisation, waive the requirement to notify an affected individual under subsection (2) subject to any conditions that the Commission thinks fit.

(8) An organisation is not, by reason only of notifying the Commission under subsection (1) or an affected individual under subsection (2), to be regarded as being in breach of —

(a) any duty or obligation under any written law or rule of law, or any contract, as to secrecy or other restriction on the disclosure of information; or

(b) any rule of professional conduct applicable to the organisation.

(9) Subsections (1) and (2) apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach.

Obligations of data intermediary of public agency

26E. Where an organisation —

(a) is a data intermediary processing personal data on behalf of and for the purposes of a public agency; and

(b) has reason to believe that a data breach has occurred in relation to that personal data, the organisation must, without undue delay, notify the public agency of the occurrence of the data breach.

PART 7

27. to 32. [Repealed by Act 40 of 2020]

PART 8

33. [Repealed by Act 40 of 2020]

34. [Repealed by Act 40 of 2020]

35. [Repealed by Act 40 of 2020]

PART 9

DO NOT CALL REGISTRY

Ref. code: 25646301033624ADV

Division 1 — Preliminary

Interpretation of this Part

36.—(1) In this Part, unless the context otherwise requires —

"calling line identity" means the telephone number or information identifying the sender;

"checker" means a person mentioned in section 43A(1);

"financial services" has the meaning given by section 2 of the Consumer Protection (Fair Trading) Act 2003;

" goods" means any personal property, whether tangible or intangible, and is deemed to include —

(a) chattels that are attached or intended to be attached to real property on or after delivery;

(b) financial products and credit, including credit extended solely on the security of land;

(c) any residential property; and

(d) a voucher;

"message" means any message, whether in sound, text, visual or other form;

"register" means any Do Not Call Register kept and maintained under section 39;

"send", in relation to a message, means —

(a) to send the message, cause the message to be sent, or authorise the sending of the message; or

(b) to make a voice call containing the message, cause a voice call containing the message to be made, or authorise the making of a voice call containing the message;

"sender", in relation to a message, means a person —

(a) who sends the message, causes the message to be sent, or authorises the sending of the message; or

(b) who makes a voice call containing the message, causes a voice call containing the message to be made, or authorises the making of a voice call

Ref. code: 25646301033624ADV

containing the message;

"services" includes —

(a) a service offered or provided that involves the addition to or maintenance, repair or alteration of goods or any residential property;

(b) a membership in any club or organisation if the club or organisation is a business formed to make a profit for its owners;

(c) the right to use time share accommodation under a time share contract; and

(d) financial services;

"Singapore telephone number" means —

(a) a telephone number, with 8 digits beginning with the digit "3", "6", "8" or "9", that is in accordance with the National Numbering Plan mentioned in regulation 12A of the Telecommunications (Class Licences) Regulations; or

(b) any other telephone numbers as may be prescribed;

"subscriber", in relation to a Singapore telephone number, means the subscriber of the telecommunications service to which the Singapore telephone number is allocated;

"time share accommodation" means any living accommodation, in Singapore or elsewhere, used or intended to be used (wholly or partly) for leisure purposes by a class of persons all of whom have rights to use, or participate in arrangements under which they may use, that accommodation or accommodation within a pool of accommodation to which that accommodation belongs;

"time share contract" means a contract which confers or purports to confer on an individual time share rights that are exercisable during a period of not less than 3 years;

"voice call" includes —

(a) a call that involves a recorded or synthetic voice; or

(b) in the case of a recipient with a disability (for example, a hearing impairment), a call that is equivalent to a voice call.

Ref. code: 25646301033624ADV

(2) For the purposes of this Part, a telecommunications service provider who merely provides a service that enables a specified message to be sent is, unless the contrary is proved, presumed not to have sent the message and not to have authorised the message to be sent.

(3) For the purposes of this Part, if a specified message is sent and at the relevant time the telecommunications device, service or network from which it was sent was controlled by a person without the knowledge of the owners or authorised users of the telecommunications device, service or network, the owners or authorised users are, unless the contrary is proved, presumed not to have sent the message and not to have authorised the sending of the message.

(4) In subsection (3), "control" means either physical control or control through the use of software or other means.

Meaning of "specified message"

37.—(1) Subject to subsection (5), for the purposes of this Part, a specified message is a message where, having regard to the following, it would be concluded that the purpose, or one of the purposes, of the message is an applicable purpose:

(a) the content of the message;

(b) the presentational aspects of the message;

(c) the content that can be obtained using the numbers, URLs or contact information (if any) mentioned in the message;

(d) if the telephone number from which the message is made is disclosed to the recipient (whether by calling line identity or otherwise), the content (if any) that can be obtained by calling that number.

(2) For the purposes of subsection (1), where the applicable purpose relates to offering, supplying, advertising or promoting any goods, service, land, interest in land, business opportunity or investment opportunity, it does not matter whether or not —

(a) the goods, service, land, interest or opportunity exists; or

(b) it is lawful to acquire the goods, service, land or interest or take up the opportunity.

Ref. code: 25646301033624ADV

(3) Subject to subsection (4), a person (A) who authorises another person (B) to offer, advertise or promote A's goods, services, land, interest or opportunity is deemed to have authorised the sending of any message sent by B that offers, advertises or promotes A's goods, services, land, interest or opportunity

(4) For the purposes of subsection (3), a person who takes reasonable steps to stop the sending of a message mentioned in that subsection is deemed not to have authorised the sending of the message.

(5) For the purposes of this Part, a specified message does not include any message mentioned in the Eighth Schedule.

(6) In this section, "applicable purpose" means a purpose specified in the Tenth Schedule.

Application of this Part

38. This Part applies to a specified message addressed to a Singapore telephone number where —

(a) the sender of the specified message is present in Singapore when the specified message is sent; or

(b) the recipient of the specified message is present in Singapore when the specified message is accessed.

Division 2 — Administration

Register

39.—(1) The Commission must cause to be kept and maintained one or more registers of Singapore telephone numbers, each known as a Do Not Call Register, for the purposes of this PAriticle

(2) Each register must be kept in such form and must contain such particulars as the Commission thinks fit.

(3) The Commission may authorise another person to maintain any register, on its behalf, subject to such conditions or restrictions as the Commission may think fit.

Ref. code: 25646301033624ADV

Applications

40.—(1) A subscriber may apply to the Commission, in the form and manner prescribed —

(a) to add his or her Singapore telephone number to a register; or

(b) to remove his or her Singapore telephone number from a register.

(2) Any person may apply to the Commission, in the form and manner required by the Commission, to confirm whether any Singapore telephone number is listed in a register.

Evidence

41. A certificate purporting to be signed by the Chief Executive of the Authority or an authorised officer and stating that a Singapore telephone number was or was not listed in a register at a date specified in the certificate is admissible as evidence of its contents in any proceedings.

Information on terminated Singapore telephone number

42.—(1) Every telecommunications service provider must report to the Commission, in the form and manner prescribed, all terminated Singapore telephone numbers.

(2) A telecommunications service provider which contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000.

(3) In this section, "terminated Singapore telephone number" means —

(a) a Singapore telephone number to which the following apply:

(i) the Singapore telephone number has been allocated to a subscriber;

(ii) the telecommunications service associated with the Singapore telephone number has been terminated by the subscriber or telecommunications service provider; and

(iii) the Singapore telephone number has not been allocated to a different subscriber; or

(b) any other telephone numbers and circumstances as may be prescribed.

Ref. code: 25646301033624ADV

(4) For the purpose of subsection (1), where —

(a) a Singapore telephone number has been allocated to a subscriber by a telecommunications service provider (called in this subsection the first provider);

(b) the telecommunications service associated with the Singapore telephone number has been terminated by the subscriber;

(c) the subscriber contracts for a telecommunications service associated with the Singapore telephone number with another telecommunications service provider (called in this subsection the subsequent provider);

(d) the telecommunications service mentioned in paragraph (c) has been terminated by the subscriber or the subsequent provider; and

(e) the Singapore telephone number has not subsequently been allocated to any subscriber, it is the responsibility of the first provider to satisfy subsection (1).

(5) Without affecting the obligations of the telecommunications service provider under subsections (1) to (4), the Commission must pay the prescribed fees to the telecommunications service provider for each terminated Singapore telephone number reported to the Commission in accordance with this section.

Division 3 — Specified message to Singapore telephone number

Duty to check register

43.—(1) Subject to section 48(2), a person must not send a specified message addressed to a Singapore telephone number unless the person has, at the time the person sends the specified message, valid confirmation that the Singapore telephone number is not listed in the relevant register.

(2) For the purposes of subsection (1), the person has valid confirmation that a Singapore telephone number is not listed in the relevant register in either of the following circumstances:

(a) the person has, within the prescribed duration before sending the specified message —

Ref. code: 25646301033624ADV

(i) made an application to the Commission under section 40(2) to confirm whether the Singapore telephone number is listed in the relevant register; and

(ii) received confirmation from the Commission that the Singapore telephone number is not listed in the relevant register;

(b) the person has obtained from a checker information that the Singapore telephone number is not listed in the relevant register (called in this section the relevant information) and has no reason to believe that, and is not reckless as to whether —

(i) the prescribed period in relation to the relevant information has expired; or

(ii) the relevant information is false or inaccurate.

(3) In subsection (2)(b)(i), "prescribed period", in relation to relevant information, means the prescribed period beginning after the date on which the checker received confirmation from the Commission, in response to the checker's application to the Commission under section 40(2), that a Singapore telephone number is not listed in the relevant register.

(4) A person does not contravene subsection (1) if the subscriber or user of the Singapore telephone number to which a specified message is sent —

(a) gave clear and unambiguous consent to the sending of the specified message to that Singapore telephone number; and

(b) the consent is evidenced in written or other form so as to be accessible for subsequent reference.

(5) For the purposes of this section and section 43A —

(a) where there is only one register kept or maintained under section 39, the relevant register refers to that register; and

(b) where there are 2 or more registers kept or maintained under section 39 for different types of specified messages, the relevant register refers to the register relevant for the particular type of specified message.

Ref. code: 25646301033624ADV

Duty of checkers

43A.—(1) This section applies to a person (called the checker) that, for reward, provides to another person (P) information on whether a Singapore telephone number is listed in the relevant register (called in this section the applicable information) for the purpose of P's compliance with section 43(1), other than —

(a) the Commission;

(b) an individual who is an employee of P; and

(c) an individual who is an employee or agent of a checker.

(2) A checker must —

(a) ensure that the applicable information provided to P is accurate; and

(b) provide the applicable information to P in accordance with any prescribed requirements.

(3) A checker is deemed to have complied with subsection (2)(a) if —

(a) the applicable information that the checker provides to P is in accordance with a reply from the Commission in response to the checker's application under section 40(2) and

(b) the checker provides the applicable information to P before the expiry of the prescribed period mentioned in section 43(2)(b)(i).

Contact information

44. Subject to section 48(2), a person must not send a specified message addressed to a Singapore telephone number unless —

(a) the specified message includes clear and accurate information identifying the individual or organization that sent or authorised the sending of the specified message;

(b) the specified message includes clear and accurate information about how the recipient can readily contact that individual or organisation;

(c) the specified message includes the information, and complies with the conditions, specified in the regulations, if any; and

Ref. code: 25646301033624ADV

(d) the information included in the specified message in compliance with this section is reasonably likely to be valid for at least 30 days after the message is sent.

Calling line identity not to be concealed

45. Subject to section 48(3), a person that makes a voice call containing a specified message or causes a voice call containing a specified message to be made or authorises the making of a voice call containing a specified message, addressed to a Singapore telephone number, from a telephone number or fax number, must not do any of the following:

(a) conceal or withhold from the recipient the calling line identity of the sender;

(b) perform any operation or issue any instruction in connection with the sending of the specified message for the purpose of, or that has the effect of, concealing or withholding from the recipient the calling line identity of the sender.

Consent

46.—(1) A person must not, as a condition for supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that Singapore telephone number or any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user, and any consent given in such circumstance is not validly given.

(2) If a person obtains or attempts to obtain consent for sending a specified message to a Singapore telephone number —

(a) by providing false or misleading information with respect to the sending of the specified message; or

(b) by using deceptive or misleading practices, any consent given in such circumstances is not validly given.

Ref. code: 25646301033624ADV

Withdrawal of consent

47.—(1) On giving notice, a subscriber or user of a Singapore telephone number may at any time withdraw any consent given to a person for the sending of any specified message to that Singapore telephone number.

(2) A person must not prohibit a subscriber or user of a Singapore telephone number from withdrawing the subscriber's or user's consent to the sending of a specified message to that Singapore telephone number, but this section does not affect any legal consequences arising from such withdrawal.

(3) If a subscriber or user of a Singapore telephone number gives notice withdrawing consent given to a person for the sending of any specified message to that Singapore telephone number, the person must cease (and cause its agent to cease) sending any specified message to that Singapore telephone number after the expiry of the prescribed period.

(4) For the purposes of this Part, a subscriber or user of a Singapore telephone number is deemed to have given his or her consent to a person to send a specified message to that Singapore telephone number if the subscriber or user —

(a) consents to the sending of the specified message before 2 January 2014; and

(b) that consent has not been withdrawn on or after 2 January 2014.

(5) For the purposes of this Part, where a subscriber or user of a Singapore telephone number —

(a) consents to a person sending a specified message to that Singapore telephone number before, on or after 2 January 2014; and

(b) subsequently applies to add or adds that Singapore telephone number to the register on or after 2 January 2014, the application to add or the addition of that Singapore telephone number is not to be regarded as a withdrawal of the consent.

(6) To avoid doubt, a subscriber of a Singapore telephone number may, at any time on or after 2 January 2014, withdraw any consent given for the sending of a specified message to that Singapore telephone number.

Ref. code: 25646301033624ADV

Defence for employee

48.—(1) In any proceedings for an offence under this Part brought against any employee in respect of an act or conduct alleged to have been done or engaged in (as the case may be) by the employee, it is a defence for the employee to prove that he or she did the act or engaged in the conduct in good faith —

(a) in the course of his or her employment; or

(b) in accordance with instructions given to him or her by or on behalf of his or her employer in the course of his or her employment.

(2) Section 43(1) or 44 does not apply to an employee (X) who sends a specified message addressed to a Singapore telephone number in good faith —

(a) in the course of X's employment; or

(b) in accordance with instructions given to X by or on behalf of X's employer in the course of X's employment.

(3) Section 45 does not apply to an employee (Y) who makes, causes to be made or authorises the making of a voice call containing a specified message, addressed to a Singapore telephone number, from a telephone number or fax number, in good faith —

(a) in the course of Y's employment; or

(b) in accordance with instructions given to Y by or on behalf of Y's employer in the course of Y's employment.

(4) Subsection (1), (2) or (3) does not apply to an employee (Z) who, at the time the act was done or the conduct was engaged in, was an officer or a partner of Z's employer and it is proved that —

(a) Z knew or ought reasonably to have known that the telephone number is a Singapore telephone number listed in the relevant register; and

(b) the specified message was sent with Z's consent or connivance, or the sending of the specified message was attributable to any neglect on Z's pAriticle

(5) In this section —

"corporation" has the meaning given by section 52(7);

Ref. code: 25646301033624ADV

"officer" —

(a) in relation to a corporation, has the meaning given by section 52(7); or

(b) in relation to an unincorporated association (other than a partnership), has the meaning given by section 52A(7);

"partner", in relation to a partnership, has the meaning given by section 52A(7).

PART 9A

DICTIONARY ATTACKS AND ADDRESS-HARVESTING SOFTWARE

Interpretation of this Part

48A.—(1) In this Part, unless the context otherwise requires —

" address-harvesting software" means software that is specifically designed or marketed for use for —

(a) searching the Internet for telephone numbers; and

(b) collecting, compiling, capturing or otherwise harvesting those telephone numbers;

" applicable message" means a message with a Singapore link that is sent to any applicable telephone number;

"applicable telephone number" means a telephone number that is generated or obtained through the use of —

(a) a dictionary attack; or

(b) address-harvesting software;

" dictionary attack" means the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations;

"message", "send", "sender" and "Singapore telephone number" have the meanings given by section 36(1).

(2) In this Part, an applicable message has a Singapore link in any of the following circumstances:

(a) the message originates in Singapore;

Ref. code: 25646301033624ADV

(b) the sender of the message —

(i) where the sender is an individual — is physically present in Singapore when the message is sent; or

(ii) in any other case —

(A) is formed or recognised under the law of Singapore; or

(B) has an office or a place of business in Singapore;

(c) the telephone, mobile telephone or other device that is used to access the message is located in Singapore;

(d) the recipient of the message —

(i) where the recipient is an individual — is physically present in Singapore when the message is accessed; or

(ii) in any other case — carries on business or activities in Singapore when the message is accessed;

(e) if the message cannot be delivered because the telephone number to which the message is sent has ceased to exist (assuming that the telephone number existed), it is reasonably likely that the message would have been accessed using a telephone, mobile telephone or other device located in Singapore.

(3) For the purposes of the definition of "applicable message" in subsection (1), it does not matter —

(a) whether the telephone number to which the message is sent is a Singapore telephone number;

(b) whether that telephone number exists; or

(c) whether the message reaches its intended destination.

(4) For the purposes of this Part, a telecommunications service provider that merely provides a service that enables an applicable message to be sent is, unless the contrary is proved, presumed not to have sent, caused to be sent or authorised the sending of the applicable message.

Ref. code: 25646301033624ADV

(5) For the purposes of this Part, if, at the time an applicable message is sent, the telecommunications device, service or network from which it was sent was controlled by a person without the knowledge of the owner or authorised user of the telecommunications device, service or network (as the case may be), the owner or authorised user (as the case may be) is, unless the contrary is proved, presumed not to have sent, caused to be sent or authorised the sending of the applicable message.

(6) In subsection (5), "control" means —

(a) physical control; or

(b) control through the use of software or other means.

Prohibition on use of dictionary attacks and address-harvesting software

48B.—(1) Subject to subsections (2) and (3), a person must not send, cause to be sent or authorise the sending of an applicable message.

(2) Subsection (1) does not apply to an employee (P) who sends, causes to be sent or authorises the sending of an applicable message in good faith —

(a) in the course of P's employment; or

(b) in accordance with instructions given to P by or on behalf of P's employer in the course of P's employment.

(3) However, subsection (2) does not apply to a person (P) who, at the time the applicable message was sent, was an officer or a partnerof the sender and it is proved that —

(a) P knew or ought reasonably to have known that the telephone number is an applicable telephone number; and

(b) the applicable message was sent with P's consent or connivance, or the sending of the applicable message was attributable to any neglect on P's pAriticle

(4) In this section —

"corporation" has the meaning given by section 52(7);

"officer" —

Ref. code: 25646301033624ADV

(a) in relation to a corporation, has the meaning given by section 52(7); or

(b) in relation to an unincorporated association (other than a partnership), has the meaning given by section 52A(7);

"partner", in relation to a partnership, has the meaning given by section 52A(7).

PART 9B

OFFENCES AFFECTING PERSONAL DATA AND ANONYMISED INFORMATION

Interpretation and application of this Part

48C.—(1) In this Part, unless the context otherwise requires —

"disclose", in relation to personal data, includes providing access to personal data;

"gain" means —

(a) a gain in property or a supply of services, whether temporary or permanent; or

(b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration;

"harm", in relation to an individual, means —

(a) any physical harm; or

(b) harassment, alarm or distress caused to the individual;

"loss" means —

(a) a loss in property or a supply of services, whether temporary or permanent; or

(b) a loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration, but excludes, in relation to an individual, the loss of personal data about the individual;

"Monetary Authority of Singapore" means the Monetary Authority of Singapore established by section 3 of the Monetary Authority of Singapore Act 1970;

"relevant public official" has the meaning given by section 7(7) of the Public Sector (Governance) Act 2018;

Ref. code: 25646301033624ADV

"Singapore public sector agency" has the meaning given by section 2(1) of the Public Sector (Governance) Act 2018.

(2) This Part does not apply to an individual who —

(a) at the time of the commission of any offence under section 48D(1), 48E(1) or 48F(1), is a relevant public official in a Singapore public sector agency; or

(b) is or has been a director or an officer or employee of the Monetary Authority of Singapore in respect of the disclosure, use or re-identification of information acquired in the performance of the individual's duties or the exercise of the individual's functions.

Unauthorised disclosure of personal data

48D.—(1) If —

(a) an individual discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person;

(b) the disclosure is not authorised by the organisation or

public agency, as the case may be; and

(c) the individual does so —

(i) knowing that the disclosure is not authorised by the organisation or public agency, as the case may be; or

(ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency, as the case may be, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following:

(a) that —

(i) the personal data in the possession or under the control of the organisation or public agency (as the case may be) that was disclosed was, at the time of the disclosure, publicly available; and

(ii) where the personal data was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) that the accused disclosed, or caused the disclosure of, personal data in the possession or under the control of the organisation or public agency, as the case may be —

(i) as permitted or required by or under an Act or other law (apart from this Act);

(ii) as authorised or required by an order of court;

(iii) in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so; or

(iv) in any other circumstances, or for any other purpose, prescribed.

(3) To avoid doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the disclosure of personal data in the possession or under the control of an organisation or a public agency (as the case may be) by or under any other written law or other law.

(4) In this section, "applicable contravention" means a contravention of any of the following:

(a) subsection (1);

(b) section 48F(1);

(c) section 7(1) or 8(1) of the Public Sector (Governance) Act 2018;

(d) section 14A(1) or 14C(1) of the Monetary Authority of Singapore Act 1970.

Improper use of personal data

48E.—(1) If —

(a) an individual makes use of personal data in the possession or under the control of an organisation or a public agency;

Ref. code: 25646301033624ADV

(b) the use is not authorised by the organisation or public agency, as the case may be;

(c) the individual does so —

(i) knowing that the use is not authorised by the organisation or public agency, as the case may be; or

(ii) reckless as to whether the use is or is not authorized by the organisation or public agency, as the case may be; and

(d) the individual, as a result of that use —

(i) obtains a gain for the individual or another person;

(ii) causes harm to another individual; or

(iii) causes a loss to another person, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following:

(a) that —

(i) the personal data in the possession or under the control of the organisation or public agency (as the case may be) that was used was, at the time of the use, publicly available; and

(ii) where the personal data was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) that the accused used the personal data in the possession or under the control of the organisation or public agency, as the case may be —

(i) as permitted or required by or under an Act or other law (apart from this Act);

(ii) as authorised or required by an order of court;

(iii) in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so; or

(iv) in any other circumstances, or for any other purpose, prescribed.

Ref. code: 25646301033624ADV

(3) To avoid doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the use of personal data in the possession or under the control of an organisation or a public agency (as the case may be) by or under any other written law or other law. [40/2020] (4) In this section, "applicable contravention" means a contravention of any of the following: (a) section 48D(1) or 48F(1); (b) section 7(1) or 8(1) of the Public Sector (Governance) Act 2018; (c) section 14A(1) or 14C(1) of the Monetary Authority of Singapore Act 1970.

Unauthorised re-identification of anonymised information

48F.—(1) If —

(a) an individual takes any action to re-identify or cause re-identification of the person to whom anonymized information in the possession or under the control of an organisation or a public agency relates (called in this section the affected person);

(b) the re-identification is not authorised by the organisation or public agency, as the case may be; and

(c) the individual does so —

(i) knowing that the re-identification is not authorized by the organisation or public agency, as the case may be; or

(ii) reckless as to whether the re-identification is or is not authorised by the organisation or public agency, as the case may be, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following:

(a) that —

(i) the information on the identity of the affected person is publicly available; and

Ref. code: 25646301033624ADV

(ii) where that information was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) the action to re-identify or cause re-identification is —

(i) permitted or required by or under an Act or other law (apart from this Act); or

(ii) authorised or required by an order of court;

(c) the accused —

(i) reasonably believed that the re-identification was for a specified purpose; and

(ii) notified the Commission or the organisation or public agency (as the case may be) of the re-identification as soon as was practicable;

(d) the accused took the action to re-identify or cause re-identification in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so, other than for a specified purpose;

(e) in any other circumstances, or for any other purpose, prescribed.

(3) To avoid doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the re-identification of the affected person by or under any other written law or other law.

(4) In this section — "applicable contravention" means a contravention of any of the following: (a) subsection (1); (b) section 8(1) of the Public Sector (Governance) Act 2018; (c) section 14C(1) of the Monetary Authority of Singapore Act 1970; "specified purpose" means any purpose specified in the Eleventh Schedule.

PART 9C

ENFORCEMENT

Alternative dispute resolution

48G.—(1) If the Commission is of the opinion that any complaint by an individual (called in this section the complainant) against an organisation may more appropriately be resolved by mediation, the Commission may, without the consent

of the complainant and the organisation, refer the matter to mediation under a dispute resolution scheme.

(2) Subject to subsection (1), the Commission may, with or without the consent of the complainant and the organisation, direct the complainant or the organisation or both to attempt to resolve the complaint of the complainant in the way directed by the Commission.

(3) For the purposes of subsection (1), the Commission may establish or approve one or more dispute resolution schemes for the resolution of complaints by individuals against organisations.

(4) The Commission may, with the approval of the Minister, make regulations under section 65 to provide for matters relating to the operation by an operator of a dispute resolution scheme, including —

(a) the standards or requirements of the services provided under the dispute resolution scheme;

(b) the fees that the operator may charge for the services provided under the dispute resolution scheme;

(c) the records that the operator must keep, and the period of retention of those records;

(d) the reports that the operator must submit to the Commission, and the manner and time for those submissions;

(e) matters relating to the administration of the dispute resolution scheme; and

(f) generally to give effect to or for carrying out the purposes of subsections (1) and (3).

Power to review

48H.—(1) On the application of a complainant, the Commission may review —

(a) a refusal by an organisation to provide access to personal data or other information requested by the complainant under section 21, or the organisation's failure to provide that access within a reasonable time;

Ref. code: 25646301033624ADV

(b) a refusal by an organisation to correct personal data in accordance with a request by the complainant under section 22, or the organisation's failure to make the correction within a reasonable time;

(c) a refusal by a porting organisation to transmit any applicable data pursuant to a data porting request under section 26H, or the porting organisation's failure to transmit the applicable data within a reasonable time;

(d) a fee required from the complainant by an organisation in relation to a request by the complainant under section 21 or 22; or

(e) a fee required from the complainant or a receiving organisation by a porting organisation in relation to a data porting request by the complainant under section 26H.

(2) Upon completion of its review under subsection (1), the Commission may —

(a) confirm the refusal to provide access to the personal data or other information, or direct the organisation to provide access to the personal data or other information within the time specified by the Commission;

(b) confirm the refusal to correct the personal data, or direct the organisation to correct the personal data in the manner and within the time specified by the Commission;

(c) confirm the refusal to transmit the applicable data, or direct the porting organisation to transmit the applicable data in the manner and within the time specified by the Commission; or

(d) confirm, reduce or disallow a fee, or direct the organization or porting organisation (as the case may be) to make a refund to the complainant or receiving organisation, as the case may be.

Directions for non-compliance

48I.—(1) The Commission may, if it is satisfied that —

(a) an organisation has not complied or is not complying with any provision of Part 3, 4, 5, 6, 6A or 6B; or

(b) a person has not complied or is not complying with any provision of Part 9 or section 48B(1), give the organisation or person (as the case may be) any direction that the Commission thinks fit in the circumstances to ensure compliance with that provision.

(2) Without limiting subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with any provision of Part 3, 4, 5, 6, 6A or 6B, give an organisation all or any of the following directions:

(a) to stop collecting, using or disclosing personal data in contravention of this Act;

(b) to destroy personal data collected in contravention of this Act;

(c) to comply with any direction of the Commission under section 48H(2).

[40/2020]

Financial penalties

48J.—(1) Subject to subsection (2), the Commission may, if it is satisfied that —

(a) an organisation has intentionally or negligently contravened any provision of Part 3, 4, 5, 6, 6A or 6B; or

(b) a person has intentionally or negligently contravened —

(i) any provision of Part 9; or

(ii) section 48B(1), require, by written notice, the organisation or person (as the case may be) to pay a financial penalty.

(2) Subsection (1) does not apply in relation to any contravention of a provision of this Act, the breach of which is an offence under this Act.

(3) A financial penalty imposed on an organisation under subsection (1)(a) must not exceed the maximum amount to be prescribed, which in no case may be more than $1 million.

Ref. code: 25646301033624ADV

(4) A financial penalty imposed on a person under subsection (1)(b) must not exceed the maximum amount to be prescribed, which in no case may be more than the following:

(a) in the case of an individual — $200,000;

(b) in any other case — $1 million.

(5) For the purposes of subsections (3) and (4), different maximum amounts may be prescribed in respect of contraventions of different provisions of this Act.

(6) The Commission must, in determining the amount of a financial penalty imposed under subsection (1), have regard to, and give such weight as the Commission considers appropriate to, all of the following matters:

(a) the nature, gravity and duration of the non-compliance by the organisation or person, as the case may be;

(b) the type and nature of the personal data affected by the non-compliance by the organisation or person, as the case may be;

(c) whether the organisation or person (as the case may be), as a result of the non-compliance, gained any financial benefit or avoided any financial loss;

(d) whether the organisation or person (as the case may be) took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;

(e) whether the organisation or person (as the case may be) had, despite the non-compliance, implemented adequate and appropriate measures for compliance with the requirements under this Act;

(f) whether the organisation or person (as the case may be) had previously failed to comply with this Act;

(g) the compliance of the organisation or person (as the case may be) with any direction given under section 48I or 48L(4) in relation to remedying or mitigating the effect of the non-compliance;

(h) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with this Act;

Ref. code: 25646301033624ADV

(i) the likely impact of the imposition of the financial penalty on the organisation or person (as the case may be), including the ability of the organisation or person to continue the usual activities of the organisation or person;

(j) any other matter that may be relevant.

Procedure for giving of directions and imposing of financial penalty

48K.—(1) Before giving any direction under section 48I or imposing a financial penalty under section 48J(1), the Commission must give written notice to the organisation or person concerned —

(a) stating that the Commission intends to take action against the organisation or person under section 48I or 48J(1), as the case may be;

(b) where the Commission intends to give any direction under section 48I, specifying the direction the Commission proposes to give;

(c) specifying each instance of non-compliance that is the subject of the proposed action, or the reason or reasons for the proposed action; and

(d) subject to subsections (2) and (3), specifying the time within which written representations may be made to the Commission with respect to the proposed action.

(2) Where the Commission intends to impose a financial penalty under section 48J(1) on an organisation or a person, the time specified in the notice within which written representations may be made to the Commission must be at least 14 days after the date the notice is served on that organisation or person.

(3) The Commission may, on written application by the organisation or person concerned (whether before, on or after the expiry of the time specified in the notice), extend the time for the organisation or person to make written representations to the Commission if the Commission is satisfied that the extension should be granted by reason of exceptional circumstances in the particular case.

(4) The Commission may decide to give the direction under section 48I or impose the financial penalty under section 48J(1), as the case may be —

Ref. code: 25646301033624ADV

(a) after considering any written representation made to the Commission pursuant to the notice mentioned in subsection (1); or

(b) upon the expiry of the time specified in the notice under subsection (1)(d), or as extended by the Commission under subsection (3), where no representation is so made or any written representation made is subsequently withdrawn.

(5) Subsection (1) does not apply where the organisation or person (as the case may be) has died, is adjudged bankrupt, has been dissolved or wound up or has otherwise ceased to exist.

(6) Where the Commission decides to give the direction under section 48I or impose the financial penalty under section 48J(1) (as the case may be), the Commission must serve a notice of the decision on the following persons:

(a) the organisation or person concerned;

(b) the complainant whose complaint against the organization or person concerned resulted in the giving of the direction or the imposition of the financial penalty (as the case may be), if any.

(7) A direction given under section 48I or the imposition of a financial penalty under section 48J(1) takes effect only when the Commission serves the notice in subsection (6)(a) on the organization or person concerned.

(8) Where the Commission imposes a financial penalty under section 48J(1) on an organisation or a person, the written notice issued by the Commission to the organisation or person must specify the date before which the financial penalty is to be paid, being a date not earlier than 28 days after the notice is issued.

(9) The Commission may, on written application by an organization or a person on whom a financial penalty under section 48J(1) is imposed —

(a) extend the time for the organisation or person to pay the financial penalty; or

(b) allow the financial penalty to be paid by instalments.

(10) The interest payable —

Ref. code: 25646301033624ADV

(a) on the outstanding amount of any financial penalty imposed under section 48J(1); and

(b) for payment by instalments (as the Commission may allow) of any financial penalty imposed under section 48J(1), must be at such rate as the Commission may direct, which must not exceed the rate prescribed in the Rules of Court in respect of judgment debts.

Voluntary undertakings

48L.—(1) Without affecting sections 48I, 48J(1) and 50(1), where the Commission has reasonable grounds to believe that —

(a) an organisation has not complied, is not complying or is likely not to comply with any provision of Part 3, 4, 5, 6, 6A or 6B; or

(b) a person has not complied, is not complying or is likely not to comply with any provision of Part 9 or section 48B(1), the organisation or person concerned may give, and the Commission may accept, a written voluntary undertaking.

(2) Without limiting the matters to which the voluntary undertaking may relate, the voluntary undertaking may include any of the following undertakings by the organisation or person concerned:

(a) an undertaking to take specified action within a specified time;

(b) an undertaking to refrain from taking specified action;

(c) an undertaking to publicise the voluntary undertaking.

(3) Subject to subsection (4), the Commission may, after accepting the voluntary undertaking and with the agreement of the organization or person who gave the voluntary undertaking —

(a) vary the terms of any undertaking included in the voluntary undertaking; or

(b) include, in the voluntary undertaking, any additional undertaking mentioned in subsection (2).

(4) Where an organisation or a person fails to comply with any undertaking in a voluntary undertaking —

Ref. code: 25646301033624ADV

(a) the Commission may give the organisation or person concerned any direction that the Commission thinks fit in the circumstances to ensure the compliance of the organisation or person with that undertaking; and

(b) section 48K(1), (3), (4), (5), (6) and (7) applies to the direction given under paragraph (a) as if the direction were given under section 48I.

(5) In addition, where an organisation or a person fails to comply with an undertaking mentioned in subsection (2)(c), the Commission may publicise the voluntary undertaking in accordance with the undertaking, and recover the costs and expenses so incurred from the organisation or person as a debt due to the Commission.

Enforcement of directions of or written notices by Commission in District Court

48M.—(1) For the purposes of enforcing a direction or written notice mentioned in subsection (2) —

(a) the Commission may apply for the direction or written notice (as the case may be) to be registered in a District Court in accordance with the Rules of Court; and

(b) the District Court is to register the direction or written notice in accordance with the Rules of Court.

(2) Subsection (1) applies to any of the following:

(a) a direction made by the Commission under section 48H(2), 48I or 48L(4);

(b) a written notice by the Commission for the payment of any sum comprising —

(i) a financial penalty imposed under section 48J(1); and

(ii) any interest payable under section 48K(10) on that financial penalty.

(3) From the date of registration of a direction or written notice under subsection (1), the direction or written notice (as the case may be) has the same force and effect, and all proceedings may be taken on the direction or written notice (as the case may be), for the purposes of enforcement, as if it had been an order originally obtained in the District Court which has power to enforce it accordingly.

Ref. code: 25646301033624ADV

(4) A District Court may, for the purpose of enforcing a direction in accordance with subsection (3), make any order —

(a) to secure compliance with the direction; or

(b) to require any person to do anything to remedy, mitigate or eliminate any effects arising from —

(i) anything done which ought not, under the direction, to have been done; or

(ii) anything not done which ought, under the direction,

to have been done, which would not have occurred had the direction been complied with.

(5) A District Court has jurisdiction to enforce a written notice in accordance with subsection (3) regardless of the amount of the sum mentioned in subsection (2)(b).

Reconsideration of directions or decisions

48N.—(1) An organisation or a person (including any individual who is a complainant) aggrieved by —

(a) any direction made by the Commission under section 48G(2), 48I(1) or (2) or 48L(4); or

(b) any direction or decision made under section 48H(2), may make a written application to the Commission to reconsider the direction or decision in accordance with this section.

(2) An organisation or a person aggrieved by a financial penalty imposed by the Commission under section 48J(1) on the organization or person may make a written application to the Commission to reconsider the decision to impose the financial penalty or the amount of the financial penalty so imposed in accordance with this section.

(3) Unless the Commission decides otherwise in any particular case, an application for reconsideration does not suspend the effect of the direction or decision to be reconsidered except in the case of an application for reconsideration under subsection (2).

Ref. code: 25646301033624ADV

(4) The application for reconsideration —

(a) subject to subsection (5), must be submitted to the Commission within the prescribed period;

(b) must be made in the form and manner required by the Commission; and

(c) must set out the grounds on which the applicant is requesting the reconsideration.

(5) The Commission may, on written application by the organisation or person concerned (whether before, on or after the expiry of the prescribed period mentioned in subsection (4)(a)), extend the time for the organisation or person to make the application for reconsideration if the Commission is satisfied that the extension should be granted by reason of exceptional circumstances in the particular case.

(6) If an application for reconsideration is made in accordance with this section, the Commission must —

(a) reconsider the direction or decision;

(b) take any of the following actions as the Commission thinks fit:

(i) affirm, revoke or vary the direction or decision;

(ii) affirm or revoke, or vary the amount of, the financial penalty; and

(c) notify the applicant in writing of the result of the reconsideration.

(7) There is to be no application for reconsideration of a decision made under subsection (6)(b).

Right of private action

48O.—(1) A person who suffers loss or damage directly as a result of a contravention —

(a) by an organisation of any provision of Part 4, 5, 6, 6A or 6B; or

(b) by a person of any provision of Division 3 of Part 9 or section 48B(1), has a right of action for relief in civil proceedings in a court.

(2) If the Commission has made a decision under this Act in respect of a contravention specified in subsection (1), an action accruing under subsection (1)

Ref. code: 25646301033624ADV

may not be brought in respect of thatcontravention until after the decision has become final as a result of there being no further right of appeal.

(3) The court may grant to the claimant in an action under subsection (1) all or any of the following:

(a) relief by way of injunction or declaration;

(b) damages;

(c) any other relief as the court thinks fit.

PART 9D

APPEALS

Data Protection Appeal Panel and Data Protection Appeal Committees

48P.—(1) There is established a Data Protection Appeal Panel.

(2) The Minister must appoint the members of the Appeal Panel.

(3) The Chairperson of the Appeal Panel must be appointed by the Minister from among the members of the Appeal Panel.

(4) For the purpose of hearing any appeal under section 48Q, the Chairperson of the Appeal Panel may nominate a Data Protection Appeal Committee comprising 3 or more members of the Appeal Panel.

(5) The Seventh Schedule has effect with respect to the Appeal Panel, Appeal Committees and their members and the proceedings of Appeal Committees, as the case may be.

Appeal from direction or decision of Commission

48Q.—(1) An organisation or a person (including an individual who is a complainant) aggrieved by —

(a) any direction made by the Commission under section 48G(2), 48I(1) or (2) or 48L(4);

(b) any direction or decision made by the Commission under section 48H(2); or

Ref. code: 25646301033624ADV

(c) any decision made by the Commission under section 48N(6)(b), may, within the prescribed period, appeal to the Chairperson of the Appeal Panel against that direction or decision.

(2) An organisation or a person aggrieved by a financial penalty imposed by the Commission under section 48J(1) on the organization or person may, within the prescribed period, appeal to the Chairperson of the Appeal Panel against the decision to impose the financial penalty or the amount of the financial penalty so imposed.

(3) Where an application for reconsideration has been made under section 48N, every appeal in respect of the same direction or decision which is the subject of the application for reconsideration is deemed to be withdrawn.

(4) Unless the Appeal Committee decides otherwise in any particular case, the making of an appeal under this section does not suspend the effect of the direction or decision to which the appeal relates except in the case of an appeal under subsection (2).

(5) An Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal and, in particular, may —

(a) remit the matter to the Commission;

(b) impose or revoke, or vary the amount of, a financial penalty;

(c) give any direction, or take any other step, that the Commission could itself have given or taken; or

(d) make any other direction or decision that the Commission could itself have made.

(6) A direction or decision of an Appeal Committee on an appeal has the same effect, and may be enforced in the same manner, as a direction or decision of the Commission, except that there is to be no application for further reconsideration under section 48N and no further appeal under this section from the direction or decision of the Appeal Committee.

Ref. code: 25646301033624ADV

(7) If an Appeal Committee confirms the direction or decision which is the subject of the appeal, it may nevertheless set aside any finding of fact on which the direction or decision was based.

Appeals to General Division of High Court, etc.

48R.—(1) An appeal against, or with respect to, a direction or decision of an Appeal Committee lies to the General Division of the High Court —

(a) on a point of law arising from the direction or decision of the Appeal Committee; or

(b) from any direction of the Appeal Committee as to the amount of a financial penalty.

(2) An appeal under this section may be made within the prescribed time only at the instance of —

(a) the organisation or person aggrieved by the direction or decision of the Appeal Committee;

(b) if the decision relates to a complaint, the complainant; or

(c) the Commission.

(3) The General Division of the High Court is to hear and determine any appeal under this section and may —

(a) confirm, modify or reverse the direction or decision of the Appeal Committee; and

(b) make any further or other order on the appeal, whether as to costs or otherwise, as the General Division of the High Court thinks fit.

(4) There is such further right of appeal from decisions of the General Division of the High Court under this section as exists in the case of decisions made by the General Division of the High Court in the exercise of its original civil jurisdiction.

Ref. code: 25646301033624ADV

PART 10

GENERAL

Advisory guidelines

49.—(1) The Commission may issue written advisory guidelines indicating the manner in which the Commission will interpret the provisions of this Act.

(2) Guidelines issued under this section may be varied, amended or revoked by the Commission.

(3) The Commission must publish the guidelines in any way the Commission thinks fit, but failure to comply with this subsection in respect of any guidelines does not invalidate the guidelines.

Powers of investigation

50.—(1) The Commission may, upon complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation or a person is complying with this Act, including a voluntary undertaking given by the organisation or person under section 48L(1).

(2) The powers of investigation under this section of the Commission and the inspectors are set out in the Ninth Schedule.

(3) The Commission may suspend, discontinue or refuse to conduct an investigation under this section if it thinks fit, including but not limited to any of the following circumstances:

(a) the complainant has not complied with a direction under section 48G(2);

(b) the parties involved in the matter have mutually agreed to settle the matter;

(c) any party involved in the matter has commenced legal proceedings against another party in respect of any contravention or alleged contravention of this Act by the other party;

(ca) the Commission accepts a voluntary undertaking given by an organisation or a person under section 48L(1) in relation to the matter;

Ref. code: 25646301033624ADV

(d) the Commission is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority;

(e) the Commission is of the opinion that —

(i) a complaint is frivolous or vexatious or is not made in good faith; or

(ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation.

(3A) To avoid doubt, despite subsection (3)(ca), the Commission may conduct or resume an investigation under this section at any time if an organisation or a person fails to comply with a voluntary undertaking given by the organisation or person under section 48L(1) in relation to any matter.

(4) An organisation must retain records relating to an investigation under this section for one year after the conclusion of the investigation or any longer period specified in writing by the Commission.

Offences and penalties

51.—(1) A person shall be guilty of an offence if the person —

(a) makes a request under section 21(1) to obtain access to personal data about another individual without the authority of that other individual;

(b) makes a request under section 22(1) to change personal data about another individual without the authority of that other individual; or

(c) subject to subsection (1A), gives a porting organisation a data porting request under section 26H(1) to transmit personal data about another individual to a receiving organisation without the authority of that other individual.

(1A) Subsection (1)(c) does not apply to an individual who gives a data porting request under section 26H(1), in the individual's personal or domestic capacity, to transmit any user activity data or user-provided data about the individual even though the user activity data or user-provided data (as the case may be) includes personal data about another individual.

Ref. code: 25646301033624ADV

(2) A person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both.

(3) An organisation or person commits an offence if the organisation or person —

(a) with an intent to evade a request under section 21 or 22, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy, a record containing —

(i) personal data; or

(ii) information about the collection, use or disclosure of personal data;

(b) obstructs or hinders the Commission, an inspector or an authorised officer in the performance of any function or duty, or the exercise of any power, under this Act;

(ba) without reasonable excuse, neglects or refuses to provide any information or produce any document which the organisation or person is required by or under this Act to provide or produce to the Commission or an inspector;

(bb) without reasonable excuse, neglects or refuses to attend before the Commission or an inspector as required by or under this Act; or

(c) makes a statement, or provides any information or document, to the Commission, an inspector or an authorised officer under this Act, which the organization or person knows, or ought reasonably to know, to be false or misleading in any material particular.

(4) An organisation or person that commits an offence under subsection (3)(a) is liable —

(a) in the case of an individual, to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both; and

(b) in any other case, to a fine not exceeding $50,000.

(5) An organisation or person that commits an offence under subsection (3)(b) or (c) is liable —

(a) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and

Ref. code: 25646301033624ADV

(b) in any other case, to a fine not exceeding $100,000.

(6) An organisation or a person that commits an offence under subsection (3)(ba) or (bb) is liable —

(a) in the case of an individual — to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both; and

(b) in any other case — to a fine not exceeding $10,000.

Offences by corporations

52.—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that —

(a) an officer, employee or agent of the corporation engaged in that conduct within the scope of the actual or apparent authority of the officer, employee or agent, as the case may be; and

(b) the officer, employee or agent had that state of mind, is evidence that the corporation had that state of mind.

(2) Where a corporation commits an offence under this Act, a person —

(a) who is —

(i) an officer of the corporation; or

(ii) an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence; and

(b) who —

(i) consented or connived, or conspired with others, to effect the commission of the offence;

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the corporation; or

(iii) knew or ought reasonably to have known that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop

Ref. code: 25646301033624ADV

the commission of that offence, shall be guilty of that same offence as is the corporation, and shall be liable on conviction to be punished accordingly.

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the corporation if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the corporation would bear.

(4) To avoid doubt, this section does not affect the application of —

(a) Chapters 5 and 5A of the Penal Code 1871; or

(b) the Evidence Act 1893 or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of the corporation for an offence under this Act, and applies whether or not the corporation is convicted of the offence.

(6) The Minister may make regulations to provide for the application of any provision of this section, with such modifications as the Minister considers appropriate, to any corporation formed or recognised under the law of a territory outside Singapore.

(7) In this section —

"corporation" includes a limited liability partnership within the meaning of section 2(1) of the Limited Liability Partnerships Act 2005;

"officer", in relation to a corporation, means any director, partner, chief executive, manager, secretary or other similar officer of the corporation, and includes —

(a) any person purporting to act in any such capacity; and

(b) for a corporation whose affairs are managed by its members, any of those members as if the member were a director of the corporation;

"state of mind" of a person includes —

(a) the knowledge, intention, opinion, belief or purpose of the person; and

(b) the person's reasons for the intention, opinion, belief or purpose.

Ref. code: 25646301033624ADV

Offences by unincorporated associations or partnerships

52A.—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of an unincorporated association or a partnership in relation to a particular conduct, evidence that —

(a) an employee or agent of the unincorporated association or partnership engaged in that conduct within the scope of the actual or apparent authority of the employee or agent, as the case may be; and

(b) the employee or agent had that state of mind, is evidence that the unincorporated association or partnership had that state of mind.

(2) Where an unincorporated association or a partnership commits an offence under this Act, a person —

(a) who is —

(i) an officer of the unincorporated association or a member of its governing body;

(ii) a partner in the partnership; or

(iii) an individual involved in the management of the unincorporated association or partnership and in a position to influence the conduct of the unincorporated association or partnership (as the case may be) in relation to the commission of the offence; and

(b) who —

(i) consented or connived, or conspired with others, to effect the commission of the offence;

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the unincorporated association or partnership; or

(iii) knew or ought reasonably to have known that the offence by the unincorporated association or partnership (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence, shall be guilty of the same offence as is the unincorporated association or partnership

Ref. code: 25646301033624ADV

(as the case may be), and shall be liable on conviction to be punished accordingly.

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the unincorporated association or partnership if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the unincorporated association or partnership would bear.

(4) To avoid doubt, this section does not affect the application of —

(a) Chapters 5 and 5A of the Penal Code 1871; or

(b) the Evidence Act 1893 or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of an unincorporated association or a partnership for an offence under this Act, and applies whether or not the unincorporated association or partnership is convicted of the offence.

(6) The Minister may make regulations to provide for the application of any provision of this section, with such modifications as the Minister considers appropriate, to any unincorporated association or partnership formed or recognized under the law of a territory outside Singapore.

(7) In this section —

"officer", in relation to an unincorporated association (other than a partnership), means the president, the secretary or any member of the committee of the unincorporated association, and includes —

(a) any person holding a position analogous to that of president, secretary or member of the committee of the unincorporated association; and

(b) any person purporting to act in any such capacity;

"partner" includes a person purporting to act as a partner;

"state of mind" of a person includes —

(a) the knowledge, intention, opinion, belief or purpose of the person; and

(b) the person's reasons for the intention, opinion, belief or purpose.

Ref. code: 25646301033624ADV

Liability of employers for acts of employees

53.—(1) Any act done or conduct engaged in by a person in the course of his or her employment (called in this section the employee) is treated for the purposes of this Act as done or engaged in by his or her employer as well as by the employee, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) In any proceedings for an offence under this Act brought against any person in respect of an act or conduct alleged to have been done or engaged in (as the case may be) by an employee of that person, it is a defence for that person to prove that the person took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his or her employment, acts or conduct (as the case may be) of that description.

Jurisdiction of court

54. Despite any provision to the contrary in the Criminal Procedure Code 2010, a District Court has jurisdiction to try any offence under this Act and has power to impose the full penalty or punishment in respect of the offence.

Composition of offences

55.—(1) The Commission may compound any offence under this Act (except Part 9) that is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding the lower of the following:

(a) one half of the amount of the maximum fine that is prescribed for the offence;

(b) a sum of $5,000.

(2) The Commission may compound any offence under Part 9 that is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding $1,000.

Ref. code: 25646301033624ADV

(3) On payment of the sum of money, no further proceedings are to be taken against that person in respect of the offence.

(4) The Commission may, with the approval of the Minister, make regulations prescribing the offences that may be compounded.

General penalties

56. A person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part of a day during which the offence continues after conviction.

Public servants and public officers

57.—(1) All individuals appointed under section 8(1) —

(a) are deemed to be public servants for the purposes of the Penal Code 1871; and

(b) are, in relation to their administration, assessment, collection or enforcement of payment of composition sums under this Act, deemed to be public officers for the purposes of the Financial Procedure Act 1966; and section 20 of that Act applies to these individuals even though they are not or were not in the employment of the Government.

(2) All members of the Appeal Panel, and all members of an advisory committee, are deemed to be public servants for the purposes of the Penal Code 1871.

Evidence in proceedings

58.—(1) The Commission, the Appeal Panel, an Appeal Committee, their members and anyone acting for or under the direction of the Commission must not give or be compelled to give evidence in a court or in any other proceedings in respect of any information obtained in performing their duties or exercising their powers or functions under this Act, except —

Ref. code: 25646301033624ADV

(a) in a prosecution for perjury or for the provision of false information;

(b) in a prosecution for an offence under this Act; or

(c) in an application for judicial review or an appeal from a decision with respect to such an application.

(2) Subsection (1) applies also in respect of evidence of the existence of proceedings conducted before the Commission.

Preservation of secrecy

59.—(1) Subject to subsection (5), every specified person must preserve, and aid in the preservation of, secrecy with regard to —

(a) any personal data an organisation would be required or authorised to refuse to disclose if it were contained in personal data requested under section 21;

(b) whether information exists, if an organisation in refusing to provide access under section 21 does not indicate whether the information exists;

(c) all matters that have been identified as confidential under subsection (3); and

(d) all matters relating to the identity of persons providing information to the Commission, that may come to the specified person's knowledge in the performance of the specified person's functions and discharge of the specified person's duties under this Act and must not communicate any such matter to any person, except insofar as such communication —

(e) is necessary for the performance of any such function or discharge of any such duty; or

(f) is lawfully required by any court, or lawfully required or permitted under this Act or any other written law.

(2) A person who fails to comply with subsection (1) shall be guilty of an offence.

(3) A person, when providing any information to the Commission, may identify information that the person claims to be confidential information.

(4) Every claim made under subsection (3) must be supported by a written statement giving reasons why the information is confidential.

Ref. code: 25646301033624ADV

(5) Despite subsection (1), the Commission may disclose, or authorise any specified person to disclose, any information relating to any matter referred to in subsection (1) in any of the following circumstances:

(a) where the consent of the person to whom the information relates has been obtained;

(b) if the Commission considers there is evidence of an offence, disclose information relating to the commission of an offence to the Public Prosecutor, any police officer and other law enforcement authorities;

(c) to give effect to any provision of this Act;

(d) for the purposes of a prosecution, an application or an appeal mentioned in section 58(1)(a), (b) or (c);

(e) to comply with any provision of a cooperation agreement entered into under section 10, where the conditions specified in subsection (6) are satisfied; or

(f) to a public body in such circumstances as the Minister may prescribe.

(6) The conditions mentioned in subsection (5)(e) are —

(a) that the information or documents requested by the foreign country are in the possession of the Commission;

(b) that unless the Government otherwise allows, the foreign country undertakes to keep the information given confidential at all times; and

(c) that the disclosure of the information is not likely to be contrary to the public interest.

(7) In this section, "specified person" means a person who is or has been —

(a) a member or an officer of a relevant body;

(aa) a person authorised or appointed by a relevant body to perform the relevant body's functions or duties, or exercise the relevant body's powers, under this Act or any other written law;

(b) a member of a committee of a relevant body or any person authorised, appointed or employed to assist the relevant body; or

Ref. code: 25646301033624ADV

(c) an inspector or a person authorised, appointed or employed to assist an inspector.

Protection from personal liability

60. No liability shall be incurred by —

(a) any member or officer of a relevant body;

(b) any person authorised, appointed or employed to assist a relevant body;

(c) any person who is on secondment or attachment to a relevant body;

(d) any person authorised or appointed by a relevant body to exercise the relevant body's powers, perform the relevant body's functions or discharge the relevant body's duties or to assist the relevant body in the exercise of its powers, the performance of its functions or the discharge of its duties under this Act or any other written law; or

(e) any inspector or any person authorised, appointed or employed to assist an inspector in connection with any function or duty of the inspector under this Act, as a result of anything done (including any statement made) or omitted to be done with reasonable care and in good faith in the course of or in connection with —

(f) the exercise or purported exercise of any power under this Act or any other written law;

(g) the performance or purported performance of any function or the discharge or purported discharge of any duty under this Act or any other written law; or

(h) the compliance or purported compliance with this Act or any other written law.

Symbol of Commission

61.—(1) The Commission has the exclusive right to the use of such symbol or representation as may be prescribed in connection with its activities or affairs.

(2) A person who, without the authority of the Commission, uses a symbol or representation identical with that of the Commission, orwhich so resembles the

symbol or representation of the Commission as to deceive or cause confusion, or to be likely to deceive or to cause confusion, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 6 months or to both.

Power to exempt

62. The Commission may, with the approval of the Minister, by order in the Gazette, exempt any person or organisation or any class of persons or organisations from all or any of the provisions of this Act, subject to such terms or conditions as may be specified in the order.

Certificate as to national interest

63. For the purposes of this Act, if any doubt arises as to whether anything is necessary for the purpose of, or could be contrary to, the national interest, a certificate signed by the Minister charged with responsibility for that matter is conclusive evidence of the matters stated in the certificate.

Amendment of Schedules

64.—(1) The Minister may, by order in the Gazette, amend any of the Schedules, except the Ninth Schedule.

(2) An order under this section must be presented to Parliament as soon as possible after publication in the Gazette.

Power to make regulations

65.—(1) The Commission may, with the approval of the Minister, make such regulations as may be necessary or expedient for carrying out the purposes and provisions of this Act and for prescribing anything that may be required or authorised to be prescribed by this Act.

(2) Without limiting subsection (1), the Commission may, with the approval of the Minister, make regulations for or with respect to all or any of the following matters:

Ref. code: 25646301033624ADV

(a) [Deleted by Act 22 of 2016]

(b) the form, manner and procedures, relating to the making and responding to requests under section 21 or 22, including the content of responses to such requests, the period for such responses, the circumstances in which an organisation may refuse to provide a response or refuse to confirm or deny the existence of any matter and the fees that an organisation may charge in respect of such requests;

(ba) the assessment and notification of notifiable data breaches, including —

(i) the steps and measures that an organisation must take in relation to the investigation and assessment of data breaches; and

(ii) the form and manner in which the Commission and affected individuals must be notified of notifiable data breaches;

(bb) the form, manner and procedures relating to data porting requests, including —

(i) the information and particulars that must be provided for such requests;

(ii) the time for and content of a porting organisation's responses to such requests;

(iii) the steps that a receiving organisation must take to confirm the accessibility and completeness of any applicable data transmitted by a porting organisation; and

(iv) the fees that a porting organisation may charge in respect of such requests;

(c) the classes of persons who may act under this Act for minors, deceased persons or any other individuals who lack capacity to act under this Act and regulating the manner in which, and the extent to which, any rights or powers of individuals under this Act may be exercised on their behalf;

(d) the form, manner and procedures relating to applications and complaints under this Act;

(e) the conduct of reviews by the Commission under section 48H;

Ref. code: 25646301033624ADV

(f) the form, manner and procedures for applications for reconsideration by the Commission under section 48N, including the fees to be paid in respect of such applications;

(g) the form, manner and procedures for appeals to an Appeal Committee, including the fees to be paid in respect of such appeals;

(h) the award of costs of or incidental to any proceedings before the Commission or Appeal Committee, and the award of expenses, including any allowances payable topersons in connection with their attendance before the Commission or Appeal Committee;

(i) the criteria for determining whether a Singapore telephone number is eligible to be listed in a register;

(j) the manner in which entries in the register are to be made, corrected or removed;

(k) the manner and form of giving or withdrawing consent for the sending of a specified message;

(l) any other matter relating to the establishment, operation or administration of the register;

(m) the fees to be paid in respect of applications, and services provided by or on behalf of the Commission, under this Act, including applications made under section 40(2);

(n) the requirements that checkers must comply with for the purposes of this Act.

(3) Regulations made under this section may provide differently for different organisations, individuals, classes of organisations or classes of individuals.

Rules of Court

66. Rules of Court may be made to provide for the practice and procedure relating to actions under section 48O and appeals under section 48R, including the requirement that the claimant notify the Commission upon commencing any such action or appeal, and for matters related thereto.

Ref. code: 25646301033624ADV

Saving and transitional provisions

67.—(1) Every act done by or on behalf of the Former Commission before 1 October 2016 remains valid and has effect as though it has been done by or on behalf of the Commission, until such time as the Commission invalidates, revokes, cancels or otherwise determines that act.

(2) Where any thing has been started by or on behalf of the Former Commission before 1 October 2016, the Commission may carry on and complete that thing on or after that date.

(3) Any approval, authorisation, decision, direction, exemption, guideline or notice (or other document) given or made by the Former Commission under this Act before 1 October 2016 remains valid and is deemed to have been given or made by the Commission under this Act, to the extent that it is not inconsistent with this Act as amended by the Info-communications Media Development Authority Act 2016.

(4) Any application that is made to the Former Commission under this Act and is pending on 1 October 2016 is deemed to be an application made to the Commission under this Act, to the extent that it is not inconsistent with this Act as amended by the Info-communications Media Development Authority Act 2016.

(5) Any appeal made before 1 October 2016 under Part 8 in respect of any direction or decision of the Former Commission is deemed to be an appeal in respect of the direction or decision of the Commission.

(6) Any authorisation made by, or any certificate or other document signed by, the Chairman of the Former Commission under this Act before 1 October 2016 remains valid and is deemed to have been made or signed by the Chief Executive of the Authority under this Act.

(7) [Omitted as spent]

(8) This section does not affect the operation of section 16 of the Interpretation Act 1965.

Ref. code: 25646301033624ADV

(9) In this section, "Former Commission" means the Personal Data Protection Commission established by section 5(1) as in force immediately before 1 October 2016.

Dissolution

68.—(1) The Former Commission is dissolved.

(2) In this section, "Former Commission" has the meaning given by section 67(9)

FIRST SCHEDULE

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA WITHOUT CONSENT

PART 1 VITAL INTERESTS OF INDIVIDUALS

1.—(1) Subject to sub-paragraph (2), the collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any purpose which is clearly in the individual's interests, and —

(a) consent for the collection, use or disclosure (as the case may be) cannot be obtained in a timely way; or

(b) the individual would not reasonably be expected to withhold consent.

(2) Where the organisation collects, uses or discloses (as the case may be) personal data about the individual under sub-paragraph (1), the organisation must, as soon as is practicable, notify the individual of the collection, use or disclosure (as the case may be) and the purpose for the collection, use or disclosure, as the case may be.

2. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual.

3. The collection, use or disclosure (as the case may be) of personal data about an individual, where —

(a) consent for the collection, use or disclosure (as the case may be) cannot be obtained in a timely way; and

Ref. code: 25646301033624ADV

(b) there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected.

4. The collection, use or disclosure of personal data is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual.

PART 2 MATTERS AFFECTING PUBLIC

1. The collection, use or disclosure (as the case may be) of personal data about an individual that is publicly available.
2. The collection, use or disclosure (as the case may be) of personal data about an individual is in the national interest.
3. The collection, use or disclosure (as the case may be) of personal data about an individual is solely for artistic or literary purposes.
4. The collection, use or disclosure (as the case may be) of personal data about an individual is solely for archival or historical purposes, if a reasonable person would not consider the personal data to be too sensitive to the individual to be collected, used or disclosed (as the case may be) at the proposed time.
5. The personal data about an individual is collected, used or disclosed (as the case may be) by a news organisation solely for its news activity.
6. In this Part —

"broadcasting service" has the meaning given by section 2(1) of the Broadcasting Act 1994;

"news activity" means —

(a) the gathering of news, or the preparation or compilation of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning —

(i) news;

(ii) observations on news; or

(iii) current affairs;

"news organisation" means —

Ref. code: 25646301033624ADV

(a) any organisation —

(i) the business of which consists, in whole or in part, of news activity carried out in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper; and

(ii) which, if the organisation publishes a newspaper in Singapore which is not exempted from the provisions of Part 3 of the Newspaper and Printing Presses Act 1974, is a newspaper company defined in section 2(1) of that Act; or

(b) any organisation which provides a broadcasting service in or from Singapore and holds a broadcasting licence granted under section 8 of the Broadcasting Act 1994;

"newspaper" has the meaning given by section 2(1) of the Newspaper and Printing Presses Act 1974;

"relevant broadcasting service" means any of the following licensable broadcasting services within the meaning of the Broadcasting Act 1994:

(a) free-to-air nationwide television services;

(b) free-to-air localised television services;

(c) free-to-air international television services;

(d) subscription nationwide television services;

(e) subscription localised television services;

(f) subscription international television services;

(g) special interest television services;

(h) free-to-air nationwide radio services;

(i) free-to-air localised radio services;

(j) free-to-air international radio services;

(k) subscription nationwide radio services;

(l) subscription localised radio services;

(m) subscription international radio services;

(n) special interest radio services.

PART 3 LEGITIMATE INTERESTS

Ref. code: 25646301033624ADV

1.—(1) Subject to sub-paragraphs (2), (3) and (4) —

(a) the collection, use or disclosure (as the case may be) of personal data about an individual is in the legitimate interests of the organisation or another person; and

(b) the legitimate interests of the organisation or other person outweigh any adverse effect on the individual.

(2) For the purposes of sub-paragraph (1), the organisation must —

(a) conduct an assessment, before collecting, using or disclosing the personal data (as the case may be), to determine whether sub-paragraph (1) is satisfied; and

(b) provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data (as the case may be) in accordance with sub-paragraph (1).

(3) The organisation must, in respect of the assessment mentioned in sub-paragraph (2)(a) —

(a) identify any adverse effect that the proposed collection, use or disclosure (as the case may be) of personal data about an individual is likely to have on the individual;

(b) identify and implement reasonable measures —

(i) to eliminate the adverse effect;

(ii) to reduce the likelihood that the adverse effect will occur; or

(iii) to mitigate the adverse effect; and

(c) comply with any other prescribed requirements.

(4) Sub-paragraph (1) does not apply to the collection, use or disclosure of personal data about an individual for the purpose of sending to that individual or any other individual a message for an applicable purpose within the meaning given by section 37(6).

2. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for evaluative purposes.

Ref. code: 25646301033624ADV

3. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any investigation or proceedings.

4. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for the organisation —

(a) to recover a debt owed by the individual to the organisation; or

(b) to pay to the individual a debt owed by the organisation.

5. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services.

6.—(1) Subject to sub-paragraph (2), the collection, use or disclosure (as the case may be) of personal data about an individual —

(a) is for the purpose of the preparation by a credit bureau of a credit report; or

(b) relates to a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual.

(2) Sub-paragraph (1) does not apply to a credit bureau that, being required to obtain a licence under any other written law, does not hold such a licence.

7. The collection, use or disclosure (as the case may be) of personal data about an individual is to —

(a) confer an interest or a benefit on the individual under a private trust or benefit plan; and

(b) administer that trust or benefit plan, at the request of the settlor or the person establishing the benefit plan, as the case may be.

8. The personal data about an individual —

(a) is provided to the organisation by another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual; and

(b) is collected, used or disclosed (as the case may be) by the organisation solely for the purpose in sub-paragraph (a).

Ref. code: 25646301033624ADV

9. The personal data about an individual —

(a) is included in a document produced in the course, and for the purposes, of the individual's employment, business or profession; and

(b) is collected, used or disclosed (as the case may be) for purposes consistent with the purpose for which the document was produced.

10. The personal data about an individual is collected, used or disclosed (as the case may be) by the organisation, and the collection, use or disclosure (as the case may be) of the personal data is reasonable for the purpose of or in relation to the organisation —

(a) entering into an employment relationship with the individual or appointing the individual to any office; or

(b) managing or terminating the employment relationship with or appointment of the individual.

PART 4 BUSINESS ASSET TRANSACTIONS

1.—(1) Subject to the conditions in sub-paragraphs (2), (3), (4) and (5), where an organisation (X) is a party or a prospective party to a business asset transaction with another organisation (Y), personal data about an applicable individual of Y —

(a) is collected from Y by X for the purposes of the business asset transaction;

(b) is used or disclosed by X in relation to the business asset transaction; or

(c) is disclosed by Y to X for the purposes of the business transaction.

(2) Where the business asset transaction concerns any part of Y or Y's business assets, the personal data mentioned in sub-paragraph (1) must relate directly to that part of Y or Y's business assets, as the case may be.

(3) If X is a prospective party to the business asset transaction, the following conditions apply:

(a) X may collect, and Y may disclose, only personal data that is necessary for X to determine whether to proceed with the business asset transaction;

(b) X and Y must have entered into an agreement that requires X to use or disclose the personal data solely for purposes related to the business asset transaction.

Ref. code: 25646301033624ADV

(4) If X enters into the business asset transaction, the following conditions apply:

(a) X may use or disclose the personal data X collected from Y only for the same purposes for which Y would have been permitted to use or disclose the personal data;

(b) if any personal data X collects from Y does not relate directly to the part of Y or Y's business assets with which the business asset transaction entered into is concerned, X must destroy, or return to Y, that personal data;

(c) X or Y must notify the applicable individuals of Y whose personal data is disclosed that —

(i) the business asset transaction has taken place; and

(ii) the personal data about them has been disclosed to X.

(5) If the business asset transaction does not proceed or is not completed, X must destroy, or return to Y, all personal data collected.

2.—(1) Subject to the conditions in sub-paragraphs (2), (3) and (4), where an organisation (X) is a party or a prospective party to a business asset transaction with another organisation (Y) in respect of Y's interest in a third organisation (Z) (called in this paragraph the relevant transaction), personal data about an applicable individual of Z —

(a) is collected from Y or Z by X, or from Z by Y, for the purposes of the relevant transaction;

(b) is used or disclosed by X or Y in relation to the relevant transaction; or

(c) is disclosed by Y or Z (as the case may be) to X, or by Z to Y, for the purposes of the relevant transaction.

(2) If X is a prospective party to the relevant transaction, the following conditions apply:

(a) where X collects the personal data mentioned in sub-paragraph (1) from Y or Z —

(i) X may collect, and Y or Z (as the case may be) may disclose, only personal data that is necessary for X to determine whether to proceed with the relevant transaction; and

(ii) X and Y or Z (as the case may be) must have entered into an agreement that requires X to use or disclose the personal data solely for purposes related to the relevant transaction;

(b) where Y collects the personal data mentioned in sub-paragraph (1) from Z —

(i) Y may collect, and Z may disclose, only personal data that is necessary for X or Y (as the case may be) to determine whether to proceed with the relevant transaction; and

(ii) Y and Z must have entered into an agreement that requires Y to use or disclose the personal data solely for purposes related to the relevant transaction.

(3) If X enters into the relevant transaction, the following conditions apply:

(a) X may use or disclose the personal data collected from Y or Z (as the case may be) only for the same purposes for which Y or Z (as the case may be) would have been permitted to use or disclose the personal data;

(b) Y may use or disclose the personal data collected from Z only for the same purposes for which Z would have been permitted to use or disclose the personal data;

(c) X, Y or Z must notify the applicable individuals of Z whose personal data is disclosed that —

(i) the relevant transaction has taken place; and

(ii) the personal data about them has been disclosed to X.

(4) If the relevant transaction does not proceed or is not completed —

(a) X must destroy, or return to Y or Z (as the case may be), all personal data collected; and

(b) Y must destroy, or return to Z, all personal data collected.

3. In this Part —

"applicable individual", in relation to an organisation, includes a contractor, a customer, a director, an employee, an officer or a shareholder of the organisation;

"business asset transaction" —

(a) means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of —

(i) an organisation or a portion of an organisation;

(ii) an interest in an organisation; or

(iii) any of the business or assets of an organisation, other than any personal data to be disclosed under paragraph 1(1) or 2(1), as the case may be; and

(b) includes —

(i) the amalgamation of a corporation with one or more related corporations; and

(ii) the transfer or disposal of any of the business or assets of a corporation to a related corporation;

"business trust" has the meaning given by section 2 of the Business Trusts Act 2004;

"corporation" and "related corporation" have the meanings given by section 4(1) of the Companies Act 1967;

"interest" means —

(a) in relation to a corporation — a share in that corporation;

(b) in relation to an entity other than a corporation — any right or interest (whether legal or equitable) in that entity, by whatever name called;

(c) in relation to a business trust — a unit in that business trust; and

(d) in relation to a trust other than a business trust — any right or interest (whether legal or equitable) in that trust, by whatever name called.

PART 5 BUSINESS IMPROVEMENT PURPOSES

1.—(1) Subject to the conditions in sub-paragraphs (3), (4) and (5), personal data about an individual (P) —

(a) is collected by an organisation (X) that is a corporation from a related corporation (Y) for a purpose specified in sub-paragraph (2) (called the relevant purpose);

(b) is used by X for a relevant purpose; or

(c) is disclosed by Y to X for a relevant purpose.

Ref. code: 25646301033624ADV

(2) The relevant purposes mentioned in sub-paragraph (1) are the following:

(a) improving or enhancing any goods or services provided, or developing new goods or services to be provided, by X or Y;

(b) improving or enhancing the methods or processes, or developing new methods or processes, for the operations of X or Y;

(c) learning about and understanding the behaviour and preferences of P or another individual in relation to the goods or services provided by X or Y;

(d) identifying any goods or services provided by X or Y that may be suitable for P or another individual, or personalising or customising any such goods or services for P or another individual.

(3) Sub-paragraph (1)(a) and (c) applies only if —

(a) the relevant purpose for which X collects, or Y discloses, personal data about P cannot reasonably be achieved without the collection, use or disclosure (as the case may be) of the personal data in an individually identifiable form;

(b) a reasonable person would consider the collection or disclosure of personal data about P for the relevant purpose to be appropriate in the circumstances; and

(c) X and Y are bound by any contract or other agreement or binding corporate rules requiring the recipient of personal data about P to implement and maintain appropriate safeguards for the personal data.

(4) Sub-paragraph (1)(b) applies only if —

(a) the relevant purpose for which X uses personal data about P cannot reasonably be achieved without the use of the personal data in an individually identifiable form; and

(b) a reasonable person would consider the use of personal data about P for the relevant purpose to be appropriate in the circumstances.

(5) Where X collects from Y, and Y discloses to X, personal data about P for a purpose mentioned in sub-paragraph (2)(c) or (d), P must be, at the time of the collection or disclosure, as the case may be —

(a) an existing customer of Y; and

(b) an existing customer or a prospective customer of X.

(6) To avoid doubt, sub-paragraph (1) does not apply to the collection, use or disclosure of personal data about P for the purpose of sending to P or another individual a message for an applicable purpose within the meaning given by section 37(6).

2. In this Part —

"corporation" and "related corporation" have the meanings given by section 4(1) of the Companies Act 1967;

"existing customer", in relation to a corporation, means an individual who purchases, hires or uses, or has purchased, hired or used, any goods or services provided by the corporation;

"prospective customer of X" means an individual who, at the time mentioned in paragraph 1(5) —

(a) has informed X of the individual's interest in purchasing, hiring or using any goods or services provided by X; or

(b) is conducting negotiations with X that lead or may lead to an agreement between the individual and X for the purchase, hire or use of any goods or services provided by X.

Ref. code: 25646301033624ADV

ภาคผนวก ง

บันทึกการสัมภาษณ์ คุณสุวรรณโชติ ศิริมหาศาล ที่ปรึกษาด้านการพัฒนาระบบ และวิทยากรเรื่องข้อมูลส่วนบุคคล สำนักงานพัฒนารัฐบาลดิจิทัล สัมภาษณ์ทางโทรศัพท์ วันที่ 19 กรกฎาคม 2565 เวลา 12.33-12.56 น.

คุณสุวรรณโชติ ศิริมหาศาล ที่ปรึกษาด้านการพัฒนาระบบ และวิทยากรเรื่องการธรรมาภิบาลข้อมูล (Data Governance) และข้อมูลส่วนบุคคล สังกัดสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยคุณสุวรรณโชติได้ผ่านการอบรมหลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หลักสูตร 80 ชั่วโมงจากบูโร เวอริทัส ประเทศไทย และหลักสูตร การคุ้มครองข้อมูลส่วนบุคคลสำหรับพนักงาน จากจุฬาลงกรณ์มหาวิทยาลัย นอกจากนี้ คุณสุวรรณโชติยังเป็นวิทยากรให้ความรู้ด้านข้อมูลส่วนบุคคลแก่หลากหลายหน่วยงานทั้งภาครัฐและภาคเอกชน เช่น กรมอนามัย มหาวิทยาลัยมหิดล มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ชมรมบริหารบุคคลไทยเอชอาร์ออนไลน์ เป็นต้น

ผู้สัมภาษณ์ : สวัสดีค่ะ นางสาวปรารถนา สุวรรณศักดิ์ นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ ซึ่งทำหัวข้อการค้นคว้าอิสระเรื่องปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวในภาคธุรกิจประกันภัย วันนี้จะมาขอสัมภาษณ์คุณสุวรรณโชติเกี่ยวกับความเห็นของคุณสุวรรณโชติสำหรับการจัดการข้อมูลส่วนบุคคลในภาคธุรกิจประกันภัย โดยเฉพาะการจัดการตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

คุณสุวรรณโชติ : ครับ ยินดีครับ

ผู้สัมภาษณ์ : ข้อแรกขอสอบถามความคิดเห็นของคุณสุวรรณโชติในเรื่องของการที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยออกประกาศมาให้บริษัทประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัยสามารถเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของลูกค้าเพื่อการรับประกันภัย การชดใช้ค่าสินไหมทดแทน โดยอาศัยฐานการจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ และไม่ต้องขอความยินยอมจากลูกค้า คุณสุวรรณโชติมีความคิดเห็นเป็นอย่างไรกับเรื่องนี้คะ

คุณสุวรรณโชติ : โดยส่วนตัวผมคิดว่าต้องกลับไปดูก่อนว่าทำไมกฎหมายถึงให้ขอความยินยอม ซึ่งจากกฎหมายหลายฉบับ ทั้ง GDPR และ CCPA เกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว

Ref. code: 25646301033624ADV

มีข้อกำหนดที่จะต้องให้ขอความยินยอมกับการใช้ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อที่จะให้เจ้าของข้อมูลได้ตระหนักว่ามีการให้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวกับบุคคลนั้นๆ ซึ่งหากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยออกกฎหมายมาในลักษณะนี้ ผมมีความเห็นว่าอาจจะไม่ค่อยเป็นธรรมกับเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะสำหรับผู้ที่ค่อนข้างใส่ใจในเรื่องสิทธิในข้อมูลส่วนบุคคล ซึ่งถ้าเป็นผม ผมก็จะถามหาการขอความยินยอมนะครับ ผมยังมองว่าเป็นเรื่องไม่ควรละเว้นเพราะกฎหมายมีเจตนารมณ์แน่นอนว่าป้องกันเรื่องการเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ผู้สัมภาษณ์ : ในประเด็นการบ่งชี้ว่าการประกันภัยเป็นประโยชน์สาธารณะที่สำคัญ คุณสุวรรณโชติ มีความคิดเห็นต่อเรื่องนี้เป็นอย่างไรคะ

คุณสุวรรณโชติ : ผมมองว่ายังเป็นเรื่องที่ต้องไปชั่งน้ำหนักดูในหลายๆมิติ อาจไม่ใช่เพียงแค่เจ้าของข้อมูลหรือผู้ควบคุมข้อมูลได้ประโยชน์เพียงอย่างเดียว ยังมีอีกหลายมิติที่จะต้องคำนึงถึง ซึ่งผมมองว่าการระบุว่าประกันภัยเป็นประโยชน์สาธารณะยังไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และไม่สอดคล้องกับหลักการการคุ้มครองข้อมูลส่วนบุคคล ถ้าคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยออกประกาศในลักษณะนี้แล้ว คิดว่าในภาคธุรกิจอื่นๆ ก็อาจจะอยากที่จะออกประกาศมายกเว้นการขอความยินยอมเช่นกัน แต่ผมไม่แน่ใจว่าในต่างประเทศมีแนวปฏิบัติอย่างไรสำหรับภาคธุรกิจประกันภัย

ผู้สัมภาษณ์ : จากที่ศึกษามาทางคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยน่าจะนำแนวปฏิบัติในเรื่องการการบ่งชี้ว่าการประกันภัยเป็นประโยชน์สาธารณะ มาจาก Data Protection Act 2018 ของประเทศอังกฤษค่ะ

คุณสุวรรณโชติ : แต่ในสหภาพยุโรปตาม GENERAL DATA PROTECTION REGULATION (GDPR) ไม่ได้เป็นแนวทางเดียวกันนะครับ ถ้ามองย้อนไปถึงกฎหมายที่เป็นที่มาของ GDPR ก็จะเห็นว่า GDPR ดูครอบคุลมกว่า Data Protection Act 2018 โดยเฉพาะในเรื่องของสิทธิ เสรีภาพ

ผู้สัมภาษณ์ : ทางคุณสุวรรณโชติมีความคิดเห็นว่าประกาศที่บ่งชี้ว่าการประกันภัยเป็นประโยชน์สาธารณะควรออกมาจากคณะกรรมการข้อมูลส่วนบุคคลหรือไม่คะ

คุณสุวรรณโชติ : ผมมองว่าด้วยความที่เป็นเรื่องข้อมูลส่วนบุคคลที่มีความอ่อนไหว ก็ควรเป็นคณะกรรมการข้อมูลส่วนบุคคลที่ออกกฎหมาย แต่ก็ต้องถามว่าคณะกรรมการข้อมูลส่วนบุคคลเข้าใจหรือมองเรื่องนี้ในมิติไหน เพราะการบังคับใช้ก็จะถูกบังคับใช้กับทุกคน ซึ่งก็จะมีทั้งคนที่ให้ความสำคัญในเรื่องข้อมูลส่วนบุคคล และคนที่ไม่ให้ความสำคัญในเรื่องนี้เลย ซึ่งถ้าถามผมผมยังอยากให้มีการขอความยินยอมนะครับ แต่ถ้าประกาศออกมาจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็

Ref. code: 25646301033624ADV

ยอมรับได้ครับ แต่ก็ต้องมองไปถึงว่าถ้ามีเหตุการณ์ที่ข้อมูลส่วนบุคคลที่มีความอ่อนไหวหลุดไปจากกลุ่มธุรกิจประกันภัยเราจะไปป้องกันและควบคุมอย่างไร

ผู้สัมภาษณ์ : คุณสุวรรณโชติก็ยังให้ความสำคัญกับเรื่องการขอความยินยอมเป็นหลักถูกต้องหรือไม่คะ

คุณสุวรรณโชติ : ใช่ครับ ผมมองว่าข้อมูลส่วนบุคคลก็เหมือนทรัพย์สินของเราที่ไม่ใช่ว่าหน่วยงานใดจะเอาไปทำอะไรก็ได้ ทำให้ผมให้ความสำคัญในเรื่องความยินยอม แต่ก็เข้าใจว่าอีกมุมหนึ่งหากต้องทำความยินยอมก็อาจจะเป็นเรื่องยุ่งยาก แต่ก็ต้องหาทางออกร่วมกันเพราะต้องบอกว่าการทำให้เกิดความปลอดภัยของข้อมูลอาจจะอยู่ตรงข้ามกับความสะดวกสบาย

ผู้สัมภาษณ์: ขอขอบคุณคุณสุวรรณโชตินะคะที่มาช่วยให้สัมภาษณ์ในวันนี้

สัมภาษณ์โดย นางสาวปรารถนา สุวรรณศักดิ์

Ref. code: 25646301033624ADV

ภาคผนวก จ

บันทึกการสัมภาษณ์ คุณรุ่งเรือง สัมฤทธิ์ทรัพย์

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน)

สัมภาษณ์ทาง Google Meet วันที่ 18 กรกฎาคม 2565 เวลา 12.20-12.40 น.

คุณรุ่งเรือง สัมฤทธิ์ทรัพย์ เป็นเจ้าหน้าที่เทคโนโลยีสารสนเทศอาวุโส และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน) โดยทำหน้าที่ติดตามตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในบริษัท รวมถึง ให้คำปรึกษาแก่ผู้บริหารและพนักงานฝ่ายต่างๆ เพื่อปฏิบัติให้ถูกต้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผู้สัมภาษณ์ : สวัสดีค่ะ นางสาวปรารถนา สุวรรณศักดิ์ นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ ซึ่งทำหัวข้อการค้นคว้าอิสระเรื่องปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวในภาคธุรกิจประกันภัย วันนี้จะมาขออนุญาตสัมภาษณ์คุณรุ่งเรืองเกี่ยวกับการจัดการข้อมูลส่วนบุคคลในภาคธุรกิจประกันภัยค่ะ

คุณรุ่งเรือง : สวัสดีครับ ผมรุ่งเรือง สัมฤทธิ์ทรัพย์ครับ เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทครับ

ผู้สัมภาษณ์: คุณรุ่งเรือง ได้มีโอกาสอ่านประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 บ้างหรือยังคะ

คุณรุ่งเรือง: ได้ศึกษามาบ้างแล้วครับ

ผู้สัมภาษณ์: มีหนึ่งเรื่องซึ่งทางปรารถนากำลังทำการค้นคว้าอิสระอยู่ คือเรื่องการที่บริษัทประกันภัย นายหน้าประกันภัย หรือตัวแทนประกันภัยจะสามารถเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อวัตถุประสงค์ในการประกันภัยที่จำเป็นโดยไม่ต้องขอความยินยอม ไม่แน่ใจว่าทางคุณรุ่งเรืองมีความเห็นว่าอย่างไรคะ

คุณรุ่งเรือง: สำหรับประเด็นนี้ ผมเองได้ติดตามและมีโอกาสได้เข้าร่วมสัมมนาของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหลายครั้งนะครับ ก็เห็นมีการยกประเด็นขึ้นมาพูดคุยกันไม่น้อยครับ แต่ในเมื่อผู้ออกประกาศเป็นหน่วยงานกำกับดูแลของธุรกิจประกันภัย ผู้อยู่ใต้การกำกับดูแลก็มีหน้าที่ต้องเดินตามแนวทางปฏิบัตินั้น ซึ่งก็ต้องบอกว่าบริษัทเราก็มีมาตรการในการปฏิบัติตามนั้นนะครับ ถ้าถามในมุมผู้ปฏิบัติงานผมว่าการที่บริษัทประกันภัย นายหน้าประกันภัยต้องมาขอความยินยอมในข้อมูลที่จำเป็นต้องมีเพื่อรับประกันภัย ก็ค่อนข้างแปลกครับ การมีประกาศมายกเว้นแบบนี้ก็ทำให้ผู้ปฏิบัติงานทำงานได้ง่ายขึ้น ไม่สร้างขั้นตอนการทำงานเพิ่ม

Ref. code: 25646301033624ADV

ผู้สัมภาษณ์: ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยที่กล่าวถึง มีการยกเว้นการขอความยินยอมโดยอาศัย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 มาตรา 26 (5) (จ) คือฐานความจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญ ถ้าหากบอกว่าประกันภัย เป็น ประโยชน์สาธารณะที่สำคัญ ทางคุณรุ่งเรืองมีความเห็นว่าอย่างไรคะ

คุณรุ่งเรือง: ถ้าจะบอกว่าการประกันภัยเป็นประโยชน์สาธารณะที่สำคัญก็อาจจะทำได้ครับ แต่ก็ต้องบอกว่าถ้าในฐานะบุคคลทั่วไปเมื่อพูดถึงประโยชน์สาธารณะแล้ว เราก็อาจจะนึกถึงการดำเนินการของภาครัฐมากกว่า และการประกันภัยอาจไม่ใช่สิ่งที่คนทั่วไปจะนึกถึงในฐานะประโยชน์สาธารณะครับ ซึ่งพอ คปภ. ออกประกาศว่าเป็นประโยชน์สาธารณะผมก็ว่าก็ชัดเจนว่าการประกันภัยเป็นประโยชน์สาธารณะที่สำคัญอย่างหนึ่งนะครับ

ผู้สัมภาษณ์: สุดท้ายขอสอบถามถึงการดำเนินการในบริษัทที่คุณรุ่งเรืองสังกัดอยู่ ว่าในบริษัทเองมีการขอความยินยอมเพื่อเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่ขอความยินยอมตามประกาศ คปภ. ที่เรากล่าวถึงมาหรือไม่คะ

คุณรุ่งเรือง: ต้องออกตัวก่อนว่าบริษัทจะเน้นขายประกันรถยนต์เป็นหลักนะครับ ซึ่งอาจมีการขายประกันอื่นๆ บ้างเมื่อลูกค้าสอบถามรายละเอียด หรือขอซื้อประกันบางชนิด เช่น พวกประกันโควิด-19 ในช่วงปีที่แล้ว แต่ตั้งแต่ 1 มิถุนายนปีนี้มา เรายังคงโฟกัสที่ประกันรถยนต์ซึ่งไม่มีการเก็บพวกข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงไม่ได้มีการขอความยินยอม ความยินยอมที่พบส่วนมากตอนนี้จะเป็นการขอความยินยอมเพื่อการขายมากกว่า ส่วนในภาคธุรกิจประกันภัยนั้น ข้อมูลส่วนใหญ่จะสามารถเก็บ ใช้ เปิดเผยได้ตามฐานสัญญาครับ

ผู้สัมภาษณ์: ขอขอบคุณคุณรุ่งเรืองนะคะที่มาช่วยให้สัมภาษณ์ในวันนี้

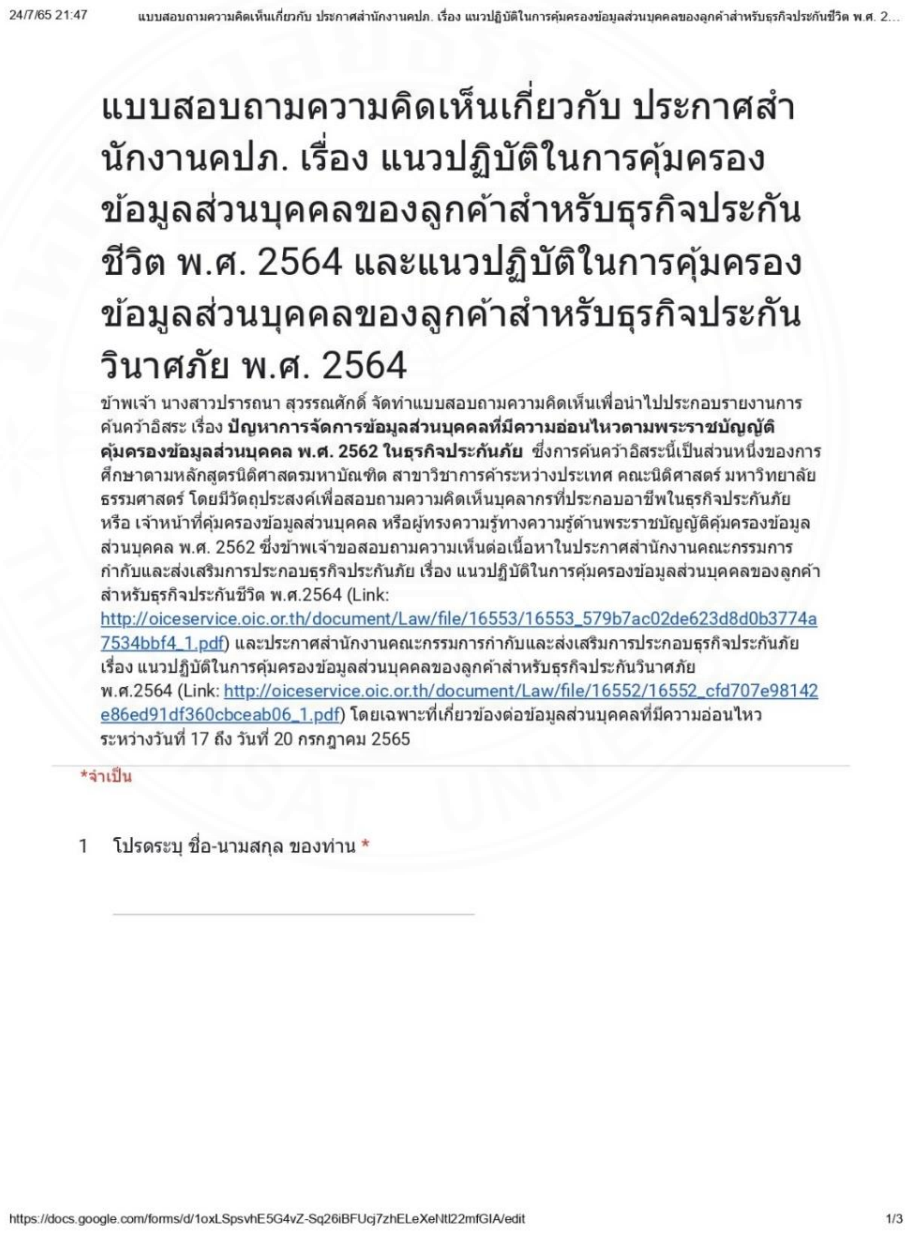
สัมภาษณ์โดย นางสาวปรารถนา สุวรรณศักดิ์

Ref. code: 25646301033624ADV

ภาคผนวก ฉ

ผลสำรวจการตอบแบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

แบบสอบถามสำรวจความคิดเห็นผ่าน Google Form ระหว่างวันที่ 17 ถึง 20 กรกฎาคม 2565



24/7/65 21:47 แบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2...

แบบสอบถามความคิดเห็นเกี่ยวกับ ประกาศสำนักงานคปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ. 2564 และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564

ข้าพเจ้า นางสาวปรารถนา สุวรรณศักดิ์ จัดทำแบบสอบถามความคิดเห็นเพื่อนำไปประกอบรายงานการค้นคว้าอิสระ เรื่อง **ปัญหาการจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในธุรกิจประกันภัย** ซึ่งการค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต สาขาวิชาการค้าระหว่างประเทศ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ โดยมีวัตถุประสงค์เพื่อสอบถามความคิดเห็นบุคลากรที่ประกอบอาชีพในธุรกิจประกันภัย หรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้ทรงความรู้ทางความรู้ด้านพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งข้าพเจ้าขอสอบถามความเห็นต่อเนื้อหาในประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันชีวิต พ.ศ.2564 (Link: http://oiceservice.oic.or.th/document/Law/file/16553/16553_579b7ac02de623d8d0b3774a7534bbf4_1.pdf) และประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ.2564 (Link: http://oiceservice.oic.or.th/document/Law/file/16552/16552_cfd707e98142e86ed91df360cbceab06_1.pdf) โดยเฉพาะที่เกี่ยวข้องต่อข้อมูลส่วนบุคคลที่มีความอ่อนไหว ระหว่างวันที่ 17 ถึง วันที่ 20 กรกฎาคม 2565

*จำเป็น

1 โปรดระบุ ชื่อ-นามสกุล ของท่าน *

https://docs.google.com/forms/d/1oxLSpsvhE5G4vZ-Sq26iBFUcj7zhELeXeNtl22mfGIA/edit 1/3

Ref. code: 25646301033624ADV

2 ท่านคือ *

ทำเครื่องหมายเพียงหนึ่งช่อง

- ผู้ประกอบอาชีพในบริษัทประกันชีวิตหรือบริษัทประกันวินาศภัย
- ตัวแทนประกันชีวิตหรือตัวแทนประกันวินาศภัย
- ผู้ประกอบอาชีพในบริษัทนายหน้าประกันภัย
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3 1. ตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา ท่านพบการขอความยินยอมเพื่อเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำประกันภัยหรือไม่ *

ทำเครื่องหมายเพียงหนึ่งช่อง

- พบ
- ไม่พบ
- ยังมิได้มีการทำสัญญาประกันภัยหลัง ตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา

4 2. ท่านมีความคิดเห็นว่าการรับประกันภัยเป็นประโยชน์สาธารณะที่สำคัญหรือไม่ *

ทำเครื่องหมายเพียงหนึ่งช่อง

- ใช่
- ไม่ใช่
- อื่นๆ: _____

Ref. code: 25646301033624ADV

5 3. ตามประกาศสำนักงาน คปภ. ที่อ้างถึงในคำอธิบายนั้น มีการกำหนดให้การที่บริษัทประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัย อาจเก็บ ใช้ เปิดเผย ข้อมูลสุขภาพของลูกค้าและบุคคลอื่นที่จำเป็น เพื่อวัตถุประสงค์ในการพิจารณารับประกันภัย เอาประกันภัยต่อ การพิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัยโดยไม่ต้องขอความยินยอม ท่านเห็นด้วยหรือไม่ *

ทำเครื่องหมายเพียงหนึ่งช่อง

- ◯ เห็นด้วย
- ◯ ไม่เห็นด้วย
- ◯ อื่นๆ: _____

6 ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติม

_____

_____

_____

_____

_____

เนื้อหานี้มิได้ถูกสร้างขึ้นหรือรับรองโดย Google

Google ฟอร์ม

มีผู้ตอบแบบสอบถามซึ่งเป็นบุคลากรในบริษัทประกันภัย ทั้งหมด 11 ท่าน นายหน้าประกันภัยหรือบุคลากรในบริษัทนายหน้าประกันภัย ทั้งหมด 10 ท่าน ตัวแทนประกันภัย ทั้งหมด 6 ท่าน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 1 ท่าน และบุคลากรในฝ่ายงานกำกับการปฏิบัติตาม

Ref. code: 25646301033624ADV

กฎหมายในหน่วยงานต่างๆ ซึ่งเป็นผู้มีความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งหมด 19 ท่าน โดยมีผลการตอบแบบสอบถามทั้ง 3 ประเด็น ดังนี้

1. ตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา ท่านพบการขอความยินยอมเพื่อเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำประกันภัยหรือไม่

พบ 57.4% ไม่พบ 8.5% ยังไม่มีการทำสัญญา 34%

2. ท่านมีความคิดเห็นว่าการรับประกันภัยเป็นประโยชน์สาธารณะที่สำคัญหรือไม่

ใช่ 61.7% ไม่ใช่ 38.3%

3. ตามประกาศสำนักงาน คปภ. ที่อ้างถึงในคำอธิบายนั้น มีการกำหนดให้การที่บริษัทประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัย อาจเก็บ ใช้ เปิดเผย ข้อมูลสุขภาพของลูกค้าและบุคคลอื่นที่จำเป็น เพื่อวัตถุประสงค์ในการพิจารณารับประกันภัย เอาประกันภัยต่อ การพิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัยโดยไม่ต้องขอความยินยอม ท่านเห็นด้วยหรือไม่

เห็นด้วย 61.7% ไม่เห็นด้วย 38.3%

ทั้งนี้ มีรายละเอียดการตอบแบบสอบถาม จำแนกตามผู้ตอบแบบสอบถาม ดังนี้

1. ตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา ท่านพบการขอความยินยอมเพื่อเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวในการทำประกันภัยหรือไม่

กลุ่มผู้ตอบแบบสอบถาม	พบ	ไม่พบ	ยังไม่มีการทำสัญญา
ผู้ประกอบอาชีพในบริษัทประกันชีวิตหรือบริษัทประกันวินาศภัย	8	0	3
ตัวแทนประกันชีวิตหรือตัวแทนประกันวินาศภัย	5	1	0
ผู้ประกอบอาชีพในบริษัทนายหน้าประกันภัย / นายหน้าประกันภัย	6	2	2
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	1	0	0
ผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	7	2	10

Ref. code: 25646301033624ADV

2. ท่านมีความคิดเห็นว่าการรับประกันภัยเป็นประโยชน์สาธารณะที่สำคัญหรือไม่

กลุ่มผู้ตอบแบบสอบถาม	ใช่	ไม่ใช่
ผู้ประกอบอาชีพในบริษัทประกันชีวิตหรือบริษัทประกันวินาศภัย	10	1
ตัวแทนประกันชีวิตหรือตัวแทนประกันวินาศภัย	6	0
ผู้ประกอบอาชีพในบริษัทนายหน้าประกันภัย / นายหน้าประกันภัย	4	6
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	0	1
ผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	9	10

3. ตามประกาศสำนักงาน คปภ. ที่อ้างถึงในคำอธิบายนั้น มีการกำหนดให้การที่บริษัทประกันภัย นายหน้าประกันภัย และตัวแทนประกันภัย อาจเก็บ ใช้ เปิดเผย ข้อมูลสุขภาพของลูกค้าและบุคคลอื่นที่จำเป็น เพื่อวัตถุประสงค์ในการพิจารณารับประกันภัย เอาประกันภัยต่อ การพิจารณารับประกันภัยต่อ คำนวณเบี้ยประกันภัย ปฏิเสธการรับประกันภัย หรือชดใช้ค่าสินไหมทดแทนตามสัญญาประกันภัยโดยไม่ต้องขอความยินยอม ท่านเห็นด้วยหรือไม่

กลุ่มผู้ตอบแบบสอบถาม	เห็นด้วย	ไม่เห็นด้วย
ผู้ประกอบอาชีพในบริษัทประกันชีวิตหรือบริษัทประกันวินาศภัย	10	1
ตัวแทนประกันชีวิตหรือตัวแทนประกันวินาศภัย	5	1
ผู้ประกอบอาชีพในบริษัทนายหน้าประกันภัย / นายหน้าประกันภัย	5	5
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	0	1
ผู้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	9	10

Ref. code: 25646301033624ADV

ประวัติผู้เขียน

ชื่อ	ปรารถนา สุวรรณศักดิ์
วันเดือนปีเกิด	7 กันยายน พ.ศ. 2534
วุฒิการศึกษา	ปีการศึกษา 2555: นิติศาสตรบัณฑิต มหาวิทยาลัยรามคำแหง
ตำแหน่ง	ผู้จัดการฝ่ายกฎหมายและบริหารความเสี่ยง

Ref. code: 25646301033624ADV