



ผลกระทบบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย

โดย

นางสาวจตุพร บุญเหมย

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
บริหารธุรกิจมหาบัณฑิต
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2563
ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

ผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย

โดย

นางสาวจตุพร บุญเหมย



การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
บริหารธุรกิจมหาบัณฑิต
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2563
ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

THE IMPACT OF PERSONAL DATA PROTECTION ACT, B.E. 2562
ON COMMERCIAL BANKING INDUSTRY IN THAILAND

BY

MISS JATUPORN BOONMOEY



AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF BUSINESS ADMINISTRATION
FACULTY OF COMMERCE AND ACCOUNTANCY
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2020
COPYRIGHT OF THAMMASAT UNIVERSITY

มหาวิทยาลัยธรรมศาสตร์
คณะพาณิชยศาสตร์และการบัญชี

การค้นคว้าอิสระ

ของ

นางสาวจตุพร บุญเหมย

เรื่อง

ผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีต่อธุรกิจธนาคารพาณิชย์
ในประเทศไทย

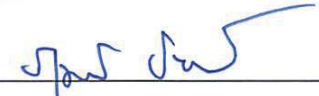
ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
บริหารธุรกิจมหาบัณฑิต

เมื่อ วันที่ 13 ธันวาคม 2563

ประธานกรรมการสอบการค้นคว้าอิสระ


(ผู้ช่วยศาสตราจารย์ ดร. ภิญดา เมธารมณ)

กรรมการและอาจารย์ที่ปรึกษาการค้นคว้าอิสระ


(อาจารย์ ดร. ภูมินันท์ ปิยทัตน์นันท์)

คณบดี


(รองศาสตราจารย์ ดร. รุธีร์ พนมยงค์)

หัวข้อการค้นคว้าอิสระ	ผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย
ชื่อผู้เขียน	นางสาวจตุพร บุญเหมย
ชื่อปริญญา	บริหารธุรกิจมหาบัณฑิต
คณะ/มหาวิทยาลัย	คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ	อาจารย์ ดร. ภูมิรัตน์ ปิยทัศน์นันท์
ปีการศึกษา	2563

บทคัดย่อ

การวิจัยเรื่องผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย มีวัตถุประสงค์เพื่อศึกษาถึงผลกระทบที่เกิดขึ้นต่อปัจจัยในด้านต่าง ๆ ขององค์กร และศึกษาถึงแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย รวมถึงแนวทางการพัฒนาการบริหารองค์กรภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) เก็บข้อมูลผ่านการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้บริหารและเจ้าหน้าที่ที่ปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของธนาคารพาณิชย์ นอกจากนี้ยังมีการสัมภาษณ์เชิงลึกกับ ผู้เชี่ยวชาญทางด้านกฎหมาย ผู้เชี่ยวชาญทางด้านบริหารจัดการข้อมูล และหน่วยงานกำกับดูแล

ผลการศึกษาพบว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ทั้งในภาพรวมของอุตสาหกรรมและในระดับองค์กร โดยในภาพรวมของอุตสาหกรรมเป็นการเพิ่มโอกาสการแข่งขันในระดับสากล เสริมสร้างความเชื่อมั่นและความแข็งแกร่งให้กับภาคธุรกิจ และคุณภาพของข้อมูลส่วนบุคคลที่เพิ่มขึ้นซึ่งเป็นการเพิ่มประสิทธิภาพในการบริหารจัดการข้อมูลของธนาคารในยุคปัจจุบันแต่อย่างไรก็ตามกฎหมายก็อาจเป็นอุปสรรคในการพัฒนาภาคธุรกิจหากเกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาดที่ส่งผลกระทบต่อผู้เล่นขนาดกลางและขนาดเล็กรวมถึงการใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม ในระดับองค์กรนั้นกฎหมายได้ส่งผลกระทบทำให้ต้นทุนในการบริหารจัดการข้อมูลเพิ่มสูงขึ้นจากต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) ซึ่งเกิดจากการที่บริษัทต้องมีการปรับโครงสร้างองค์กร ทบทวนและปรับปรุงกระบวนการทำงานทั่วทั้งองค์กร พนักงานในองค์กรต้องรับภาระงานเพิ่มหรือต้องมีการ

สรรหาพนักงานใหม่ รวมถึงมีการอบรมให้ความรู้แก่พนักงานและเพิ่มทักษะด้านการใช้ข้อมูล (Data Literacy) นอกจากนี้ยังมีการปรับปรุงและลงทุนในเทคโนโลยีใหม่ ๆ เพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ในขณะเดียวกันแม้ว่าลูกค้าจะได้รับสิทธิในการคุ้มครองข้อมูลส่วนบุคคลแต่ก็ต้องแลกกับค่าบริการที่เพิ่มขึ้นในรูปแบบของต้นทุนแฝงจากอัตราดอกเบี้ยเงินกู้ที่เพิ่มขึ้น หรือปรับลดอัตราดอกเบี้ยเงินฝากเพื่อที่ธนาคารจะสามารถชดเชยต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามกฎหมาย

สำหรับแนวทางการบริหารจัดการองค์กรเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามกฎหมายควบคู่กับการดำเนินธุรกิจอย่างมีประสิทธิภาพนั้นต้องมีการบริหารจัดการทั้งปัจจัยภายในและภายนอกองค์กร ปัจจัยภายในองค์กรมีองค์ประกอบสำคัญ 3 องค์ประกอบ ได้แก่ คน (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ซึ่งบริษัทจะต้องบริหารทุกองค์ประกอบให้มีความสอดคล้องกันและเป็นไปตามกลยุทธ์และนโยบายขององค์กร ส่วนในมุมมองของลูกค้าการสื่อสารเป็นเรื่องที่สำคัญองค์กรจะต้องสื่อสารให้ลูกค้าตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลและให้ลูกค้ารู้สึกถึงประโยชน์ของการให้ความยินยอม รวมถึงสื่อสารเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความเชื่อมั่นในการให้ข้อมูลแก่บริษัทด้วย เช่นเดียวกันกับแนวทางการพัฒนาองค์กรเพื่อตอบรับการปฏิบัติตามกฎหมายการสื่อสารเป็นสิ่งสำคัญที่ทั้งภาครัฐและภาคเอกชนต้องร่วมมือกันให้ความรู้และสร้างความตระหนักรู้ (Awareness) เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ผู้บริโภคและพนักงานภายในองค์กร อีกทั้งในภาคธุรกิจธนาคารต้องจัดทำแนวทางการปฏิบัติงาน (Industry Guidelines) เพื่อเป็นมาตรฐานและแนวทางการปฏิบัติงานที่ชัดเจน รวมถึงองค์กรต้องมีการควบคุมติดตาม และประเมินผลการปฏิบัติงานหลังมีการปรับใช้กฎหมายอย่างเต็มรูปแบบเพื่อปรับปรุงกระบวนการอย่างต่อเนื่อง

ข้อเสนอแนะจากการศึกษาเพื่อสนับสนุนให้การบริหารจัดการองค์กรภายใต้การปฏิบัติตามกฎหมายมีประสิทธิภาพมากขึ้น นอกจากการออกแบบกระบวนการทำงานให้เป็นไปตามที่กฎหมายกำหนดแล้วองค์กรควรศึกษาถึงความคาดหวังของผู้บริโภคต่อการคุ้มครองข้อมูลส่วนบุคคลเพื่อนำมาปรับปรุงกระบวนการอย่างต่อเนื่อง ควบคู่กับการสื่อสารเรื่องการคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ

คำสำคัญ: การคุ้มครองข้อมูลส่วนบุคคล, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, ผลกระทบ, ธนาคารพาณิชย์

Independent Study Title	THE IMPACT OF PERSONAL DATA PROTECTION ACT, B.E. 2562 ON COMMERCIAL BANKING INDUSTRY IN THAILAND
Author	Miss Jatuporn Boonmoey
Degree	Master of Business Administration
Faculty/University	Faculty of Commerce and Accountancy Thammasat University
Independent Study Advisor	Bhuminan Piyathasanan, Ph.D.
Academic Year	2020

ABSTRACT

The research titled “The Impact of Personal Data Protection Act, B.E. 2562 on commercial banking industry in Thailand” aims to study the impact of the act on organizational influencing factors and the approach to the organizational management in response to the personal protection data law, as well as the approaches to organizational development in compliance with the Personal Data Protection Act, B.E. 2562. The research was conducted through the qualitative research methods and the in-depth interviews with the executives and officers whose works relate to the field of the personal data protection of commercial banks as well as the in-depth interviews with legal experts, data management experts and regulators.

According to the result of the study, Personal Data Protection Act, B.E. 2562 has some effects on the business sectors of the commercial banks in the aspects of the overall industry and organizations. As for the overall industry, greater international competitiveness and business confidence have been achieved in the business sector and its capacity and quality of the personal data have been strengthened, all of which result in the banks’ increased capacity of information administration and management in the present. However, the law is a probable impediment to the development of the business sector if the personal data

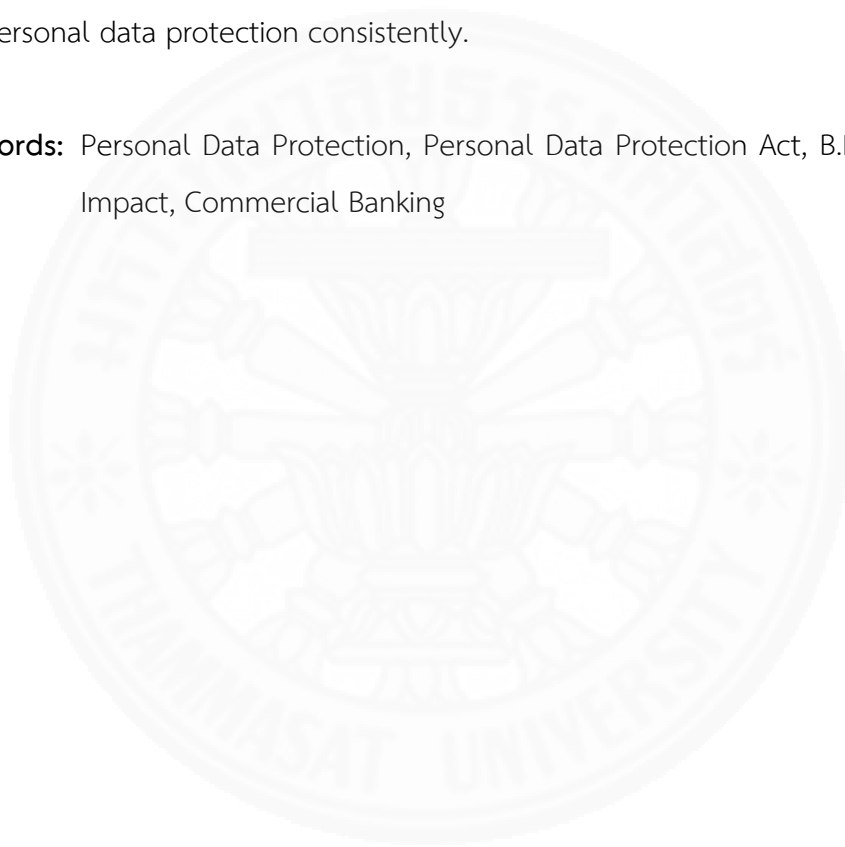
protection standards have been established by large companies, which will affect the medium and small-size players, and the data subject rights have been exercised improperly. As for the level of organizations, the imposition of the law has resulted in the higher cost of data management caused by the compliance cost, which is resulted from the organization's structural change, review and improvement of the whole work process. The organizations' employees have to bear more responsibilities or the organizations must recruit more employees and provide educational trainings to their employees and improve their employees' data literacy skill. Moreover, the organizations need to develop and invest in new technology in preparation for the compliance with the Personal Data Protection act. While the customers enjoy the right of personal data protection, they have to pay more in the form of implicit cost resulted from increased lending interest rates or decreased deposit interest rate so that this amount will compensate the compliance cost of the banks.

The approach to organizational management in order to implement the compliance policy and operate business effectively is the management of internal and external factors of the organizations. The internal factors include people, process and technology, all of which are the responsibilities of the organizations to manage them harmoniously and in compliance with the organizations' strategies and policies. In regard to customers, the communication is key to the organizations' success as the organizations are required to communicate with the customers so that they become aware of the personal data protection, the advantages of giving the organizations their consent to share their personal data and the standards of personal data protection to build their confidence in providing their data to the organizations. Accordingly, communication is listed in the approaches to organizational development in response to the organization's compliance with the law as the cooperation between the public and private sectors is required in educating and creating the customers and employees' awareness on the personal data protection. Additionally, in business sector, the banks need to set the industry guidelines to be applied as clear standards guidelines and need to control, monitor

and assess the performance after the law enters into forces in order to improve the work process continuously.

According to the study, there are some recommendations to effectively encourage the organizational management in compliance with the law. Apart from designing the work process as complying with the regulations, the organizations should study the expectation of the customers towards the personal data protection in order to develop the process continuously together with communicating about the personal data protection consistently.

Keywords: Personal Data Protection, Personal Data Protection Act, B.E. 2562 (2019), Impact, Commercial Banking



กิตติกรรมประกาศ

งานวิจัยเรื่อง “ผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย” ฉบับนี้สามารถสำเร็จลุล่วงไปได้ด้วยดี เนื่องจากได้รับความอนุเคราะห์จาก อาจารย์ ดร.ภูมิพันธ์ ปิยทัศน์นันท์ อาจารย์ที่ปรึกษาการวิจัยในครั้งนี้ ซึ่งต้องขอขอบคุณอาจารย์ที่ได้กรุณาสละเวลาในการให้คำปรึกษา ให้คำแนะนำที่เป็นประโยชน์ต่อกระบวนการค้นคว้าวิจัยและคอยติดตามงานอย่างใกล้ชิดมาโดยตลอด นอกจากนี้ผู้วิจัยยังต้องขอขอบคุณผู้ช่วยศาสตราจารย์ ดร.ภิญรดา เมธารมณี ประธานกรรมการสอบการค้นคว้าอิสระ ที่ให้คำแนะนำข้อเสนอแนะเพิ่มเติมที่เป็นประโยชน์ รวมถึงขอพระคุณอาจารย์โครงการปริญญาโทบริหารธุรกิจ คณะพาณิชยศาสตร์และการบัญชีทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชาความรู้ต่าง ๆ อันเป็นพื้นฐานสำคัญในการเรียนและการทำวิจัยในครั้งนี้ให้สำเร็จ

นอกจากนี้ผู้วิจัยต้องขอขอบคุณผู้ให้ข้อมูลเชิงลึกทั้ง 20 ท่าน ที่ได้สละเวลาอันมีค่ามาให้ข้อมูลที่เป็นประโยชน์ต่องานวิจัยฉบับนี้ ขอขอบคุณหัวหน้างานที่เข้าใจและให้ความช่วยเหลือเป็นอย่างดี อีกทั้งขอขอบคุณครอบครัว โดยเฉพาะคุณแม่ที่คอยให้การสนับสนุนทุกเรื่องมาโดยตลอด รวมถึงเพื่อนๆ MBA ที่คอยให้กำลังใจกัน ร่วมฝ่าฟันความยากลำบากร่วมกันมาตลอดระยะเวลาการศึกษา 2 ปี และที่ขาดไม่ได้เลยก็คือขอขอบคุณน้อง ๆ พี่ ๆ คนใกล้ชิดที่น่ารัก กล้าถามมิตรทุกท่าน ผู้ที่อยู่เบื้องหลังความสำเร็จ คอยช่วยเหลือทำให้งานวิจัยฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยนี้จะเป็นประโยชน์ต่อองค์กร และบุคคลทั่วไปที่สนใจ หากมีข้อบกพร่องหรือผิดพลาดประการใด ผู้วิจัยขอน้อมรับคำแนะนำติชมด้วยความยินดีทุกประการ

นางสาวจตุพร บุญเหมย

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	(1)
บทคัดย่อภาษาอังกฤษ	(3)
กิตติกรรมประกาศ	(6)
สารบัญตาราง	(14)
สารบัญภาพ	(15)
บทที่ 1 บทนำ	1
1.1 ที่มาและความสำคัญ	1
1.2 วัตถุประสงค์งานวิจัย	3
1.3 ขอบเขตการศึกษา	4
1.4 ประโยชน์ที่คาดว่าจะได้รับ	4
1.5 คำนิยามศัพท์ที่ใช้ในการวิจัย	5
บทที่ 2 การทบทวนวรรณกรรม	7
2.1 ธนาคารพาณิชย์ในประเทศไทย (Commercial Bank)	8
2.2 แนวทางการปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจธนาคาร	9
2.2.1 แนวทางการปฏิบัติสำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคล แก่ผู้บริโภคทางการเงินของธนาคารโลก	9
2.2.2 แนวทางการปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจ ธนาคารในประเทศไทย	10
2.2.2.1 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545	10

2.2.2.2 แนวปฏิบัติในการติดตามทางถามหนี้	11
2.2.2.3 ประกาศธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการ ด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)	11
(1) การดูแลรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า	11
(2) การเปิดเผยข้อมูลลูกค้าให้แก่บุคคลอื่น	11
(3) การเปิดเผยข้อมูลลูกค้าให้บุคคลอื่นเพื่อวัตถุประสงค์อื่นที่ไม่ใช่ การตลาด	11
2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019): PDPA)	12
2.3.1 หลักการและเหตุผล	13
2.3.2 แนวปฏิบัติพื้นฐานที่จำเป็นต่อการดำเนินการเพื่อการคุ้มครองข้อมูล ส่วนบุคคล	13
2.3.2.1 แนวปฏิบัติที่กำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline for Personal Data Classification)	13
(1) ขอบเขตของข้อมูลส่วนบุคคล	14
(2) การกำหนดและแยกแยะข้อมูลส่วนบุคคล	14
2.3.2.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล (Guideline on Lawful Basis for Processing Personal Data)	15
2.3.2.3 แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุม และผู้ประมวลผลข้อมูล (Guideline on Duties and Responsibilities of Controllers and Processors)	17
2.3.2.4 แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูล ส่วนบุคคล (Guideline on Data Protection Impact Assessment)	18
2.3.2.5 แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)	19
2.3.3 บทลงโทษ	19
2.3.3.1 ความรับผิดทางแพ่ง	19
2.3.3.2 ความรับผิดทางอาญา	20
2.3.3.3 โทษทางปกครอง	20

2.4 การบริหารการเปลี่ยนแปลง (Change Management)	21
2.4.1 ความหมายของการบริหารการเปลี่ยนแปลง	21
2.4.2 ปัจจัยที่ส่งผลให้เกิดการเปลี่ยนแปลง	21
2.5 การเปลี่ยนแปลงองค์การ (Organizational Change)	23
2.6 แนวคิดการบริหารคุณภาพในองค์กรอย่างต่อเนื่อง	24
2.7 งานวิจัยที่เกี่ยวข้อง	25
2.7.1 งานวิจัยแนวทางการดำเนินธุรกิจหลังมีการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล	25
2.7.1.1 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร	25
(1) ผลกระทบทางด้านต้นทุน (Cost)	26
(2) ผลกระทบทางด้านเทคโนโลยี (Technology)	26
(3) ผลกระทบทางด้านกระบวนการปฏิบัติงาน (Process)	27
(4) ผลกระทบทางด้านทรัพยากรบุคคล (Human Resource)	27
(5) ผลกระทบด้านรายได้ (Revenue)	28
2.7.1.2 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร	28
(1) ผลกระทบต่อลูกค้า (Customer)	28
(2) ผลกระทบต่อคู่ค้า (Supplier/Vendor)	29
2.7.1.3 แนวทางการบริหารองค์กรภายใต้การปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล	29
(1) การบริหารจัดการสภาพแวดล้อมภายในองค์กร	29
(2) การบริหารจัดการสภาพแวดล้อมภายนอกองค์กร	29
2.7.2 งานวิจัยแนวทางการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย	30
2.7.2.1 ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน	31
2.7.2.2 ลักษณะร่วมกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน	31
(1) การปฏิบัติตามมาตรฐานสากล (Standardization)	32
(2) การคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาทางเศรษฐกิจ	32
(3) การยอมรับมาตรฐานสากลและกรอบความร่วมมือระหว่างประเทศ	32

2.7.2.3 บทเรียนการเตรียมความพร้อมในการบังคับใช้กฎหมายคุ้มครอง ข้อมูลส่วนบุคคลของประเทศสิงคโปร์	32
2.7.2.4 ข้อเสนอการเตรียมความพร้อมเพื่อการบังคับใช้กฎหมายคุ้มครอง ข้อมูลส่วนบุคคลของประเทศไทย	33
2.8 กรอบแนวคิดการวิจัย	34
บทที่ 3 วิธีการวิจัย	36
3.1 แหล่งข้อมูลที่ใช้ในการวิจัย	36
3.1.1 ข้อมูลปฐมภูมิ (Primary Source)	36
3.1.2 ข้อมูลทุติยภูมิ (Secondary Source)	36
3.2 ลักษณะประชากร	37
3.3 กลุ่มตัวอย่างที่ใช้ในการวิจัย	37
3.4 เครื่องมือที่ใช้ในการวิจัย	38
3.4.1 การสัมภาษณ์เชิงลึก (In-Depth Interview)	38
3.4.2 การศึกษาข้อมูลจากแหล่งข้อมูลทุติยภูมิ (Secondary Source)	41
3.5 การเก็บรวบรวมข้อมูลและการวิเคราะห์ข้อมูล	42
บทที่ 4 ผลการวิจัย	43
4.1 ข้อมูลเบื้องต้นของกลุ่มตัวอย่าง	43
4.1.1 ข้อมูลของกลุ่มตัวอย่างผู้ให้ข้อมูลหลัก (Key Informants)	43
4.1.2 ข้อมูลของกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants)	44
4.2 ผลกระทบของธุรกิจธนาคารพาณิชย์จากพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562	45
4.2.1 ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562	46
4.2.1.1 ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงบวก	46
4.2.1.2 ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงลบ	47
(1) เกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดย บริษัทใหญ่ในตลาด	47

(2) การใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม	48
4.2.2 ผลกระทบในระดับองค์กรจากการปรับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	50
4.2.2.1 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร	50
(1) ผลกระทบต่อโครงสร้างองค์กร	50
(2) ผลกระทบต่อกลยุทธ์และนโยบายบริษัท	51
(3) ผลกระทบต่อกระบวนการปฏิบัติงาน	52
(4) ผลกระทบต่อทรัพยากรบุคคล	59
(5) ผลกระทบต่อเทคโนโลยี	62
(6) ผลกระทบรายได้และต้นทุนขององค์กร	65
4.2.1.2 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร	68
(1) ผลกระทบต่อลูกค้า	68
(2) ผลกระทบต่อคู่ค้า	69
4.3 แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคล ภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	70
4.3.1 ปัจจัยสภาพแวดล้อมภายในองค์กร	71
4.3.1.1 คน (People)	71
4.3.1.2 กระบวนการ (Process)	73
4.3.1.3 เทคโนโลยี (Technology)	74
4.3.2 ปัจจัยสภาพแวดล้อมภายนอกองค์กร	77
4.3.2.1 ลูกค้า (Customer)	77
4.3.2.2 คู่ค้า (Supplier/Vendor)	78
4.4 แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้ การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	78
4.4.1 มีแนวทางการปฏิบัติงานที่ชัดเจนสำหรับภาคธุรกิจ	79
4.4.2 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริหารและ พนักงานภายในองค์กร	81
4.4.3 การควบคุม ติดตาม และประเมินผลการปฏิบัติงานหลังมีการปรับใช้จริง เพื่อปรับปรุงกระบวนการงานอย่างต่อเนื่อง	82

บทที่ 5 สรุปผลวิจัย อภิปรายผลและข้อเสนอแนะ	84
5.1 การสรุปและอภิปรายผลการวิจัย	84
5.1.1 ผลกระทบของธุรกิจธนาคารพาณิชย์จากข้อบังคับตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	84
5.1.1.1 ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562	85
(1) ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงบวก	85
(2) ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงลบ	85
5.1.1.2 ผลกระทบในระดับองค์กรจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562	88
(1) ผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร	88
(2) ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร	103
5.1.2 แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูล ส่วนบุคคลภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	106
5.1.2.1 ปัจจัยสภาพแวดล้อมภายในองค์กร	106
(1) คน (People)	106
(2) กระบวนการ (Process)	107
(3) เทคโนโลยี (Technology)	108
5.1.2.2 ปัจจัยสภาพแวดล้อมภายนอกองค์กร	114
(1) ลูกค้า (Customer)	114
(2) คู่ค้า (Supplier/Vendor)	114
5.1.3 แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้ การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	116
5.1.3.1 มีแนวทางการปฏิบัติงานที่ชัดเจนสำหรับภาคธุรกิจ	116
5.1.3.2 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริโภค และพนักงานภายในองค์กร	117
5.1.3.3 การควบคุม ติดตาม และประเมินผลการปฏิบัติงาน หลังมีการปรับใช้จริงเพื่อปรับปรุงกระบวนการอย่างต่อเนื่อง	118

5.2 ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์	120
5.2.1 ประโยชน์ในการประยุกต์ใช้กับธุรกิจ (Implications for Business)	120
5.2.1.1 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริโภคและพนักงานภายในองค์กร	120
5.2.1.2 ภาครัฐกิจธนาคารพาณิชย์ควรมองความคาดหวังของผู้บริโภคต่อการคุ้มครองข้อมูลส่วนบุคคล	121
5.2.1.3 ต้องมีการควบคุม ตรวจสอบ และประเมินผลเพื่อปรับปรุงกระบวนการปฏิบัติงานอย่างต่อเนื่อง	121
5.2.2 ประโยชน์เชิงวิชาการ (Implication for Academic)	122
5.3 ข้อจำกัดของงานวิจัย	122
5.4 ข้อเสนอแนะในการทำวิจัยครั้งต่อไป	122
รายการอ้างอิง	124
ประวัติผู้เขียน	128

สารบัญตาราง

ตารางที่	หน้า
2.1 ธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทย	8
2.2 ธนาคารพาณิชย์เพื่อรายย่อย	9
2.3 ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ	9
2.4 สาขาของธนาคารต่างประเทศ	9
4.1 ข้อมูลเบื้องต้นของกลุ่มตัวอย่างผู้ให้ข้อมูลหลัก (Key Informants)	44
4.2 ข้อมูลเบื้องต้นของกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants)	44
4.3 สรุปการปรับปรุงกระบวนการปฏิบัติงานเดิม	53
4.4 สรุปกระบวนการปฏิบัติงานใหม่	58
5.1 สรุปผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล พ.ศ. 2562	87
5.2 สรุปผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร	96
5.3 สรุปผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร	105
5.4 สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (ปัจจัยสภาพแวดล้อมภายในองค์กร)	110
5.5 สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (ปัจจัยสภาพแวดล้อมภายนอกองค์กร)	115
5.6 สรุปแนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย	118

สารบัญภาพ

ภาพที่	หน้า
2.1 กรอบแนวคิดงานวิจัยเรื่องผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย	35



บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญ

จากการเข้าสู่ยุคดิจิทัล ทำให้ผู้คนในยุคปัจจุบันมีการแลกเปลี่ยนข้อมูลกันตลอดเวลา และมีการทำธุรกรรมต่าง ๆ ผ่านระบบออนไลน์มากขึ้น ผู้บริโภคได้เปิดเผยข้อมูลส่วนตัวไปกับการทำธุรกรรมต่าง ๆ มากมาย เช่น การติดต่อกับธนาคาร หน่วยงานบริการสุขภาพ การลงทะเบียนใช้งานผ่านอินเทอร์เน็ต หรือโซเชียลเน็ตเวิร์ก ซึ่งผู้บริโภคไม่สามารถทราบได้เลยว่าผู้ให้บริการออนไลน์หรือบริษัทต่าง ๆ เหล่านี้นำข้อมูลไปทำอะไรบ้าง ยิ่งในช่วงของการรักษาระยะห่างทางสังคม (Social Distancing) จากผลกระทบของโควิด-19 เป็นปัจจัยหนึ่งที่ทำให้เกิดการให้บริการเทคโนโลยีหลากหลายมากขึ้นและทำให้เกิดการเข้าถึงข้อมูลส่วนบุคคลเป็นจำนวนมาก เกิดคลังข้อมูล (Big Data) ที่มีประโยชน์ต่อภาคธุรกิจอย่างมากดังที่ Tim Berners-Lee ผู้สร้าง World Wide Web ได้ชี้ให้เห็นว่า “ข้อมูลจะเป็นวัตถุดิบชนิดใหม่ของศตวรรษที่ 21”

ผู้ประกอบการสามารถนำข้อมูลพฤติกรรมของผู้บริโภคมาวิเคราะห์พยากรณ์ความต้องการของผู้บริโภคเพื่อนำเสนอสินค้าและบริการได้ตรงกับกลุ่มเป้าหมายและตรงตามความต้องการของลูกค้ามากขึ้น สามารถช่วยเพิ่มยอดขายและสร้างโอกาสในการแข่งขันให้กับธุรกิจ โดยอาศัยข้อมูลชื่อ ที่อยู่ หมายเลขโทรศัพท์ พฤติกรรม การติดต่อสื่อสาร ที่สามารถระบุถึงตัวเจ้าของข้อมูลได้ (สุพิศ ประณีตพลกรัง, 2563) ในขณะเดียวกันก็เกิดการล่วงละเมิดข้อมูลส่วนบุคคลในการแสวงหาผลประโยชน์ทั้งในทางที่ดีและทางที่ไม่ดี ประกอบกับปัจจุบันโลกมีการถ่ายทอด โอน เชื่อมโยงข้อมูลกันอย่างหลากหลาย ทำให้ข้อมูลส่วนบุคคลมีการแพร่หลายและเกิดอาชญากรรมในรูปแบบต่าง ๆ

ดังนั้นในหลายประเทศจึงมีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล อาทิเช่น ประเทศในกลุ่มอาเซียน ได้แก่ ประเทศอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ เวียดนาม รวมถึงสหรัฐอเมริกาและสหภาพยุโรปก็มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน โดยสหภาพยุโรปได้ออกกฎหมาย General Data Protection Regulation (GDPR) บังคับใช้ในปี 2561 GDPR ทำให้ประเทศต่าง ๆ ที่มีการติดต่อทางธุรกิจกับประเทศในกลุ่มสหภาพยุโรปต้องมีการปรับปรุงกฎหมายการคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานเหมาะสมเพียงพอ ทัดเทียมกับกฎหมายของสหภาพยุโรป (สุพิศ ประณีตพลกรัง, 2563)

สำหรับประเทศไทยก็ได้มีการประกาศพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019): PDPA) โดยมีต้นแบบมาจาก GDPR

ของประเทศยุโรปเหตุผลในการประกาศใช้กฎหมายฉบับนี้เนื่องจากปัจจุบันมีการล่วงละเมิด สิทธิ ความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากประกอบกับความก้าวหน้าของเทคโนโลยีทำให้ การเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคลทำได้โดยง่าย สะดวกและรวดเร็วก่อให้เกิดการล่วง ละเมิดดังกล่าว (สุพิศ ประณีตพลกรัง, 2563) โดยใจความสำคัญของกฎหมายฉบับนี้มุ่งเน้นไปที่ องค์กร หน่วยงาน หรือนิติบุคคลให้มีมาตรฐานในการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและ เพียงพอ ซึ่งเดิม PDPA จะมีผลบังคับใช้อย่างเต็มรูปแบบในวันที่ 27 พฤษภาคม 2563 หากแต่ทุก ภาคส่วนยังไม่พร้อมและด้วยผลกระทบจากการแพร่ระบาดของโรคโควิด-19 ทำให้ภาคเอกชนไม่ว่า ขนาดใหญ่ ขนาดกลาง และขนาดเล็ก เกิดปัญหาสภาพคล่องในการลงทุนเพื่อปรับปรุงกระบวนการ ระบบสารสนเทศ และการจัดหาหรือจัดอบรมบุคลากรที่มีความรู้ความสามารถด้านการคุ้มครองข้อมูล ส่วนบุคคลให้มีความพร้อมปฏิบัติตามกฎหมาย จึงได้เลื่อนการบังคับใช้อย่างเต็มรูปแบบออกไปเป็น เวลา 1 ปี (ประชาชาติธุรกิจ, 2563)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลกับธุรกิจในยุคดิจิทัลยังต้อง ใช้ข้อมูลดิจิทัลมากเท่าใดก็ยิ่งทำให้เกิดประเด็นการบริหารจัดการเกี่ยวกับข้อมูลที่ตนเองใช้โดยเฉพาะ อย่างยิ่งการบริหารความเสี่ยงของการใช้ข้อมูลซึ่งรวมถึงข้อมูลส่วนบุคคล (ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจารุญลาภ, พิชพร ลิขิตพัฒน์ไพบูลย์, ชวิน อุ่นภัทร และฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, 2562) โดยเฉพาะในภาคการธนาคารที่ถือว่าเป็นปัจจัยในการพัฒนาเศรษฐกิจโดยรวมของประเทศและ นับเป็นหนึ่งในธุรกิจที่มีข้อมูลของลูกค้าอยู่ในมือมากเป็นลำดับต้น ๆ นอกจากนี้ยังเป็นธุรกิจที่มีการ ลงทุนด้านเทคโนโลยีอย่างสม่ำเสมอ (พิชพร ลิขิตพัฒน์ไพบูลย์ และณัฐพล เลิศเมธพัฒน์, 2562) ซึ่ง ปัจจัยหนึ่งที่จะทำให้เทคโนโลยีทางการเงินประสบความสำเร็จคือการเตรียมความพร้อมข้อมูล โดยคำนึงถึงสิทธิส่วนบุคคล โดยเมื่อไม่นานมานี้มีการรายงานเรื่องความปลอดภัยและความเป็น ส่วนตัวของข้อมูลจากการสำรวจผู้บริโภคในประเทศฝรั่งเศส เยอรมนี อิตาลี อังกฤษ และ สหรัฐอเมริกาพบว่าเจ้าของข้อมูลกังวลกับการสูญหายของข้อมูลทางการเงินธนาคารและจะดำเนิน บริษัทเมื่อข้อมูลสูญหายแทนการกล่าวโทษแฮกเกอร์และบอยคอตบริษัทที่ไม่ให้ความสำคัญกับการ ปกป้องข้อมูลลูกค้าแต่จะเลือกใช้บริการกับบริษัทที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล (วิชญ์ วงศ์หาญเชาว์, 2562)

ดังนั้นปัจจัยที่สำคัญที่สุดด้านข้อมูลคือการสร้างความเชื่อมั่นระหว่างเจ้าของข้อมูลกับผู้ ที่นำข้อมูลไปใช้โดยการเปิดเผยข้อมูลจะทำให้เจ้าของข้อมูลได้รับประโยชน์จากคุณภาพการบริการที่ดี ขึ้นและผลิตภัณฑ์ที่ตรงความต้องการของผู้บริโภคมากขึ้นซึ่งหากผู้ประกอบการสามารถปรับตัวได้ก็จะ เป็นการสร้างโอกาสทางการแข่งขันที่มากขึ้น (พิชพร ลิขิตพัฒน์ไพบูลย์ และณัฐพล เลิศเมธพัฒน์, 2562)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำลังจะมีผลบังคับใช้อย่างเต็มรูปแบบในปี 2564 นั้น จะเข้ามาเปลี่ยนแปลงและเป็นตัวแปรสำคัญที่จะส่งผลกระทบต่อกระบวนการทำงานด้านการวิเคราะห์ข้อมูล (Data Analytics) ตั้งแต่การจัดเก็บข้อมูล ไปจนถึงการนำข้อมูลไปใช้งานข้อมูลนั้นถือเป็นสินทรัพย์สำคัญขององค์กรโดยเฉพาะธุรกิจที่มีการจัดเก็บข้อมูลลูกค้าเป็นจำนวนมากอย่างภาคการธนาคารที่จะสามารถนำมาสร้างเป็น Insight ช่วยให้องค์กรรู้จักตัวเองและลูกค้าอย่างแท้จริง อีกทั้งข้อมูลส่วนบุคคลถือเป็นหัวใจสำคัญในการทำ Big Data Analytics เพื่อหาสิ่งเชื่อมโยงของข้อมูลเหล่านั้นและนำไปค้นหาแนวทางการตลาด หาความต้องการของลูกค้า รวมทั้งข้อมูลอื่น ๆ ที่เป็นประโยชน์ต่อธุรกิจ ซึ่งเมื่อถึงวันที่กฎหมายดังกล่าวถูกบังคับใช้องค์กรจะต้องดำเนินการจัดเก็บและใช้ข้อมูลส่วนบุคคลให้ถูกต้องและรัดกุม (พชร อารยะการกุล, 2563) โดยบริษัทต้องทำความเข้าใจในข้อกำหนด รวมถึงสิทธิและหน้าที่ต่าง ๆ ไม่ว่าจะเป็นเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงมีการสื่อสารให้ลูกค้าและพนักงานได้รับทราบถึงผลกระทบที่อาจเกิดขึ้นด้วยซึ่งการจะได้รับข้อมูลส่วนบุคคลนั้นจำเป็นต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลทำให้การได้มาซึ่งข้อมูลส่วนบุคคลของลูกค้าไม่ได้เป็นเรื่องง่ายอีกต่อไปและส่งผลต่อการใช้ประโยชน์จากข้อมูลส่วนบุคคลเพื่อเพิ่มประสิทธิภาพในการดำเนินงานด้านต่าง ๆ ถือเป็นความท้าทายต่อทุกภาคธุรกิจรวมถึงธนาคารพาณิชย์ที่มีข้อมูลส่วนบุคคลของลูกค้าจำนวนมากจากกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีความเข้มงวดขึ้น

ดังนั้นการศึกษาผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อธุรกิจธนาคารพาณิชย์ รวมถึงแนวทางการปรับตัวและการประยุกต์ใช้เมื่อต้องปฏิบัติงานตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวทางการพัฒนาการบริหารองค์กรภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงเป็นประโยชน์ต่อภาคธุรกิจการเงินและภาคธุรกิจอื่น ๆ ที่จะได้ทราบถึงผลกระทบที่เกิดขึ้นเพื่อเตรียมพร้อมรับมือกับสถานการณ์ในอนาคต และสามารถนำไปเป็นแนวทางในการปรับตัว รวมถึงแนวทางในการพัฒนาธุรกิจจากการประยุกต์ใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2 วัตถุประสงค์งานวิจัย

1.2.1 เพื่อศึกษาผลกระทบของธุรกิจธนาคารพาณิชย์จากข้อบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2.2 เพื่อศึกษาแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคารพาณิชย์ภายใต้ข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2.3 เพื่อศึกษาแนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.3 ขอบเขตการศึกษา

1.3.1 งานวิจัยในครั้งนี้ได้ทำการสัมภาษณ์ผู้บริหารและเจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยภายใต้การกำกับดูแลโดยธนาคารแห่งประเทศไทยเท่านั้น

1.3.2 ทำการสัมภาษณ์ผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร เช่น ผู้เชี่ยวชาญทางด้านกฎหมาย ผู้ปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานกำกับดูแลภาคธุรกิจ บริษัทที่ให้บริการด้านการคุ้มครองข้อมูลส่วนบุคคลและบริหารจัดการข้อมูล เป็นต้น

1.3.3 เป็นข้อมูลที่ได้จากการศึกษาข้อมูลจากแหล่งข้อมูลทุติยภูมิ อาทิเช่น บทความวิชาการที่เกี่ยวข้อง งานวิจัย อินเทอร์เน็ต โดยเก็บรวบรวมข้อมูลจากเอกสารที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นโยบายความเป็นส่วนตัว (Privacy Policy) ของแต่ละธนาคารและหนังสือให้ความยินยอมในการเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคล (Letter of Consent) เป็นต้น

1.3.4 ระยะเวลาที่ใช้ในการสัมภาษณ์ผู้บริหาร เจ้าหน้าที่ ผู้เชี่ยวชาญและหน่วยงานที่เกี่ยวข้องกับธุรกิจธนาคารอยู่ระหว่างช่วงเดือน ตุลาคม 2563 - พฤศจิกายน 2563 ซึ่งเป็นช่วงที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่ได้มีผลบังคับใช้อย่างเต็มรูปแบบ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

งานวิจัยดังกล่าวเป็นประโยชน์ต่อกลุ่มธุรกิจธนาคารพาณิชย์ซึ่งได้ทราบถึงผลกระทบของธุรกิจจากพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แนวทางการบริหารจัดการและการพัฒนาองค์กรภายใต้ข้อกำหนดของกฎหมายดังกล่าวเพื่อสามารถดำเนินธุรกิจได้อย่างมีประสิทธิภาพ เพิ่มโอกาสในการแข่งขันจากการใช้ข้อมูลควบคู่ไปกับจริยธรรมในการใช้ข้อมูลส่งเสริมการบริหารงานอย่างยั่งยืน อีกทั้งยังเป็นแนวทางในการบริหารจัดการและพัฒนาองค์กรให้กับภาคธุรกิจอื่น ๆ อีกด้วย นอกจากนี้ยังรวมถึงประโยชน์ทางด้านวิชาการโดยงานวิจัยนี้สามารถนำไปใช้ประโยชน์ให้ผู้ที่สนใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ประยุกต์ใช้กับธุรกิจธนาคารและสามารถนำไปต่อยอดการศึกษาจาก

งานวิจัยนี้เพื่อศึกษาเพิ่มเติมหลังกฎหมายมีการบังคับใช้อย่างเต็มรูปแบบหรือศึกษาเพิ่มเติมในภาคอุตสาหกรรมอื่นต่อไป

1.5 คำนิยามศัพท์ที่ใช้ในการวิจัย

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019): PDPA) คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยซึ่งจะมีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2564 โดยประเด็นหลักของกฎหมาย คือ การเก็บ ใช้เปิดเผย และถ่ายโอนข้อมูลส่วนบุคคลต้องได้รับความยินยอม และการกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

General Data Protection Regulation (GDPR) คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเพื่อตอบรับกระแสของการใช้อินเทอร์เน็ต ธุรกิจ E-commerce การโฆษณา และการตลาดออนไลน์ในโลกยุคดิจิทัล (Techtalkthai, 2561)

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลใด ๆ ที่สามารถระบุไปถึงเจ้าของข้อมูล (Data Subject) ได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม ตัวอย่างเช่น ชื่อ - นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, รูปภาพ, ข้อมูลทางการเงิน เป็นต้น (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวของบุคคล แต่มีความละเอียดอ่อนและเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์, เชื้อชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพแรงงาน เป็นต้น (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

ผู้ควบคุมข้อมูล (Data Controller) คือ บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

ผู้ประมวลผลข้อมูล (Data Processor) คือ บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) คือ บุคคลที่องค์กรแต่งตั้งขึ้นเพื่อรับผิดชอบในการดูแลข้อมูลส่วนบุคคลขององค์กรโดยให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามกฎหมายและทำหน้าที่

ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

ธนาคารพาณิชย์ (Commercial Bank) คือ บริษัทมหาชนจำกัดที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์และหมายความรวมถึงธนาคารพาณิชย์เพื่อรายย่อย ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ และสาขาของธนาคารพาณิชย์ต่างประเทศที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ (ธนาคารแห่งประเทศไทย, 2563)

หน่วยงานกำกับดูแล คือ หน่วยงานที่กำกับดูแลกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

หน่วยงานกำกับดูแลภาคธุรกิจ คือ หน่วยงานกำกับดูแลภาคธุรกิจธนาคาร ซึ่งหมายถึงธนาคารแห่งประเทศไทย (ธปท.)

นโยบายความเป็นส่วนตัว(Privacy Policy) เป็นเอกสารภายในองค์กร ที่อธิบายภาระหน้าที่และแนวทางปฏิบัติขององค์กรเพื่อให้เป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Titima Thumbumrung, 2020)

ประกาศความเป็นส่วนตัว (Privacy Notice) เป็นเอกสารที่สาธารณชนสามารถเข้าถึงได้ และเขียนขึ้นเพื่อแจ้งเจ้าของข้อมูลส่วนบุคคลเรื่องการประมวลผลข้อมูล (Titima Thumbumrung, 2020)

บทที่ 2

การทบทวนวรรณกรรม

ในสังคมยุคดิจิทัลทำให้ผู้คนมีการแลกเปลี่ยนข้อมูลกันอย่างแพร่หลายและมีการทำธุรกรรมต่าง ๆ ผ่านระบบออนไลน์มากขึ้น ทำให้เกิดการเข้าถึงข้อมูลส่วนบุคคลเป็นจำนวนมาก และเกิดคลังข้อมูล (Big Data) ที่มีประโยชน์ต่อภาคธุรกิจอย่างมาก ในขณะเดียวกันก็ทำให้เกิดการล่วงละเมิดข้อมูลส่วนตัวของบุคคลในการแสวงหาผลประโยชน์ในทางที่ไม่ดี เกิดอาชญากรรมในรูปแบบต่าง ๆ มากมาย ในหลาย ๆ ประเทศจึงได้มีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล รวมถึงประเทศไทยที่ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งส่งผลให้การได้มาและการบริหารจัดการข้อมูลของลูกค้าไม่ได้เป็นเรื่องง่ายอีกต่อไปจึงส่งผลกระทบในทุกภาคธุรกิจ โดยเฉพาะอย่างยิ่งในธุรกิจภาคธนาคารที่มีการปรับตัวเข้าสู่ธุรกิจในยุคดิจิทัลและเป็นหนึ่งในธุรกิจที่มีข้อมูลของลูกค้าอยู่ในมือจำนวนมากยังต้องใช้ข้อมูลดิจิทัลมากเท่าใดก็มักจะตามมาด้วยความเสี่ยงจากการบริหารจัดการเกี่ยวกับข้อมูลที่บริษัทใช้

ดังนั้นการศึกษาถึงผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย จึงได้ศึกษาภายใต้แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อนำมากำหนดกรอบแนวคิดการวิจัย มีรายละเอียด ดังนี้

- 2.1 ธนาคารพาณิชย์ในประเทศไทย (Commercial Bank)
- 2.2 แนวทางการปฏิบัติเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลภาคธนาคาร
- 2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019): PDPA)
- 2.4 การบริหารการเปลี่ยนแปลง (Change Management)
- 2.5 การเปลี่ยนแปลงองค์การ (Organizational Change)
- 2.6 แนวคิดการบริหารคุณภาพในองค์กรอย่างต่อเนื่อง
- 2.7 งานวิจัยที่เกี่ยวข้อง
- 2.8 กรอบแนวคิดการวิจัย

2.1 ธนาคารพาณิชย์ในประเทศไทย (Commercial Bank)

ธนาคารพาณิชย์ คือ บริษัทมหาชนจำกัดที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์และหมายความรวมถึงธนาคารพาณิชย์เพื่อรายย่อย ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ และสาขาของธนาคารพาณิชย์ต่างประเทศที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ (ธนาคารแห่งประเทศไทย, 2563)

ธนาคารแห่งประเทศไทย (2563) ได้ระบุไว้ว่าการประกอบธุรกิจพื้นฐานของธนาคารพาณิชย์ ได้แก่ การรับฝากเงิน การให้สินเชื่อ การซื้อขายเงินตราต่างประเทศ การซื้อขายตราสารทางการเงิน การซื้อขายตัวแลกเปลี่ยนซึ่งรวมถึงการขายลดหรือขายช่วงลดตัวเงิน นอกจากนี้ยังให้บริการเพิ่มเติมในด้านการค้าประกันเงินกู้ยืม การชำระเงินและโอนเงิน และการเสนอผลิตภัณฑ์ทางการเงินเพื่อการบริหารความเสี่ยงให้แก่ลูกค้า เช่น ตราสารอนุพันธ์ด้านอัตราดอกเบี้ย และอัตราแลกเปลี่ยน เป็นต้น ตลอดจนธุรกิจที่ช่วยสนับสนุนพัฒนาตลาดทุนที่เกี่ยวข้องกับหลักทรัพย์ การให้บริการที่เกี่ยวข้องกับการประกันวินาศภัยและประกันชีวิต การให้บริการธนาคารอิเล็กทรอนิกส์ เป็นต้น อย่างไรก็ตามธนาคารพาณิชย์ยังไม่ได้ได้รับอนุญาตให้บริการโดยทำหน้าที่เป็นนายหน้าซื้อขายหุ้น คำหุ้น การจัดจำหน่ายหุ้น และออกกรมธรรม์ประกันวินาศภัยและประกันชีวิต

ปัจจุบันในประเทศไทยมีธนาคารพาณิชย์ภายใต้การกำกับดูแลโดย ธปท. ที่ให้บริการอยู่ทั้งหมด 30 แห่ง ประกอบด้วย ธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทย 14 แห่ง (ตารางที่ 2.1), ธนาคารพาณิชย์เพื่อรายย่อย 1 แห่ง (ตารางที่ 2.2), ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ 4 แห่ง (ตารางที่ 2.3) และสาขาของธนาคารต่างประเทศ 11 แห่ง (ตารางที่ 2.4)

ตารางที่ 2.1

ธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทย

ลำดับ	ชื่อสถาบัน	ลำดับ	ชื่อสถาบัน
1	ธนาคารกรุงเทพ จำกัด (มหาชน)	8	ธนาคารทีสโกลี จำกัด (มหาชน)
2	ธนาคารกรุงไทย จำกัด (มหาชน)	9	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
3	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	10	ธนาคารธนชาต จำกัด (มหาชน)
4	ธนาคารกสิกรไทย จำกัด (มหาชน)	11	ธนาคารยูโอบี จำกัด (มหาชน)
5	ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)	12	ธนาคารแลนด์ แอนด์ เฮาส์ จำกัด (มหาชน)
6	ธนาคารซีไอเอ็มบี ไทย จำกัด (มหาชน)	13	ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด
7	ธนาคารทหารไทย จำกัด (มหาชน)	14	ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน)

ตารางที่ 2.2

ธนาคารพาณิชย์เพื่อรายย่อย

ลำดับ	ชื่อสถาบัน
1	ธนาคารไทยเครดิต เพื่อรายย่อย จำกัด (มหาชน)

ตารางที่ 2.3

ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ

ลำดับ	ชื่อสถาบัน	ลำดับ	ชื่อสถาบัน
1	ธนาคารซูมิโตโม มิตซูบิชิ ทรัสต์ (ไทย) จำกัด (มหาชน)	3	ธนาคารแห่งประเทศไทย (ไทย) จำกัด (มหาชน)
2	ธนาคารเมกะ สากลพาณิชย์ จำกัด (มหาชน)	4	ธนาคารเอเอ็นแซด (ไทย) จำกัด (มหาชน)

ตารางที่ 2.4

สาขาของธนาคารต่างประเทศ

ลำดับ	ชื่อสถาบัน	ลำดับ	ชื่อสถาบัน
1	ธนาคารเจพีเอ็มอร์แกน เชส	7	ธนาคารแห่งอเมริกาเนชั่นแนลแอสโซซิเอชัน
2	ธนาคารซิตี้แบงก์ เอ็น.เอ.	8	ธนาคารอาร์ เอช บี จำกัด
3	ธนาคารซูมิโตโม มิตซูบิชิ แบงกิง คอร์ปอเรชั่น	9	ธนาคารอินเดียนโอเวอร์ซีส์
4	ธนาคารดอยช์แบงก์	10	ธนาคารโอเวอร์ซี-ไชนีสแบงกิงคอร์ปอเรชั่น จำกัด
5	ธนาคารบีเอ็นพี พารีบาส์	11	ธนาคารฮ่องกงและเซี่ยงไฮ้แบงกิงคอร์ปอเรชั่น จำกัด
6	ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ		

2.2 แนวทางการปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจธนาคาร

2.2.1 แนวทางการปฏิบัติสำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคลแก่ผู้บริโภคทางการเงินของธนาคารโลก

การให้บริการทางการเงินธนาคารเป็นปัจจัยในการพัฒนาเศรษฐกิจของประเทศโดยรวม ธนาคารจะต้องมีความสัมพันธ์อันดีระหว่างธนาคารและผู้บริโภค ซึ่งต้องมีความเชื่อถือซึ่งกัน

และกัน (Mutual Trust and Confidence) ดังนั้นธนาคารโลกจึงได้ทำการศึกษามาตรการให้ความคุ้มครองแก่ผู้บริโภคภาคธุรกิจธนาคารในหลายประเทศที่ได้รับการยอมรับว่ามีมาตรฐานในระดับสากลโดยพิจารณาจากเรื่องต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค ซึ่งรวมถึงมาตรการรักษาข้อมูลส่วนบุคคล (Privacy and Data Protection) โดยมาตรการดังกล่าวได้ระบุถึงเรื่องการเก็บรักษาข้อมูลส่วนบุคคลของผู้บริโภค ธนาคารจะต้องเก็บข้อมูลส่วนบุคคลของผู้บริโภคไว้เป็นความลับ ป้องกันไม่ให้เกิดการนำข้อมูลไปใช้อย่างไม่ยุติธรรม หากกรณีที่ธนาคารจะต้องมีการเปิดเผยข้อมูล จะต้องแจ้งเป็นหนังสือไปยังผู้บริโภคนอกจากนี้กฎหมายควรกำหนดเกณฑ์เกี่ยวกับการเปิดเผยข้อมูลวัตถุประสงค์ของการนำข้อมูลไปใช้ให้ชัดเจนรวมถึงการกำหนดบทลงโทษ ในกระบวนการจัดเก็บข้อมูลจะต้องมีระบบรักษาความปลอดภัย อีกทั้งควรเผยแพร่ความรู้แก่ผู้บริโภคเกี่ยวกับการจัดเก็บข้อมูล สิทธิหน้าที่ต่าง ๆ ของผู้บริโภค และผลทางกฎหมายในการจัดเก็บประวัติทางการเงินต่าง ๆ ส่วนการรายงานข้อมูลทางเครดิตต้องมีหน่วยงานกำกับดูแลตามหน้าที่กฎหมายกำหนด ระบบรายงานข้อมูลต้องมีประสิทธิภาพและป้องกันไม่ให้บุคคลภายนอกเข้าถึงข้อมูลดังกล่าวได้อย่างเคร่งครัด (เขมฤทัย สุมาวงศ์ และคณะ, 2556)

2.2.2 แนวทางการปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจธนาคารในประเทศไทย

ในอดีตก่อนมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประเทศไทยมีการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายทั่วไป คือ กฎหมายรัฐธรรมนูญ ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา ซึ่งไม่ได้บัญญัติขึ้นเพื่อควบคุมการเก็บรวบรวม ใช้ และเปิดเผย ไม่ได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลเพียงพอที่จะควบคุมข้อมูลส่วนบุคคลของตนเองได้ นอกจากนี้ยังมีกฎหมายอื่น ๆ ของประเทศไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลมากกว่ากฎหมายทั้ง 3 ฉบับดังกล่าว (อิพร สิทธิธีรรัตน์, 2558) โดยมีกฎหมายและแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร ดังนี้

2.2.2.1 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

ในส่วนของแนวทางการเปิดเผยข้อมูลกำหนดให้บริษัทข้อมูลเครดิตจะเปิดเผยหรือให้ข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์สินเชื่อและการออกบัตรเครดิตจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน โดยต้องเป็นไปตามความสมัครใจของเจ้าของข้อมูลและบริษัทข้อมูลเครดิตต้องแจ้งให้ทราบถึงวิธีการเงื่อนไขในการให้ความยินยอมแต่ละวิธีที่ลูกค้าเลือกใช้อย่างชัดเจนและในการเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการบริษัทข้อมูลบัตรเครดิตจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนทุกครั้ง (ประกาศคณะกรรมการคุ้มครองข้อมูลเครดิต เรื่อง หลักเกณฑ์วิธีการและเงื่อนไขเกี่ยวกับการได้รับความยินยอมจากเจ้าของข้อมูลเพื่อการเปิดเผยข้อมูล) นอกจากนี้เจ้าของข้อมูลยังมีสิทธิที่จะรับรู้

บริษัทข้อมูลเครดิตเก็บรักษาข้อมูลได้ และสามารถตรวจสอบหรือแก้ไขข้อมูลของตนได้ (เชมฤทัย สุมาวงศ์ และคณะ, 2556)

2.2.2.2 แนวปฏิบัติในการติดตามทวงถามหนี้

ธนาคารแห่งประเทศไทยได้ออกแนวปฏิบัติในการติดตามทวงถามหนี้ซึ่งมีการกำหนดให้ผู้เรียกเก็บหนี้ต้องรักษาข้อมูลที่เป็นความลับของลูกค้าและไม่เปิดเผยข้อมูลดังกล่าวระหว่างการติดต่อกับบุคคลอื่น อันแสดงให้ทราบว่าลูกหนี้มีหนี้สิน และห้ามเปิดเผยข้อมูลเกี่ยวกับหนี้สินเมื่อได้รับเงินจากลูกหนี้แล้ว (เชมฤทัย สุมาวงศ์ และคณะ, 2556)

2.2.2.3 ประกาศธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

เป็นการออกประกาศโดยอาศัยอำนาจตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 โดยมีการกำหนดมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้า (Data Privacy) โดยข้อมูลของลูกค้าต้องได้รับการดูแลอย่างปลอดภัย คำนึงถึงความเป็นส่วนตัว การรักษาความลับ การเปิดเผยข้อมูลลูกค้าแก่บุคคลอื่น ต้องมีกระบวนการที่ทำให้มั่นใจได้ว่าผู้รับข้อมูลสามารถรักษาความปลอดภัยของข้อมูลลูกค้าได้อย่างรัดกุม เก็บข้อมูลลูกค้าเท่าที่จำเป็น และใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งลูกค้าไว้ โดยไม่รบกวนความเป็นส่วนตัวของลูกค้า (ธนาคารแห่งประเทศไทย, 2561) และในปัจจุบัน ธนาคารแห่งประเทศไทย (2563) ได้มีการปรับปรุงหลักเกณฑ์เพื่อให้สอดคล้องกับสภาพแวดล้อมการดำเนินธุรกิจที่เปลี่ยนแปลงไปโดยมีหลักการสำคัญ 3 ประการ

(1) การดูแลรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า

มีนโยบาย วิธีปฏิบัติ และระบบงานการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้าตามมาตรฐานสากลที่ยอมรับโดยทั่วไป ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability)

(2) การเปิดเผยข้อมูลลูกค้าให้แก่บุคคลอื่น

มีกระบวนการที่ทำให้มั่นใจได้ว่าผู้รับข้อมูลสามารถรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้าได้อย่างรัดกุม เก็บข้อมูลลูกค้าเท่าที่จำเป็น และใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งลูกค้าไว้ โดยไม่รบกวนความเป็นส่วนตัวของลูกค้า หากเป็นการเปิดเผยข้อมูลให้บุคคลอื่นเพื่อวัตถุประสงค์ทางการตลาดลูกค้ามีสิทธิเลือกในการให้ความยินยอมในการเปิดเผยข้อมูลหรือไม่ก็ได้ โดยไม่กระทบต่อการพิจารณาใช้ผลิตภัณฑ์และในกรณีที่ลูกค้าต้องการยกเลิกหรือถอนความยินยอมที่เคยให้ไว้ผู้ให้บริการต้องมีช่องทางให้ลูกค้าสามารถติดต่อเพื่อขอยกเลิกหรือถอนความยินยอมได้อย่างสะดวก และต้องดำเนินการยกเลิกหรือถอนความยินยอมให้ลูกค้าโดยเร็ว

(3) การเปิดเผยข้อมูลลูกค้าให้บุคคลอื่นเพื่อวัตถุประสงค์อื่นที่ไม่ใช่การตลาด

เพื่อการปฏิบัติตามสัญญาระหว่างผู้ให้บริการกับลูกค้าให้ผู้ให้บริการกำหนดให้การเปิดเผยข้อมูลดังกล่าวเป็นส่วนหนึ่งของการขอใช้บริการได้ โดยให้ระบุวัตถุประสงค์ในการเปิดเผยข้อมูลและระบุประเภทของผู้รับข้อมูลให้ลูกค้าทราบ

อย่างไรก็ดี ยังไม่มีกฎหมายในไทยเพื่อการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะที่บัญญัติขึ้นเพื่อควบคุมการเก็บรวบรวม ใช้ และเปิดเผย ที่ปรับใช้เป็นมาตรฐานสำหรับทุกภาคธุรกิจ จนกระทั่งปี 2562 ประเทศไทยได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นกฎหมายหลักในการควบคุมการใช้ข้อมูลส่วนบุคคล ครอบคลุมกฎหมายอื่น ๆ ที่กล่าวไปข้างต้น ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะช่วยเสริมให้กฎหมายตัวอื่นสามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น

โดยพ.ร.บ. ดังกล่าวมีผลบังคับใช้หลังจากวันที่ประกาศ (วันที่ 28 พฤษภาคม 2562) ยกเว้น หมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7 และความในมาตรา 95 และมาตรา 96 ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเพื่อให้หน่วยงานที่เกี่ยวข้องได้เตรียมความพร้อม เนื้อหาสำคัญของกฎหมายว่าด้วยการเก็บรวบรวม ใช้ และเปิดเผย สิทธิการเข้าถึง การร้องเรียน การรับผิดทางแพ่ง และบทกำหนดโทษ หลังจากนั้นรัฐบาลได้มีการประกาศขยายเวลาการบังคับใช้ ออกไปอีก 1 ปี เนื่องจากหากมีการบังคับใช้ตามเดิมในขณะที่ทุกภาคส่วนไม่พร้อม อาจทำให้เกิดการไม่ปฏิบัติตามกฎหมายโดยไม่ตั้งใจ และอาจเป็นช่องทางให้ผู้ทุจริตแสวงหาผลประโยชน์ รวมถึงผลกระทบจากการแพร่ระบาดของโรคโควิด-19 ทำให้ภาคเอกชนเกิดปัญหาสภาพคล่องในการลงทุนเพื่อปรับปรุงกระบวนการงาน ระบบสารสนเทศ และการจัดหาหรือจัดอบรมบุคลากรที่มีความรู้ความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลให้มีความพร้อมปฏิบัติตามกฎหมาย (ประชาชาติธุรกิจ, 2563)

2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019): PDPA)

จากการเข้าสู่ยุค Digital Transformations ที่เทคโนโลยีเข้ามามีบทบาทให้การดำรงชีวิต และการบริหารงานขององค์กรมากขึ้น จึงทำให้ข้อมูลต่าง ๆ ของผู้บริโภคถูกบันทึกและจัดเก็บอยู่ในระบบข้อมูล โดยที่ผู้บริโภคส่วนใหญ่ไม่สามารถทราบได้เลยว่าข้อมูลเหล่านั้นถูกนำไปใช้อย่างไรบ้างประเทศไทยจึงได้ให้ความสำคัญกับเรื่องการคุ้มครองความเป็นส่วนตัวของข้อมูล (Data Privacy) โดยเมื่อปี 2562 ได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้รับอิทธิพลสำคัญมาจาก General Data Protection Regulation (GDPR) ที่ว่าด้วยการเก็บรวบรวม ใช้และเปิดเผย

ข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล การรับผิดทางแพ่ง และบทกำหนดโทษที่จะมีการบังคับใช้เต็มฉบับในวันที่ 1 มิถุนายน 2564

2.3.1 หลักการและเหตุผล

เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคล (Personal Data) ไม่ใช่ตัวบุคคล (Person) หากแต่การคุ้มครองข้อมูลส่วนบุคคลนั้นจะมีผลเป็นการปกป้องบุคคลจากผลร้ายที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นแนวทางตามแบบสหภาพยุโรปหมายความว่าจะสามารถประมวลผลข้อมูลส่วนบุคคลใด ๆ ได้ (ไม่ว่าจะเป็น การเก็บรวบรวม การใช้ การเผยแพร่ การเก็บรักษา) จะต้องมีฐานทางกฎหมายที่ถูกต้อง (Lawful Basis) ดังนั้นหลักการพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ ห้ามประมวลผลข้อมูลส่วนบุคคล เว้นแต่จะมีฐานหรือเหตุแห่งการประมวลผลให้ทำได้ตามกฎหมาย (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

โดยกฎหมายดังกล่าวบังคับใช้แก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร และอยู่นอกอาณาจักรหากมีกิจกรรมเสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักรหรือเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร หากแต่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น การดำเนินงานของหน่วยงานรัฐที่มีหน้าที่รักษาความมั่นคงของรัฐ กิจกรรมสื่อมวลชน งานศิลปกรรม งานวรรณกรรม หรือเพื่อประโยชน์สาธารณะ การดำเนินการตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภาและคณะกรรมการที่แต่งตั้ง การพิพากษาคดีของศาลและการดำเนินงานในกระบวนการ และการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิตได้รับข้อยกเว้นในการบังคับใช้กฎหมาย (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

2.3.2 แนวปฏิบัติพื้นฐานที่จำเป็นต่อการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคล

2.3.2.1 แนวปฏิบัติการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Guideline for Personal Data Classification)

ปิยะบุตร บุญอร่ามเรือง และคณะ (2562) กล่าวว่า ผู้ประกอบการต้องสามารถระบุข้อมูลและจัดการข้อมูลต่าง ๆ บนพื้นฐานของความเสี่ยงได้อย่างเหมาะสม ดังนั้นการแยกแยะข้อมูลส่วนบุคคลจึงเป็นขั้นตอนพื้นฐานที่สุดเพื่อการจัดการข้อมูลส่วนบุคคลในประเด็นอื่น ๆ ต่อไป ซึ่งจะแบ่งเป็น 2 ส่วน ได้แก่ 1) ขอบเขตของข้อมูลส่วนบุคคล 2) การกำหนดและแยกแยะข้อมูลส่วนบุคคล โดยมีรายละเอียด ดังนี้

(1) ขอบเขตของข้อมูลส่วนบุคคล

ทำให้ผู้ประกอบการทราบว่าข้อมูลใดเป็นข้อมูลที่อยู่ในขอบเขตความหมายของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลใด ๆ ที่สามารถระบุไปถึงเจ้าของข้อมูล (Data Subject) ได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม ตัวอย่างเช่น ชื่อ-นามสกุล ที่อยู่ เลขประจำตัวประชาชน เบอร์โทรศัพท์ อีเมล ข้อมูลทางการเงิน เชื้อชาติ ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม และข้อมูลสุขภาพ เป็นต้น (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

ข้อมูลอ่อนไหว (Sensitive Personal Data) เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวของบุคคล แต่มีความละเอียดอ่อนและเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรมต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ และ ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

(2) การกำหนดและแยกแยะข้อมูลส่วนบุคคล

ทำให้องค์กรสามารถระบุข้อมูลส่วนบุคคลตามกระบวนการทำงานต่าง ๆ ขององค์กรและจัดการตามความเสี่ยงได้อย่างเหมาะสม โดย ปิยะบุตร บุญอร่ามเรือง และคณะ (2562) ระบุว่าผู้ประกอบการต้องมีมาตรฐานการจัดการเกี่ยวกับข้อมูลส่วนบุคคลเพื่อที่จะสามารถแสดงให้เห็นได้ว่าได้ใช้ความระมัดระวังที่เพียงพอแล้ว โดยการกำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความรุนแรงของผลกระทบต่อสิทธิและเสรีภาพขอ โดยแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

1. Data Policy การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล
2. Data Discovery การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล
3. Data Proliferation การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย
4. Data Risk Level การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ โดยการกำหนดความเสี่ยงและความร้ายแรงของผลกระทบ (Impact Levels) เป็นไปตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ

5. Data Protection มีมาตรการคุ้มครองข้อมูลส่วนบุคคล โดยผู้ประกอบการต้องมีกระบวนการขั้นตอนรองรับการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสมตามความเสี่ยงและความร้ายแรงของผลกระทบ ได้แก่ เงื่อนไขการเข้าถึงข้อมูลส่วนบุคคล กระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ (Physical Security) กระบวนการรองรับการจัดการข้อมูลส่วนบุคคลตลอดการพัฒนาระบบเทคโนโลยีสารสนเทศ แผนเผชิญเหตุเมื่อมีการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล มาตรการเมื่อมีการไม่ปฏิบัติตามขั้นตอนการคุ้มครองข้อมูลส่วนบุคคล และกระบวนการฝึกอบรมพนักงาน

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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (2562) กล่าวว่า การประมวลผลข้อมูลไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเผยแพร่ และการเก็บรักษานั้นจะชอบด้วยกฎหมายเมื่อทำตามหลักการหนึ่งหลักการใด ดังนี้

(1) การได้รับความยินยอม (Consent) จากเจ้าของข้อมูลซึ่งต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล ต้องเป็นการจัดทำโดยชัดแจ้งเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล Consent ต้องแยกจากข้อความอื่นชัดเจน อ่านงาน ไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดได้ ทั้งนี้เจ้าของข้อมูลต้องมีความเป็นอิสระในการให้ความยินยอมและสามารถถอนความยินยอมเมื่อใดก็ได้เว้นแต่มีข้อจำกัดสิทธิ

(2) การจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุเพื่อประโยชน์สาธารณะ และการศึกษาวิจัยหรือสถิติ (Scientific or Historical Research)

(3) ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)

(4) การปฏิบัติตามสัญญา (Contract) การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูล เช่น การประมวลผลข้อมูลธุรกรรมเพื่อคำนวณดอกเบี้ยธนาคาร หรือการตรวจสอบข้อมูลส่วนบุคคลก่อนการเปิดบัญชีหรือยื่นกู้เงินจากธนาคาร หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม

(5) ภารกิจของรัฐ (Public Task) จำเป็นเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

(6) ประโยชน์อันชอบธรรม (Legitimate Interest) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่น

(7) การปฏิบัติตามกฎหมาย (Legal Obligation)

ความยินยอมที่เก็บรวบรวมไว้ก่อน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อนุญาตให้มีผลบังคับใช้ได้ตามขอบเขตวัตถุประสงค์เดิม แต่ผู้ควบคุมข้อมูลจะต้องประชาสัมพันธ์ให้สามารถถอนความยินยอมได้โดยง่ายด้วย ส่วนการเปิดเผยข้อมูลให้เป็นไปตามพ.ร.บ.

อย่างไรก็ตาม ปิยะบุตร บุญอร่ามเรือง และคณะ (2562) ได้ระบุว่า การเก็บรวบรวมข้อมูลส่วนบุคคลนั้นองค์กรจะต้องเก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์ตามกฎหมาย โดยเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง หากเก็บข้อมูลจากแหล่งอื่นต้องแจ้งให้เจ้าของข้อมูลทราบภายใน 30 วันนับจากวันที่เก็บข้อมูล ในการเก็บข้อมูลนั้นจะต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดต่าง ๆ ตามที่กฎหมายกำหนด อาทิ เช่น วัตถุประสงค์ของการเก็บรวบรวม ข้อมูลส่วนบุคคลที่ต้องการเก็บ และระยะเวลาในการเก็บรวบรวม หน่วยงานที่เก็บข้อมูล ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูล

Titima Thumbumrung (2563) ระบุว่า สิทธิของเจ้าของข้อมูลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบด้วย 7 สิทธิ ดังนี้

(1) สิทธิได้รับการแจ้งให้ทราบ (Right to be Informed) ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่ามีการรวบรวมข้อมูลอะไร อย่างไร มีการใช้ข้อมูลดังกล่าวนานแค่ไหน จะถูกเก็บไว้อย่างไร และจะแบ่งปันกับบุคคลที่สามหรือไม่อย่างไร

(2) สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of Access) เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอสำเนาข้อมูลส่วนบุคคลของตนจากผู้ควบคุมข้อมูล

(3) สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to Data Portability) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการได้รับข้อมูลส่วนบุคคลของตนเองที่เคยให้แก่ผู้ควบคุมข้อมูลในรูปแบบที่สามารถอ่านและเข้าใจได้อย่างแพร่หลาย และมีสิทธิ์ที่จะโอนข้อมูลของตนไปยังผู้ควบคุมข้อมูลรายอื่น ซึ่งเจ้าของข้อมูลมีสิทธิขอให้โอนโดยตรงได้หากสามารถกระทำได้ในทางปฏิบัติ

(4) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to Object) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล เช่น เพื่อการตลาดหรือการขายตรง

(5) สิทธิในการขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ (Right to Erasure) คือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลลบข้อมูลส่วนบุคคลของตน

(6) สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to Restriction of Processing) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องขอให้ผู้ควบคุมข้อมูลจำกัดการประมวลผล

ข้อมูล โดยผู้ควบคุมข้อมูลสามารถเก็บข้อมูลส่วนบุคคลต่อไปได้ แต่ไม่สามารถนำไปประมวลผลข้อมูลได้อีกต่อไป เว้นแต่เจ้าของข้อมูลจะให้ความยินยอมหรือได้รับการยกเว้นตามที่กฎหมายกำหนด

(7) สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (Right to Rectification) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์

ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Special Categories or Sensitive Data) การเก็บรวบรวมข้อมูลที่มีความอ่อนไหวเป็นพิเศษ จะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Explicit Consent) ยกเว้นเป็นการป้องกันหรือระงับอันตรายต่อชีวิตและร่างกาย (Vital Interest) เพื่อดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไร (Social Protection and Non-profit) ข้อมูลเปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลนั้น (Manifestly Made Public) เช่น กรณีที่เจ้าของข้อมูลได้ให้สัมภาษณ์และถูกตีพิมพ์เผยแพร่ในหนังสือพิมพ์ (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

โดยส่วนใหญ่แล้วการดำเนินงานตามปกติธุรกิจขององค์กรจะมีความเกี่ยวข้องกับการปฏิบัติตามสัญญา (Contract) และการได้รับความยินยอม (Consent) มากที่สุดซึ่งมักเกี่ยวข้องกับกิจกรรมทางการตลาด เช่น กิจกรรมการตลาดแบบตรง (Direct Marketing) ระบบสมาชิกสะสมแต้ม (Loyalty Program) การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุ้นยอดขาย (Social Network) การโฆษณาตามพฤติกรรมออนไลน์ (Online Behavioral Advertisement) เป็นต้น หรือการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย (Legal Claim) รวมถึงเรื่องจำเป็นในการปฏิบัติตามกฎหมาย (Legal Obligation) เฉพาะที่กฎหมายกำหนด (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

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

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

ปิยะบุตร บุญอร่ามเรือง และคณะ (2562) ได้ให้แนวปฏิบัติไว้ว่าผู้ควบคุมข้อมูลจะประมวลผลข้อมูลส่วนบุคคลได้ตามขอบเขตที่ได้รับตามยินยอมในการประมวลผล ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมายโดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่และความรับผิดชอบ ดังนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม
 (2) ป้องกันการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ กรณีที่ให้ข้อมูลแก่บุคคลอื่นที่ไม่ใช่ผู้ควบคุม

(3) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officers (DPO) เพื่อทำหน้าที่ให้คำแนะนำการปฏิบัติตามพ.ร.บ. ตรวจสอบการดำเนินงาน ประสานงานภายในองค์กรเมื่อเกิดปัญหาและรักษาความลับของข้อมูล ควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

(4) แจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) ภายใน 72 ชั่วโมง

(5) จัดทำบันทึกรายการเพื่อใช้ในการตรวจสอบ เช่น ข้อมูลส่วนบุคคลที่เก็บ วัตถุประสงค์ในการเก็บ ระยะเวลาในการเก็บรักษา ข้อมูลผู้ควบคุมข้อมูล เงื่อนไข สิทธิ และวิธีการเข้าถึงข้อมูล การปฏิเสธคำขอ และข้อมูลมาตรฐานการรักษาความปลอดภัย เป็นต้น

(6) มีระบบตรวจสอบเพื่อลบและทำลายข้อมูลเมื่อพ้นระยะเวลาการจัดเก็บ ข้อมูลเกินความจำเป็น หรือเมื่อเจ้าของข้อมูลขอร้อง

(7) แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีผู้ควบคุมต่างชาติต้องแต่งตั้งตัวแทนในไทย และให้อำนาจกระทำแทนโดยไม่จำกัดความรับผิดชอบ

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

ผู้ประมวลผลข้อมูลจะต้องประมวลผลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูลหรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง โดยพิจารณาถึงความเป็นไปได้ รวมถึงความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล เพื่อกำหนดมาตรการที่เหมาะสม (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

2.3.2.4 แนวปฏิบัติเพื่อการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline on Data Protection Impact Assessment)

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล หรือ DPIA เป็นกระบวนการที่ใช้ความระมัดระวังในการประมวลผลข้อมูลส่วนบุคคลกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ซึ่งจะมีประโยชน์อย่างมากโดยเฉพาะการปฏิบัติตามกฎหมาย

เพราะเป็นวิธีการที่จะทำให้สามารถประเมินความเสี่ยงและแสดงให้เห็นว่าได้มีการปฏิบัติหลักเกณฑ์ต่าง ๆ ตามกฎหมาย (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ถือเป็นประโยชน์แก่ผู้ประกอบการเป็นอย่างยิ่ง ไม่ว่าจะเป็นในแง่ของการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และในแง่ของการช่วยให้ผู้ประกอบการสามารถประเมินถึงข้อบกพร่องต่าง ๆ อันเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ทั้งนี้เพื่อสามารถปรับปรุงโครงสร้างการดำเนินงานอย่างเป็นระบบและมีความปลอดภัยในแง่ของการประมวลผลข้อมูลส่วนบุคคล (ศุภวัชร มาลานนท์, 2563)

2.3.2.5 แนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Guideline on Cross-border Data Transfer)

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่ได้รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามเกณฑ์ที่กฎหมายกำหนด เว้นแต่เป็นการปฏิบัติตามกฎหมาย ได้รับความยินยอมจากเจ้าของข้อมูล มีความจำเป็นเพื่อการปฏิบัติตามสัญญา การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ หรือจำเป็นเพื่อประโยชน์สาธารณะที่สำคัญ อนุญาตให้สามารถกระทำได้ (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2562)

2.3.3 บทลงโทษ

ปิยะบุตร บุญอร่ามเรือง และคณะ (2562) ได้อธิบายถึงบทลงโทษจากการฝ่าฝืนหรือขัดต่อกฎหมายดังกล่าว ซึ่งแบ่งออกเป็น 3 ส่วน ได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

2.3.3.1 ความรับผิดทางแพ่ง

การฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ทำให้เจ้าของข้อมูลเสียหาย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งการปฏิบัติตามหน้าที่และตามอำนาจกฎหมาย นอกจากค่าสินไหมทดแทนแล้ว ศาลอาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงแต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง

2.3.3.2 ความรับผิดทางอาญา

(1) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เป็นเหตุให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ แต่หากเป็นการกระทำเพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมาย (โดยทุจริต) สำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

(2) ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับเว้นแต่ข้อยกเว้นตามกฎหมาย

(3) กรณีนิติบุคคลเป็นผู้กระทำความผิด ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

2.3.3.3 โทษทางปกครอง

กระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายกำหนด เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ หรือขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล มีโทษปรับทางปกครองสูงสุดไม่เกิน 5,000,000 บาท

ทั้งนี้จะเห็นได้ว่ากฎหมายได้ให้ความสำคัญคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ในหลาย ๆ เรื่อง และกฎหมายดังกล่าวก็ได้กำหนดบทลงโทษอย่างชัดเจน ล้วนแล้วแต่ส่งผลกระทบต่อการบริหารจัดการองค์กรไม่มากนักน้อย และกฎหมายฉบับนี้เกี่ยวข้องกับทุกองค์กร ทุกภาคธุรกิจ แม้จะเป็นช่วงเวลาที่เราประชาชนส่วนใหญ่กำลังวิตกกังวลกับวิกฤตโควิด ก็คงมองข้ามหรือไม่ให้ความสำคัญกับกฎหมายฉบับนี้ไม่ได้ (ณัฐพล ม่วงท่า, 2563)

2.4 การบริหารการเปลี่ยนแปลง (Change Management)

2.4.1 ความหมายของการบริหารการเปลี่ยนแปลง

ปัจจุบันในธุรกิจต่าง ๆ ได้นำแนวคิดการบริหารการเปลี่ยนแปลงเข้ามาปรับใช้เพื่อให้ธุรกิจสามารถอยู่รอดได้ในยุคสมัยที่มีการเปลี่ยนแปลงอย่างหลากหลายและเพิ่มความสามารถทางการแข่งขันโดยมีผู้ให้คำนิยามเกี่ยวกับความหมายของการบริหารการเปลี่ยนแปลงองค์กร ดังนี้

เนตร์พัฒนา ยาวีราข (2560) กล่าวว่า การบริหารการเปลี่ยนแปลง หมายถึง กระบวนการที่ทำให้องค์กรมีประสิทธิภาพมากขึ้นในการทำงานเพื่อให้บรรลุวัตถุประสงค์

ทิพวรรณ หล่อสุวรรณรัตน์ (2547) กล่าวว่า การบริหารการเปลี่ยนแปลงองค์กร คือ การออกแบบโครงสร้างองค์กรใหม่ การติดตั้งระบบสารสนเทศใหม่ และการเปลี่ยนแปลงวัฒนธรรม โดยการเปลี่ยนแปลงองค์กรอาจเป็นลักษณะการเปลี่ยนแปลงวัตถุประสงค์ โครงสร้างกลยุทธ การออกแบบงาน เทคโนโลยี กระบวนการทำงาน วัฒนธรรม และสมาชิกองค์กร

การบริหารการเปลี่ยนแปลงโดยสรุป หมายถึง การวางแผนดำเนินการจัดการกับเหตุการณ์ทั้งภายในองค์กรและภายนอกองค์กร เพื่อให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป และลดผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงต่าง ๆ ทำให้เกิดแรงผลักดันให้เกิดการปรับตัว และเปลี่ยนแปลงให้เกิดการพัฒนาองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผล

2.4.2 ปัจจัยที่ส่งผลให้เกิดการเปลี่ยนแปลง

สภาพแวดล้อมที่เปลี่ยนแปลงไปอย่างรวดเร็วทำให้ธุรกิจหรือองค์กรต่าง ๆ จำเป็นต้องปรับตัวหรือเปลี่ยนแปลงเพื่อให้ทันต่อสภาวะแวดล้อมที่เปลี่ยนแปลงไป โดยเฉพาะอย่างยิ่งในยุคที่เทคโนโลยีเข้ามามีบทบาทมากขึ้น หรือเรียกว่ายุคแห่งดิจิทัล ซึ่งทำให้เกิดการเปลี่ยนแปลงอย่างรวดเร็ว โดย Black and Porter (2000) ให้ความสำคัญกับปัจจัยที่มีผลต่อการเปลี่ยนแปลง ซึ่งแบ่งเป็น 2 ประเภท คือ ปัจจัยภายนอกองค์กรและปัจจัยภายในองค์กรสอดคล้องกับ Kreitner and Kinichi (2001) ที่บอกถึงสิ่งที่ทำให้เกิดการเปลี่ยนแปลงมาจากปัจจัยภายนอกองค์กรและปัจจัยภายในองค์กร

ปัจจัยภายนอก (External Factors)

ปัจจัยภายนอก คือ แรงผลักดันที่เกิดขึ้นจากภายนอกองค์กร ซึ่งอยู่นอกเหนือการควบคุมขององค์กร เช่น นโยบายภาครัฐ เศรษฐกิจ การเมือง การแข่งขัน ความต้องการของผู้บริโภค รวมถึงเทคโนโลยีซึ่งเป็นปัจจัยสำคัญที่มีอิทธิพลต่อการเปลี่ยนแปลงอย่างมากในทุกวันนี้ เนื่องจากมีผลทำให้รูปแบบการดำเนินชีวิตของคนเปลี่ยนแปลงไป ดังนั้นสภาพแวดล้อมภายนอกจึงเป็นปัจจัยที่มีผลกระทบต่อองค์กรในการปรับตัวและเปลี่ยนแปลงเพื่อให้ธุรกิจสามารถอยู่รอดและ

สามารถแข่งขันกับองค์กรอื่น ๆ โดย Kreitner and Kinichi (2001) ได้แบ่งเป็น 4 ปัจจัยสำคัญที่ส่งผลกระทบโดยตรงต่อองค์กร ดังนี้

(1) ปัจจัยด้านประชากร (Demographic Characteristic) เช่น อายุ การศึกษา ทักษะ เพศ เป็นต้น ซึ่งส่งผลต่อการปฏิบัติงานหรือพฤติกรรมของบุคลากรแต่ละบุคคลอันมีผลต่อผลงานขององค์กร จึงถือเป็นปัจจัยสำคัญและเป็นประโยชน์ต่อองค์กร

(2) ปัจจัยด้านความก้าวหน้าทางเทคโนโลยี (Technological Advancements) เป็นปัจจัยที่มีผลกระทบต่อองค์กรเป็นอย่างมาก เนื่องจากปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลงก้าวหน้าอยู่ตลอดเวลาและทุกองค์กรต่างนำมาใช้ในการดำเนินธุรกิจทั้งการผลิต การบริการ และการบริหารงาน เมื่อเทคโนโลยีเกิดการเปลี่ยนแปลงไปจึงเป็นปัจจัยสำคัญที่ทำให้องค์กรต้องปรับเปลี่ยนระบบงานต่าง ๆ เพื่อสร้างความได้เปรียบทางการแข่งขัน และมีผลกระทบต่อการบริหารทรัพยากรมนุษย์เช่นกัน

(3) ปัจจัยด้านการตลาด (Market Changes) รวมถึงสภาพเศรษฐกิจ สังคม และคู่แข่ง ซึ่งสิ่งเหล่านี้มีการเปลี่ยนแปลงตลอดเวลา เมื่อสังคมเปลี่ยนแปลงไป พฤติกรรมหรือความต้องการของลูกค้าที่ปรับเปลี่ยนไป ซึ่งมีผลกระทบต่อการดำเนินงานขององค์กร

(4) ปัจจัยด้านแรงกดดันทางสังคม การเมือง กฎระเบียบ นโยบายภาครัฐ หรือข้อกำหนด กฎหมาย เป็นปัจจัยที่อยู่เหนือการควบคุม ซึ่งอาจส่งผลดีหรือผลเสียต่อธุรกิจได้

ปัจจัยภายใน (Internal Factors)

ศรัญญา วิริยะศาสตร์ (2561) กล่าวว่า ปัจจัยภายในเป็นปัจจัยที่เกิดขึ้นจากภายในองค์กรที่สามารถควบคุมได้ และส่งผลให้เกิดการปรับตัวหรือเปลี่ยนแปลงภายในองค์กร เช่น การเปลี่ยนโครงสร้างองค์กร การเปลี่ยนกลยุทธ์องค์กร การเปลี่ยนผู้บริหาร การปรับเปลี่ยนกระบวนการทำงาน การนำเทคโนโลยีใหม่ ๆ มาปรับใช้ในองค์กร การเปลี่ยนแปลงวัฒนธรรมองค์กร เป็นต้น ปัจจัยที่เกิดขึ้นเหล่านี้เกิดจากการปรับตัวขององค์กรเพื่อตอบรับกับปัจจัยและสภาพแวดล้อมภายนอกเพื่อให้การบริการเกิดประสิทธิภาพมากขึ้น ทำให้เกิดการเปลี่ยนแปลงแตกต่างจากสิ่งเดิมที่เคยเป็น เช่น กระบวนการทำงานใหม่ ๆ เครื่องมือการทำงานใหม่ ๆ วิธีคิดวิธีปฏิบัติที่แตกต่างไป รวมถึงวัฒนธรรมองค์กรที่เปลี่ยนไป

ดังนั้นปัจจัยภายในองค์กรและปัจจัยภายนอกองค์กร ถือเป็นองค์ประกอบที่สำคัญในการบริหารจัดการองค์กรซึ่งไม่สามารถหลีกเลี่ยงได้ องค์กรที่สามารถบริหารจัดการกับการเปลี่ยนแปลงได้ดี มีความยืดหยุ่น และสามารถตอบรับกับสภาพแวดล้อมที่เปลี่ยนแปลงไปอย่างรวดเร็วได้จะทำให้องค์กรสามารถดำเนินธุรกิจได้อย่างมีประสิทธิภาพอย่างยั่งยืน

2.5 การเปลี่ยนแปลงองค์การ (Organizational Change)

การเปลี่ยนแปลงองค์การถือเป็นความท้าทายของโลกธุรกิจ ซึ่งรูปแบบของการตอบสนองต่อการเปลี่ยนแปลงนั้นแตกต่างกันไปตามลักษณะและเป้าหมายของแต่ละองค์กรธุรกิจโดยนักวิชาการได้แบ่งการเปลี่ยนแปลงออกเป็นหลายประเภท Robbins and Coulter (2008) ที่กล่าวว่า การเปลี่ยนแปลงองค์การนั้นมีรูปแบบที่สำคัญ 3 ส่วนด้วยกันคือ

1) การเปลี่ยนแปลงทางโครงสร้าง ให้สอดคล้องกับการเปลี่ยนแปลง ที่อาจเกิดขึ้นจากปัจจัยภายนอกหรือปัจจัยภายใน ซึ่งหมายถึงการเปลี่ยนแปลงองค์ประกอบต่าง ๆ ของโครงสร้างองค์การ เช่น ความชำนาญ การเปลี่ยนแปลงรูปแบบการจัดฝ่ายและแผนงาน การจัดสายบังคับบัญชาหรือช่วงการบังคับบัญชาใหม่ การปรับเปลี่ยนระดับ การรวมอำนาจ การจัดระเบียบงาน การออกแบบงานใหม่ หรือการปรับเปลี่ยนโครงสร้างโดยรวมทั้งหมดขององค์การ

2) การเปลี่ยนแปลงเทคโนโลยี เป็นการเปลี่ยนแปลงหรือแก้ไขกระบวนการทำงานหรือวิธีการทำงาน โดยการนำเอาทั้งเครื่องจักร เครื่องมือ ระบบ หรือเทคโนโลยีสมัยใหม่เข้ามาแทนที่เทคโนโลยีเดิม ๆ เพื่อให้เกิดการทำงานได้อย่างมีประสิทธิภาพ เช่น การใช้ระบบงานเทคโนโลยีเข้ามาทำงานแทนคน เป็นต้น

3) การเปลี่ยนแปลงคน ซึ่งผู้บริหารจะต้องพยายามปรับเปลี่ยนพนักงานใน ด้านต่าง ๆ เช่น ทักษะคติ ความคาดหวัง การรับรู้ และพฤติกรรม เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพมากขึ้น

ขณะเดียวกันนักวิชาการบางท่านได้แบ่งการเปลี่ยนแปลงองค์การออกเป็น 4 ประเภท ดังนี้ (Society for Human Resource Management, 2005)

1) การเปลี่ยนแปลงโครงสร้าง (Structural Change) มองว่าองค์การเปรียบเหมือนเครื่องจักร (Machine Model) ซึ่งเกิดขึ้นจากองค์ประกอบหลายอย่างมาทำงานร่วมกัน การเปลี่ยนแปลงจึงเป็นการปรับส่วนประกอบของเครื่องจักรหรือระบบงานเพื่อให้เกิดผลงานโดยรวมที่ดีขึ้น ตัวอย่างการเปลี่ยนแปลงโครงสร้าง เช่น การควบรวมกิจการ การซื้อกิจการอื่น และการลดขนาด เป็นต้น

2) การลดต้นทุน (Cost Cutting) เป็นการลดขั้นตอนหรือวิธีการทำงานที่ไม่จำเป็นเพื่อลดต้นทุนในการทำงาน ซึ่งบางองค์การที่ประสบปัญหามักจะใช้วิธีการนี้เพื่อปรับปรุงผลการดำเนินงานเพื่อให้องค์การสามารถอยู่รอดได้

3) การเปลี่ยนแปลงกระบวนการ (Process Change) เป็นการเปลี่ยนแปลงที่ให้ความสำคัญกับการเปลี่ยนแปลงขั้นตอนการทำงาน เช่น การปรับ ระบบการอนุมัติเงินกู้ การปรับเปลี่ยนแนวทางในการบริหารหรือการตัดสินใจ เป็นต้น ทั้งนี้เพื่อวัตถุประสงค์สำคัญคือการลด

ระยะเวลาของกระบวนการต่าง ๆ การเพิ่มความน่าเชื่อถือ การลดต้นทุน และการเพิ่มประสิทธิภาพการทำงาน

4) การเปลี่ยนแปลงวัฒนธรรม (Cultural Change) เป็นการเปลี่ยนแปลงที่มุ่งเน้นไปที่คนในองค์กร เช่น การเปลี่ยนแปลงแนวทางการดำเนินธุรกิจ การเปลี่ยนแปลงระบบการบริหารงานจากการควบคุมสั่งการไปเป็นการบริหารแบบมีส่วนร่วม หรือการเปลี่ยนมุมมองการบริหารจากภายในสู่ภายนอก (Inward Focus) เป็นภายนอกเข้ามาสู่ภายใน (Outward-Looking Focus) เป็นต้น

ดังนั้นการเปลี่ยนแปลงองค์กร เพื่อการดำเนินงานที่มีประสิทธิภาพและยั่งยืนบนความท้าทายต่าง ๆ ในโลกธุรกิจยุคปัจจุบันนั้น เมื่อเกิดการเปลี่ยนแปลงอย่างใดอย่างหนึ่งย่อมส่งผลกระทบต่อการเปลี่ยนแปลงอื่น ๆ ที่ตามมา อาทิเช่น การเปลี่ยนแปลงในทางเทคโนโลยี เป็นผลทำให้กระบวนการทำงานเปลี่ยนแปลง เป็นต้น

ซึ่งเมื่อนำแนวคิดการเปลี่ยนแปลงองค์กรจากทั้งสองแนวคิดมาปรับรวมกันจึงสามารถแบ่งรูปแบบการเปลี่ยนแปลงองค์กรออกเป็น 5 ประเภท ประกอบด้วย 1) การเปลี่ยนแปลงโครงสร้างองค์กร 2) การเปลี่ยนแปลงเทคโนโลยี 3) การเปลี่ยนแปลงคน 4) การเปลี่ยนแปลงในต้นทุน และ 5) การเปลี่ยนแปลงกระบวนการทำงาน ซึ่งแนวคิดนี้จะถูกนำไปใช้ในการสรุปกรอบแนวคิดการวิจัยตามแผนภาพข้อ 2.8 กรอบแนวคิดการวิจัย

2.6 แนวคิดการบริหารคุณภาพในองค์กรอย่างต่อเนื่อง

การบริหารคุณภาพในองค์กรด้วยวงจรคุณภาพ (PDCA) หรือ Deming Cycle จัดเป็นกิจกรรมปรับปรุงและพัฒนางานให้มีประสิทธิภาพ ศศิมา สุขสว่าง (ม.ป.ป.) กล่าวว่า เมื่อมีการใช้ PDCA ในการปฏิบัติงานอย่างต่อเนื่องแล้วนั้น จะทำให้องค์กรมีการพัฒนาคุณภาพอย่างต่อเนื่อง (Continuous Improvement)

สุราสินี โพธิ์จันทร์ (2558) ได้อธิบายว่า PDCA เป็นหัวใจสำคัญของการปรับปรุงอย่างต่อเนื่อง เนื่องจาก PDCA มีเป้าหมายให้เกิดการพัฒนาอย่างต่อเนื่องปรับตัวให้สอดคล้องกับสถานการณ์ได้ เพื่อให้สามารถบรรลุวัตถุประสงค์ที่วางไว้ ในแวดวงของการทำงานจึงมักจะมีการนำ PDCA เข้ามาประยุกต์ใช้ทั้งการทำงานประจำ และการปรับปรุงงาน ซึ่งโครงสร้างของ PDCA ประกอบด้วย

(1) การวางแผน (Plan) คือ การวางแผนจากวัตถุประสงค์หรือเป้าหมายที่วางไว้ โดยวางแผนทั้งขั้นตอน วิธีการดำเนินการ เวลาที่ใช้ ทรัพยากรต่าง ๆ และผลลัพธ์ที่ต้องการ

(2) การปฏิบัติตามแผน (Do) คือ ลงมือทำตามแผนให้ได้ผลลัพธ์หรือเป้าหมายที่วางแผนไว้

(3) การตรวจสอบ (Check) คือ การตรวจสอบหรือการประเมินผลและนำผลประเมินมาวิเคราะห์ เพื่อติดตามผลการปฏิบัติงานว่าเป็นไปตามแผนหรือไม่ มีปัญหาหรืออุปสรรคอย่างไร

(4) การปรับปรุงแก้ไข (Act) คือ การปรับปรุงการดำเนินการอย่างเหมาะสมหรือการจัดทำมาตรฐานใหม่ ซึ่งถือเป็นพื้นฐานของการยกระดับคุณภาพ

การดำเนินงานไม่ว่าจะเป็นการปรับปรุงผ่านเครื่องมือการเพิ่มผลผลิตภาพ หรือการปรับปรุงคุณภาพหรือแม้แต่การบริหารกิจกรรมภายในองค์กร การวางแผนอย่างเหมาะสมเป็นจุดเริ่มต้นที่ดี และการดำเนินการที่เป็นไปตามแผนจะเป็นเส้นทางที่จะนำไปสู่การบรรลุวัตถุประสงค์ แต่อย่างไรก็ตามก็ต้องมีการตรวจสอบประเมินผลปัญหาต่าง ๆ ที่เกิดขึ้นเพื่อที่จะได้นำมาปรับปรุงแผนแนวทางปฏิบัติให้สอดคล้องกับสถานการณ์ได้ ทั้งหมดนี้ ก็คือการทำงานอย่างครบถ้วนตามแนวคิดของวงจร PDCA ซึ่งถือเป็นหัวใจสำคัญของการปรับปรุงอย่างต่อเนื่อง

2.7 งานวิจัยที่เกี่ยวข้อง

2.7.1 งานวิจัยแนวทางการดำเนินธุรกิจหลังมีการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษางานวิจัยและบทความที่เกี่ยวข้องกับการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลพบว่า การปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลส่งผลกระทบต่อปัจจัยสภาพแวดล้อมทั้งภายในและภายนอกองค์กร รวมถึงแนวทางการดำเนินงานของบริษัทที่ต้องมีแนวทางในการดำเนินธุรกิจเพื่อตอบสนองต่อการปรับใช้กฎหมายทั้งปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กรเช่นเดียวกัน โดยมีรายละเอียด ดังนี้

2.7.1.1 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร

Deloitte (2018) ได้ทำการวิจัยศึกษาถึงแนวทางการดำเนินงานอย่างยั่งยืนของธุรกิจบริการทางการเงินหลังมีการปรับใช้กฎหมาย GDPR ในสหราชอาณาจักร โดยจากการสัมภาษณ์ผู้เชี่ยวชาญทางด้านการคุ้มครองข้อมูลส่วนบุคคลจากธุรกิจบริการทางการเงินของ Deloitte องค์กรที่ให้บริการทางการเงิน และสำนักงานคณะกรรมการด้านข้อมูลข่าวสารของสหราชอาณาจักร รวมถึงสัมภาษณ์ผู้เชี่ยวชาญที่ทำงานในภาคธุรกิจต่าง ๆ ทั้งในและนอกสหภาพยุโรปพบว่า โดยทั่วไปแล้วบริษัทที่ให้บริการทางการเงินสามารถปฏิบัติตาม GDPR ได้ง่ายกว่าธุรกิจภาคส่วนอื่น ๆ เนื่องจากได้ดำเนินการอย่างเข้มงวดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลมาอย่างยาวนานโดยหน่วยงานกำกับดูแลทางการเงิน แต่อย่างไรก็ตามการปฏิบัติตาม GDPR ก็ยังมีความท้าทายและส่งผลกระทบในวงกว้าง ซึ่งสามารถแบ่งผลกระทบออกเป็น 5 ปัจจัย ดังนี้

(1) ผลกระทบทางด้านต้นทุน (Cost)

Deloitte (2018) ระบุว่า เพื่อการปฏิบัติตาม GDPR บริษัทต้องมีการลงทุนเพิ่ม พบว่า 51% ของภาคอุตสาหกรรมการเงินมีการลงทุนไปแล้วบางส่วนแต่อีก 46 % กลับมองว่าไม่ใช่เรื่องสำคัญนักจึงไม่ได้มีการลงทุนเกี่ยวกับเรื่องดังกล่าว ในขณะที่ภาคอุตสาหกรรมอื่นมีการลงทุนในเรื่องดังกล่าวมากถึง 90% และเพียง 8% เท่านั้นที่ระบุว่าปฏิบัติตามข้อกำหนดไม่ใช่เรื่องสำคัญและไม่ได้มีการลงทุนเพื่อปฏิบัติตาม

Abi (2018) กล่าวว่า ไม่มีธนาคารใดที่ไม่ได้รับผลกระทบ Sia Partners แจ้งว่าโดยเฉลี่ยแล้วค่าใช้จ่ายในการดำเนินการตาม GDPR สำหรับธนาคารในสหราชอาณาจักรมีค่าใช้จ่ายอยู่ที่ 66 ล้านปอนด์ซึ่งเป็นค่าใช้จ่ายสูงสุดของทุกภาคอุตสาหกรรม ในขณะที่ต้นทุนสำหรับ Non-Banking มีค่าใช้จ่ายที่ต่ำกว่ามาก (เฉลี่ย 8 ล้านปอนด์) อย่างไรก็ตามแม้ว่าการปฏิบัติตามข้อกำหนดจะมีค่าใช้จ่ายสูงแต่การไม่ปฏิบัติตามกฎหมายอาจมีค่าใช้จ่ายที่สูงกว่า โดยสถาบันการเงินต้องเผชิญกับค่าปรับที่สูงขึ้นอย่างมากสำหรับการละเมิดข้อมูล จากการวิเคราะห์ของ NCC Group สำนักงานคณะกรรมการข้อมูล (ICO) กำหนดค่าปรับมูลค่า 880,500 ปอนด์ ในปี 2559 ภายใต้ GDPR ค่าปรับจะอยู่ที่ 69 ล้านปอนด์ซึ่งสูงกว่า 79 เท่า

(2) ผลกระทบทางด้านเทคโนโลยี (Technology)

การลงทุนทางด้านเทคโนโลยีเพื่อช่วยในการปฏิบัติตามกฎหมาย

Deloitte (2018) จากผลการสำรวจพบว่าเกินกว่า 70% ไม่ว่าจะเป็นอุตสาหกรรมการเงินหรือภาคอุตสาหกรรมอื่น ส่วนใหญ่เลือกใช้เทคโนโลยีเข้ามาเป็นตัวช่วยในการคุ้มครองข้อมูลส่วนบุคคล เทคโนโลยีมีส่วนสำคัญในการคุ้มครองข้อมูล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ซึ่งเทคโนโลยีสามารถช่วยในการระบุและลดความเสี่ยงในการคุ้มครองข้อมูลซึ่งเป็นส่วนหนึ่งของแนวปฏิบัติตามกฎหมาย GDPR

ส่งเสริมและพัฒนาเทคโนโลยีในภาคธุรกิจมุ่งสู่ธนาคารยุคดิจิทัล

PricewaterhouseCoopers (2017) ได้วิเคราะห์ผลกระทบจาก GDPR ต่อธุรกิจธนาคารในประเทศสวิตเซอร์แลนด์ โดย PwC กล่าวว่าผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือ ระบบ IT ที่เกี่ยวข้องกับการทำงาน ซึ่ง PwC เห็นโอกาสในการปฏิบัติตาม GDPR ที่สามารถนำไปสู่ประสิทธิภาพในการปฏิบัติงานและการสร้างชื่อเสียงที่ดีเตรียมความพร้อมสู่ยุคดิจิทัล

Brian (2019) ได้กล่าวถึงผลกระทบของ GDPR ต่อธนาคารดิจิทัล (Digital Banking) ไว้ว่าการเติบโตของธนาคารดิจิทัลนั้นขึ้นอยู่กับความไว้วางใจของผู้บริโภคที่เพิ่มขึ้น โดยเฉพาะอย่างยิ่งกับการถือกำเนิดของ Open Banking การได้รับความคุ้มครองข้อมูลส่วนบุคคลและความปลอดภัยในการรักษาข้อมูลทางด้านไซเบอร์ อันเป็นผลมาจาก GDPR ที่จะช่วยผลักดันให้ผู้บริโภคหันมาใช้บริการ Open Banking ดังนั้น GDPR จึงเป็นมากกว่าชุดเครื่องมือด้านกฎระเบียบ

แต่เป็นข้อได้เปรียบเชิงกลยุทธ์ที่แท้จริง การบูรณาการการคุ้มครองข้อมูลเข้ากับกลยุทธ์การพัฒนาหลักขององค์กรทำให้เกิดการดำเนินการที่สร้างสรรค์มากขึ้น ภาคนาการกำลังสร้างสรรค์สิ่งใหม่ ๆ มากขึ้นกว่าเดิมซึ่งพิสูจน์ให้เห็นถึงความเชี่ยวชาญด้านเทคโนโลยีและข้อมูลที่เพิ่มขึ้น นอกจากนี้ยังเป็นผลดีต่อการรักษาและส่งเสริมชื่อเสียงขององค์กร

(3) ผลกระทบทางด้านกระบวนการปฏิบัติงาน (Process)

Deloitte (2018) กล่าวว่า ถึงแม้ว่าธุรกิจบริการทางการเงินจะมีความพร้อมที่มากกว่าภาคธุรกิจอื่นแต่การปฏิบัติ GDPR ก็ยังส่งผลกระทบในกระบวนการทำงานในวงกว้างกับหลายแผนกในองค์กร ระบบ IT พนักงาน และลูกค้า รวมถึงบทลงโทษที่มีความรุนแรงและมีความกังวลว่าอาจขัดขวางต่อนวัตกรรมในการประมวลผลข้อมูลของสถาบันการเงิน เช่น การใช้ปัญญาประดิษฐ์

Jennifer (2020) กล่าวว่า GDPR ได้เปลี่ยนแปลงหลายอย่างในบริษัท เช่น วิธีการขายของทีมการตลาด หรือวิธีการจัดการกิจกรรมทางการตลาด บริษัทต้องตรวจสอบกระบวนการทางธุรกิจ แอปพลิเคชันและแบบฟอร์มต่าง ๆ เพื่อให้สอดคล้องกับกฎหมายและแนวทางปฏิบัติด้าน Email Marketing ในการติดต่อสื่อสารกับกลุ่มลูกค้าเป้าหมาย

(4) ผลกระทบทางด้านทรัพยากรบุคคล (Human Resource)

Deloitte (2018) กล่าวว่า GDPR ได้ส่งผลกระทบเป็นวงกว้างทั้งองค์กร รวมถึงทรัพยากรบุคคล ซึ่งสามารถแบ่งออกเป็น 3 ประเด็น ได้แก่

สรรหาพนักงานเพิ่ม โดย GDPR ส่งผลกระทบในเรื่องของการสรรหาบุคลากร โดยองค์กรต้องสรรหาพนักงานที่มีความเชี่ยวชาญด้านการคุ้มครองข้อมูลโดยเฉพาะ ในบริษัทใหญ่ ๆ จะมีการสรรหาเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ผู้จัดการความเป็นส่วนตัวของข้อมูล และเจ้าหน้าที่อาวุโสที่ปฏิบัติงานเกี่ยวกับการปฏิบัติตามข้อกำหนด GDPR

เพิ่มภาระหน้าที่งานให้กับคนในองค์กร บริษัทขนาดเล็กอาจไม่สามารถจ้างผู้เชี่ยวชาญแบบบริษัทใหญ่ ๆ จึงจำเป็นต้องจัดสรรความรับผิดชอบในการคุ้มครองข้อมูลให้กับผู้เชี่ยวชาญด้านกฎหมายหรือผู้เชี่ยวชาญด้านการปฏิบัติตามกฎระเบียบ โดยระบุความรับผิดชอบเกี่ยวกับ GDPR เพิ่มเติมเป็นส่วนหนึ่งของหน้าที่งาน

พนักงานทุกคนในองค์กรต้องได้รับการอบรม ไม่เพียงแต่พนักงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลเท่านั้น สำหรับพนักงานในบริษัทที่ไม่ใช่ผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลที่ทำงานนอกฝ่ายจัดการข้อมูล แผนกกฎหมาย (Legal) และการปฏิบัติตามกฎระเบียบ (Compliance) เช่น ผู้จัดการฝ่ายลูกค้าสัมพันธ์ ผู้จัดการฝ่ายการตลาด ผู้จัดการฝ่ายขาย และเจ้าหน้าที่ฝ่ายขาย จะต้องได้รับการฝึกอบรมในพื้นฐานของการปฏิบัติตาม GDPR และย้ำเตือนเป็นประจำเกี่ยวกับขั้นตอนและแนวทางปฏิบัติที่ต้องปฏิบัติตาม

(5) ผลกระทบด้านรายได้ (Revenue)

Deloitte (2018) กล่าวว่า ผู้ปฏิบัติงานในอุตสาหกรรมการเงินเห็นว่าการปฏิบัติตาม GDPR ส่งผลดีต่อธุรกิจในการเพิ่มความไว้วางใจของลูกค้า ตามมาด้วยการเพิ่มประสิทธิภาพในการประมวลผลข้อมูล และลดโอกาสที่จะเกิดความเสียหายต่อชื่อเสียงเนื่องจากต้นทุนเกิดขึ้นจากการละเมิดข้อมูลนั้นไม่ได้มีเพียงค่าปรับตามกฎหมายแต่มันยังรวมถึงความเสียหายด้านชื่อเสียง การสูญเสียความไว้วางใจจากลูกค้าส่งผลต่อรายได้และผลกำไรที่ลดลง

แต่อย่างไรก็ตามสำหรับผลกระทบต่อการดำเนินธุรกิจและความสำเร็จในการดำเนินธุรกิจบางกลุ่มมองว่าการคุ้มครองข้อมูลส่วนบุคคลขัดขวางประสิทธิภาพในการดำเนินงานและความสามารถในการสร้างรายได้ของธุรกิจ แต่ทว่าสถาบันการเงินนั้นได้รับผลกระทบน้อยกว่าธุรกิจประเภทอื่น ๆ

Jennifer (2020) กล่าวว่า แม้ว่า GDPR จะสร้างความท้าทายและความเจ็บปวดกับธุรกิจแต่ก็สร้างโอกาสด้วยเช่นกัน บริษัทที่สามารถแสดงให้เห็นว่าบริษัทได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลนอกเหนือจากการปฏิบัติตามกฎหมายเท่านั้นจะเป็นการสร้างความไว้วางใจให้กับลูกค้าและเป็นการรักษาลูกค้าให้มีความภักดีต่อบริษัทมากขึ้นและส่งผลต่อรายได้ของบริษัท

ดังนั้นกล่าวโดยสรุปแล้ว GDPR ทำให้ความเชื่อมั่นของลูกค้าเพิ่มขึ้น เพิ่มประสิทธิภาพในการประมวลผลข้อมูล และลดโอกาสเสี่ยงในการถูกปรับและเสียชื่อเสียงจากการถูกฟ้องร้อง นอกจากนี้ยังเป็นการสร้างโอกาสในการแข่งขันหากบริษัทสามารถทำได้ดีและมากกว่าที่กฎหมายกำหนดจะเป็นการสร้างความไว้วางใจและรักษาลูกค้าให้มีความภักดีต่อบริษัท ซึ่งส่งผลทำให้รายได้ของบริษัทที่เพิ่มขึ้น

2.7.1.2 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร

(1) ผลกระทบต่อลูกค้า (Customer)

PricewaterhouseCoopers (2017) ได้วิเคราะห์ผลกระทบจาก GDPR ต่อธุรกิจธนาคารในประเทศสวิตเซอร์แลนด์ โดย PwC กล่าวว่าผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือประเภทยของลูกค้า การปฏิสัมพันธ์กับลูกค้า และการนำเสนอบริการแก่ลูกค้า

Steven (2020) กล่าวว่า แทนที่จะพยายามขายให้กับกลุ่มลูกค้ารายใหม่ที่ไม่ได้อยู่ในตลาด GDPR กลับมุ่งเน้นไปที่การสร้างความสัมพันธ์และขายให้กับผู้ที่ต้องการสินค้าหรือบริการที่มีความสนใจและพร้อมที่จะซื้อมากกว่า GDPR ช่วยให้ผู้มีโอกาสนี้เป็นลูกค้าที่มีคุณภาพมากกว่ากลุ่มเป้าหมายจำนวนมาก GDPR ไม่ได้เป็นข้อจำกัดในวิธีการขายกลุ่มลูกค้าใหม่ ๆ หรือธุรกิจใหม่ ๆ แต่ GDPR จะทำให้ธุรกิจและทีมขายบรรลุ KPI ได้อย่างรวดเร็วสร้างโอกาสในการขายที่มีคุณภาพมากขึ้นเข้าถึงผู้มีโอกาสเป็นลูกค้ามากขึ้นและมีอัตราการปิดการขายที่สูงขึ้น

ดังนั้นสามารถสรุปได้ว่าผลกระทบต่อลูกค้าคือกระบวนการในการให้บริการ การนำเสนอสินค้า การสื่อสารกับลูกค้า รวมถึงประเภทของลูกค้าจะเปลี่ยนแปลงไปโดยจะมุ่งเน้นไปที่กลุ่มลูกค้าที่ตรงเป้าหมายมากขึ้น

(2) ผลกระทบต่อผู้ค้า (Supplier/Vendor)

วิชญ์ วงศ์หาญเชาว์ (2562) กล่าวว่า สำหรับองค์กรที่ทำงานร่วมกับผู้ให้บริการด้านไอที หรืออยู่ระหว่างพิจารณาคัดเลือกผู้ให้บริการระบบความปลอดภัยเพิ่มเติม จะต้องแน่ใจว่า ผู้ให้บริการหรือเวนเดอร์นั้น ๆ จะต้องเข้าใจ และให้ความสำคัญกับงานด้านความปลอดภัยในการประมวลผลข้อมูลตามกฎหมายของ GDPR รวมถึงเป็นการเตรียมรับมือต่อกฎด้านความปลอดภัยอื่นใดที่จะเกิดขึ้นต่อไปในอนาคต

2.7.1.3 แนวทางการบริหารองค์กรภายใต้การปรับใช้กฎหมายคุ้มครองข้อมูล

ส่วนบุคคล

(1) การบริหารจัดการสภาพแวดล้อมภายในองค์กร

จากบทความ Information Governance (IG) ของ ธนากร แห่งประเทศไทย (2557) กล่าวว่า Information Governance มีบทบาทนอกเหนือจากการดูแลข้อมูลตั้งแต่ต้นจนจบ แต่ยังครอบคลุมถึงการบริหารจัดการความเสี่ยงการใช้งานให้ถูกต้องตามกฎหมายระเบียบ และกระบวนการทำงาน โดยอาศัย 3 ปัจจัยหลักเข้ามาควบคุม คือ คน (People), กระบวนการ (Process) และเทคโนโลยี (Technology) โดย 3 ปัจจัยดังกล่าวจำเป็นต้องสอดคล้องตามนโยบาย และกลยุทธ์ขององค์กร ตามกรอบแนวคิด คน กระบวนการ และเทคโนโลยี (PPT Framework)

People: ส่งเสริมและสร้างความตระหนักรู้ (Awareness) ให้กับพนักงานในการใช้และส่งต่อข้อมูลสำคัญด้วยความระมัดระวัง โดยใช้ช่องทางที่ปลอดภัย หรือเข้ารหัสข้อมูลด้วยโปรแกรมเสริม พร้อมทั้งประชาสัมพันธ์ และจัดอบรมให้ความรู้ ความเข้าใจในวงกว้าง

Process: มีระเบียบและวิธีปฏิบัติ เพื่อให้พนักงานได้ปฏิบัติตาม รวมถึงมีกระบวนการต่าง ๆ ในการปฏิบัติงานสำหรับพนักงานที่มีหน้าที่ดูแลระบบให้มีความปลอดภัย และพร้อมใช้งาน

Technology: มีการประยุกต์ใช้เครื่องมือและอุปกรณ์เพื่อป้องกัน ภัยคุกคามในทุกระดับ (Layer) ทั้งความเสี่ยงที่อาจเกิดขึ้นจากภายนอก และภายใน เพื่อปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

(2) การบริหารจัดการสภาพแวดล้อมภายนอกองค์กร

Emma (2019) กล่าวว่า อุตสาหกรรมดิจิทัลเป็นอุตสาหกรรมที่มีข้อมูลเป็นศูนย์กลาง ดังนั้นจึงขึ้นอยู่กับความไว้วางใจของผู้บริโภค วิธีหนึ่งที่ดีที่สุดในการสร้างความไว้วางใจต่อลูกค้าได้คือการแสดงให้เห็นว่าแนวทางการจัดการข้อมูลขององค์กรนั้นมีประสิทธิภาพและมี

จริยธรรม จะได้เปรียบในการแข่งขัน ดังนั้นความปลอดภัยของข้อมูลจึงเป็นส่วนสำคัญของกลยุทธ์ Digital Banking และสิ่งที่สำคัญอีกหนึ่งประกาศ คือ ทัศนคติของผู้มีอำนาจตัดสินใจสูงสุดโดยให้ มุ่งเน้นไปที่โอกาสในการแข่งขันมากกว่าการเป็นอุปสรรค หากผู้ที่มีอำนาจในการตัดสินใจเริ่มเห็น GDPR เป็นตัวช่วยประกอบกับวิธีการควบคุมข้อมูลลูกค้าที่สร้างความไว้วางใจ รวมถึงการสื่อสารที่มี ประสิทธิภาพกับลูกค้าเพื่อให้มั่นใจว่าข้อมูลของพวกเขาปลอดภัยจึงจะเกิดเป็นความได้เปรียบในการ แข่งขัน สิ่งนี้สามารถปูทางไปสู่การบริหารงานที่สร้างสรรค์เพื่อขับเคลื่อนนวัตกรรมและความสำเร็จ ให้กับองค์กร

มร.รอยซ์ เทียว (2561) กล่าวว่า GDPR กฎข้อบังคับใหม่นี้อาจดูเหมือน เป็นการเพิ่มภาระแต่ควรมองว่าเป็นโอกาสที่จะช่วยให้องค์กรทั้งหลายใช้ประโยชน์จากข้อมูลให้มาก ที่สุด เรากำลังก้าวสู่โลกที่ขับเคลื่อนด้วยข้อมูลการที่จะประสบความสำเร็จในการใช้ข้อมูลนี้ วิธีการ บริหารจัดการข้อมูลของธุรกิจต่าง ๆ จะต้องได้รับความไว้วางใจจากสาธารณชน สร้างความต่างในการ แสวงหาโอกาสดี ๆ ทางการตลาด หรือนำไปสู่ความสำเร็จเหนือคู่แข่งได้อีกด้วย

ข้อมูลอาจช่วยชี้ให้เห็นโอกาสที่จะลดค่าใช้จ่ายหรือเปิดตลาดใหม่ ๆ ข้อมูลจึงมีค่ามากกว่าแค่การรับรู้ แต่ต้องได้รับการบันทึก แยกแยะ ให้มีความสำคัญ และนำไปใช้ให้เป็น ประโยชน์ องค์กรธุรกิจจึงไม่ควร รอดู และทำตามข้อกำหนดขั้นต่ำของกฎหมายนี้เท่านั้น ในทาง ตรงกันข้ามหากลงมือทำทันที แนวทางการเข้าใช้ข้อมูลของตนเป็นไปตามข้อกำหนด และมีความ มั่นใจที่จะสร้างความพึงพอใจให้กับลูกค้าของตนอย่างต่อเนื่อง ด้วยบริการที่เป็นส่วนตัวให้ตรงความ ต้องการของลูกค้าแต่ละรายได้ดีขึ้นและมากขึ้น องค์กรที่ทำงานเชิงรุกและมองข้ามภาระด้าน กฎระเบียบระยะสั้นไปได้เท่านั้น จะได้รับโอกาสใหญ่ ๆ ที่มาพร้อมกับการเปลี่ยนแปลงสำคัญต่าง ๆ ที่เกิดขึ้นเสมอ

ดังนั้นจึงสามารถสรุปได้ว่าปัจจัยภายนอกที่องค์กรควรให้ความสำคัญคือ ลูกค้า (Customer) โดยบริษัทควรใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นโอกาสในการสร้างการ แข่งขันโดยมุ่งเน้นการสร้างเชื่อมั่นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้กับลูกค้า ควบคู่กับ การใช้ข้อมูลให้เกิดประโยชน์ในการสร้างความพึงพอใจให้กับลูกค้า

2.7.2 งานวิจัยแนวทางการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

จากบทความงานวิจัยของ กิตติพงศ์ กมลธรรมวงศ์ (2563) ในหัวข้อเรื่อง ประสิทธิภาพของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยสารณรัฐสิงคโปร์: บทเรียนสำหรับ ประเทศไทย เนื่องจากประเทศไทยเพิ่งมีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำเป็นต้องอาศัยประสบการณ์ของต่างประเทศที่ประสบความสำเร็จมาใช้ในการเตรียมความพร้อม สำหรับประเทศไทยและในบรรดากลุ่มประเทศอาเซียนที่น่าสนใจ คือ ประเทศสิงคโปร์ที่มีการ

ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลและมีผลบังคับใช้ทุกมาตราเมื่อวันที่ 2 กรกฎาคม ค.ศ. 2014 โดยมีการเตรียมความพร้อมมากมาย ซึ่งประกอบด้วยหลายกิจกรรมที่น่าสนใจ ได้แก่ การจัดกิจกรรมสัมมนาเผยแพร่ความรู้ในกลุ่มเป้าหมายหลายครั้ง การสร้างเครือข่ายความร่วมมือกับกลุ่มองค์กรทางการค้าและอุตสาหกรรม การผลิตสื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายไปยังประชาชนและองค์กรเอกชนในรูปแบบต่าง ๆ

ซึ่งในบทความงานวิจัยได้กล่าวถึงประเด็นต่าง ๆ โดยเฉพาะประสบการณ์ของประเทศสิงคโปร์ในการเตรียมการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเมื่อเปรียบเทียบกับประเทศอื่น ๆ ในอาเซียน ที่สามารถนำมาเป็นบทเรียนในการดำเนินงานเตรียมความพร้อมของหน่วยงานรัฐที่เกี่ยวข้องต่อไป โดยมีประเด็นที่น่าสนใจ ดังนี้

2.7.2.1 ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศ

อาเซียน

ในบรรดากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในกลุ่มประเทศอาเซียน มีตัวอย่างที่น่าสนใจของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียนจะพบอยู่สองประเทศที่มีความก้าวหน้าอย่างมาก ได้แก่ ประเทศมาเลเซีย และสิงคโปร์

โดยมาเลเซียในระยะเริ่มต้นการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล หน่วยงานต่าง ๆ โดยเฉพาะภาคเอกชนมีความตื่นตัวในการแลกเปลี่ยนข้อมูลเพื่อหาแนวทางปฏิบัติตามกฎหมายกันอย่างมาก องค์กรในภาคการเงินที่มีมาตรฐานการคุ้มครองข้อมูลค่อนข้างสูงอยู่แล้วเป็นแนวทางในการปฏิบัติตามกฎหมายและแบ่งปันแนวปฏิบัติ (Guideline) ของภาคธุรกิจให้ภาคธุรกิจส่วนอื่น ๆ ด้วย เนื่องจากเดิมองค์กรมีความเชื่อมโยงกับบริษัทในต่างประเทศโดยเฉพาะประเทศใน EU ที่มีกฎหมาย GDPR ซึ่งมีแนวปฏิบัติที่เป็นมาตรฐานสากลซึ่งสูงกว่ามาตรฐานใหม่ตามกฎหมายของมาเลเซียอยู่แล้ว

ขณะเดียวกันในประเทศสิงคโปร์นับว่าเป็นประเทศล่าสุดก่อนหน้าประเทศไทยที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้อย่างเป็นทางการเมื่อเดือนกรกฎาคม พ.ศ. 2557 สิงคโปร์ได้ใช้เวลาเตรียมความพร้อมกันเวลานานถึง 18 เดือน เพราะเห็นถึงความสำคัญของกฎหมายที่กระทบกับองค์กรธุรกิจจำนวนมาก รวมถึงบริษัทต่างชาติอื่น ๆ ที่อยู่ในต่างประเทศที่อาจมีการส่งต่อข้อมูลจากสิงคโปร์ไปยังประเทศที่สามต้องปฏิบัติตามมาตรการของกฎหมาย PDPA ด้วยเช่นกัน

2.7.2.2 ลักษณะร่วมกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศ

อาเซียน

อาเซียน 4 ประเทศ (ประเทศอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์) มีลักษณะร่วมกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคล 3 ประการ ดังนี้

(1) การปฏิบัติตามมาตรฐานสากล (Standardization)

การคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นไปในทิศทางเดียวกัน คือ เป็นการยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงแต่เพื่อรักษาสิทธิของเจ้าของข้อมูลเท่านั้น แต่เป็นการสร้างมาตรฐานที่ชัดเจนเพื่อเพิ่มโอกาสทางเศรษฐกิจให้กับเอกชนของประเทศตนด้วย นำไปสู่การสร้างโอกาสในการแข่งขันเชิงเศรษฐกิจ เนื่องจากการเพิ่มความไว้วางใจของผู้บริโภคทั้งในประเทศตนเองและในต่างประเทศ

(2) การคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาทางเศรษฐกิจ

การสร้างมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ด้อยไปกว่าประเทศอื่น ๆ และสอดคล้องกับมาตรฐานสากลจึงเป็นพื้นฐานที่จำเป็นต่อการพัฒนาธุรกิจบริการในอนาคตให้มีความสามารถแข่งขันกับนานาชาติ นอกจากนี้ยังช่วยสร้างวัฒนธรรมการเคารพสิทธิส่วนบุคคลให้เกิดขึ้นในสังคม รวมทั้งช่วยสร้างความตระหนักรู้ในสิทธิที่จะเข้าถึง ปกป้อง และควบคุมข้อมูลส่วนบุคคลของเอกชนให้เกิดขึ้น ทำให้เกิดความเข้าใจระหว่างผู้ประกอบการและผู้บริโภค เพิ่มความน่าเชื่อถือให้ผู้ประกอบการ และมีความคล่องตัวในการใช้ข้อมูลที่เก็บมาให้เป็นประโยชน์อย่างแท้จริง

(3) การยอมรับมาตรฐานสากลและกรอบความร่วมมือระหว่างประเทศ

มีมาตรฐานสากลหลากหลายที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้ง OECD Guidelines ที่มีอิทธิพลต่อการร่างกฎหมายของหลายประเทศ และ EU GDPR ที่สร้างมาตรฐานอันเคร่งครัดของยุโรปซึ่งส่งผลกระทบให้คู่ค้าของยุโรปต้องเร่งจัดทำกฎหมายภายในของตนให้มีมาตรฐานไม่ต่ำกว่าของยุโรปด้วย สำหรับประเทศไทยนั้นระหว่างการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการคำนึงถึงเป็นพิเศษในเรื่องนี้และได้มีการบัญญัติหลักการของกฎหมายไทยให้สอดคล้องกับหลักเกณฑ์ของ GDPR

2.7.2.3 บทเรียนการเตรียมความพร้อมในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์

มีประเด็นที่น่าสนใจที่ประเทศไทยควรจะต้องทำอย่างเร่งด่วน คือ เรื่องการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายไปยังประชาชนและองค์กรเอกชน กฎหมายใหม่มีผลกระทบในการปฏิบัติงานขององค์กรเอกชนในการทำหน้าที่ตามที่กฎหมายกำหนด และการให้ประชาชนได้รับรู้ถึงสิทธิต่าง ๆ ที่ได้รับการคุ้มครองตามกฎหมายในเรื่องข้อมูลส่วนบุคคล นับว่าเป็นเรื่องที่สำคัญอย่างยิ่งต่อความสำเร็จในการบังคับใช้กฎหมาย โดยมีการสัมมนาที่มีเนื้อหามุ่งเน้นไปยังการสร้างความรู้ความเข้าใจในเชิงลึกเกี่ยวกับการปฏิบัติตามกฎหมายที่ถูกต้อง การพัฒนาแผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องของตัวองค์กรธุรกิจที่เข้าร่วม ส่วนการให้ความรู้แก่ผู้บริโภคที่เป็นประชาชนโดยจัดนิทรรศการและเผยแพร่เอกสารความรู้เกี่ยวกับการคุ้มครองในรูปแบบต่าง ๆ

เช่น เอกสารแนะนำ ภาพเคลื่อนไหว (Video Clips) ซึ่งพิจารณาถึงกลุ่มเป้าหมายและเนื้อหาที่มีความสำคัญซึ่งต้องมีการเผยแพร่เพื่อให้บรรลุวัตถุประสงค์ในการเสริมสร้างความรู้ความเข้าใจที่ถูกต้อง

2.7.2.4 ข้อเสนอการเตรียมความพร้อมเพื่อการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

ความสำเร็จของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นไม่ได้เกิดจากการบัญญัติเนื้อหากฎหมายที่ดีเท่านั้น แต่ต้องมีการเตรียมความพร้อมก่อนการบังคับใช้ด้วย เพราะกฎหมายส่งผลกระทบทั้งทางด้านองค์กรธุรกิจและประชาชนซึ่งหากไม่รู้สิทธิที่ได้รับตามกฎหมายคงไม่เข้าใจถึงสิทธิของตนที่แท้จริง

ดังนั้นสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องเตรียมความพร้อมรองรับการปรับใช้กฎหมายไม่ว่าจะเป็นการสร้างการรับรู้ร่วมกันทุกภาคส่วนทั้งภาคเอกชน ภาครัฐและประชาชนทั่วไปให้รับทราบถึงข้อกำหนดสำคัญตามกฎหมาย การสร้างความตระหนักใน ความสำคัญของข้อมูลส่วนบุคคล การเผยแพร่องค์ความรู้และความเข้าใจที่ถูกต้องผ่านช่องทางสื่อสารต่าง ๆ ด้วยรูปแบบที่เหมาะสมกับกลุ่มเป้าหมายแต่ละกลุ่ม โดยเป็นความร่วมมือกันระหว่างภาครัฐ และภาคเอกชนเพื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับเรื่องดังกล่าว

จากการศึกษางานวิจัยและบทความที่เกี่ยวข้องโดยงานวิจัยของ Deloitte (2018) ได้ศึกษาถึงแนวทางการดำเนินงานอย่างยั่งยืนของธุรกิจบริการทางการเงินหลัง มีการปรับใช้กฎหมาย GDPR ในสหราชอาณาจักรที่มีการเก็บข้อมูลจากการสัมภาษณ์ผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจบริการทางการเงินของ Deloitte องค์กรที่ให้บริการทางการเงิน และสำนักงานคณะกรรมการด้านข้อมูลข่าวสารของสหราชอาณาจักร รวมถึงสัมภาษณ์ผู้เชี่ยวชาญ ที่ทำงานในภาคธุรกิจต่าง ๆ ทั้งในและนอกสหภาพยุโรป ซึ่งชี้ให้เห็นว่าองค์กรได้รับผลกระทบในด้านต่าง ๆ ทั้งภายในและภายนอกองค์กร เพื่อปรับปรุงแนวทางการปฏิบัติงานให้เป็นไปตามข้อกำหนดของกฎหมาย GDPR ซึ่งถือเป็นภาระงานที่องค์กรต้องเผชิญ แต่อย่างไรก็ตามองค์กรควรจะใช้กฎหมายฉบับนี้สร้างโอกาสในการแข่งขัน ในเรื่องของการสร้างความเชื่อมั่น ความไว้วางใจให้กับลูกค้าและส่งเสริมเทคโนโลยีในภาคธุรกิจให้สอดคล้องกับธนาคารในยุคดิจิทัลจึงต้องมีการเปลี่ยนแปลงครั้งใหญ่ในองค์กรเพื่อตอบรับกับการปรับใช้กฎหมาย

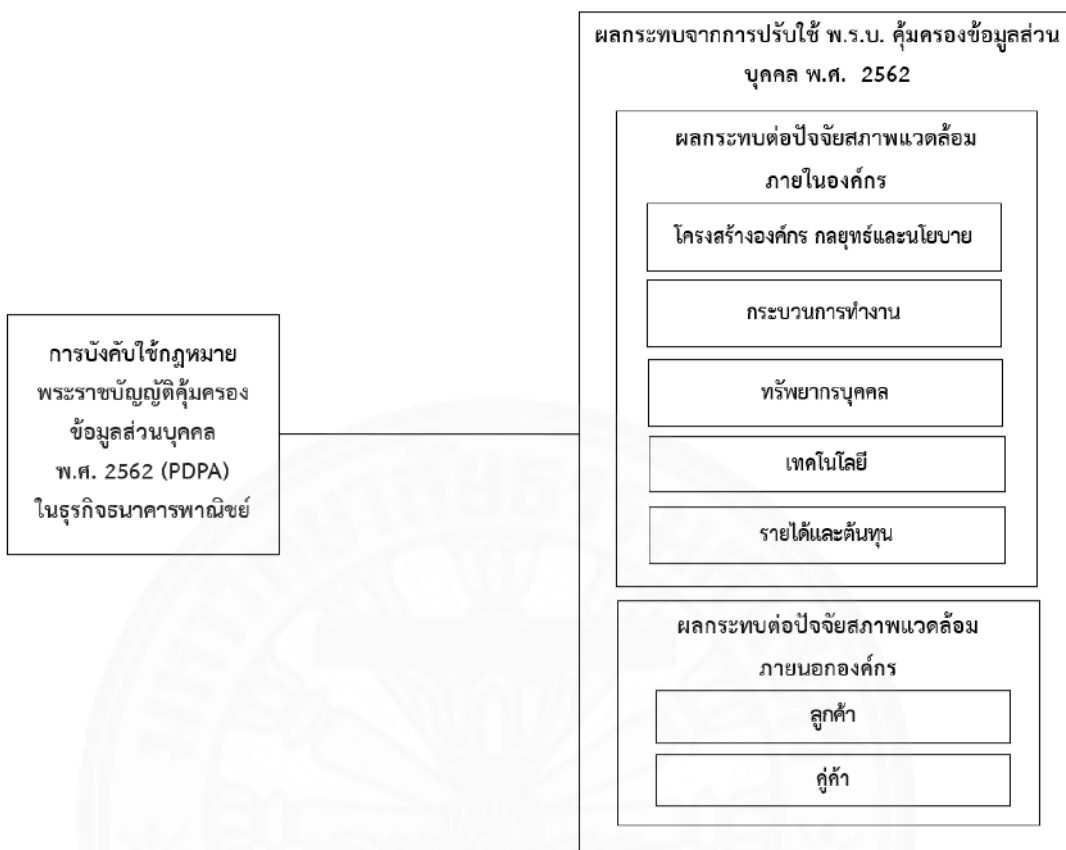
ดังนั้นงานวิจัยฉบับนี้จึงทำการศึกษาในบริบทของประเทศไทยที่มีการออกพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของประเทศไทย โดยศึกษาถึงผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในประเทศไทย รวมถึงแนวทางในการดำเนินการและการพัฒนาองค์กรภายใต้ข้อกำหนดตามกฎหมายซึ่งมีต้นแบบมาจากกฎหมาย GDPR ในประเทศยุโรป โดยทำการสัมภาษณ์ผู้บริหารและเจ้าหน้าที่ที่ปฏิบัติงานทางด้าน

การคุ้มครองข้อมูลส่วนบุคคลในธุรกิจธนาคารพาณิชย์ในประเทศไทย และผู้เชี่ยวชาญทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้เชี่ยวชาญทางด้านการบริหารจัดการข้อมูล และหน่วยงานกำกับดูแลภาคธุรกิจ

2.8 กรอบแนวคิดการวิจัย

กรอบแนวคิดการวิจัย (Research Framework) อ้างอิงตามแนวคิดการบริหารการเปลี่ยนแปลงและรูปแบบการเปลี่ยนแปลงองค์กรประกอบกับงานวิจัยแนวทางการดำเนินงานอย่างยั่งยืนของธุรกิจบริการทางการเงินหลังมีการปรับใช้กฎหมาย GDPR ในสหราชอาณาจักร

ดังนั้นจึงนำไปสู่กรอบแนวคิดการวิจัยที่อธิบายว่าเมื่อมีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นปัจจัยภายนอกที่ทำให้ธนาคารต้องมีการเปลี่ยนแปลงเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามกฎหมายธนาคารจึงต้องมีการเปลี่ยนแปลงสภาพแวดล้อมภายในองค์กรตามแนวคิดรูปแบบการเปลี่ยนแปลงองค์กรซึ่งส่งผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร ได้แก่ การเปลี่ยนแปลงโครงสร้างองค์กร การเปลี่ยนแปลงเทคโนโลยี การเปลี่ยนแปลงทรัพยากรบุคคล การเปลี่ยนแปลงต้นทุน และกระบวนการทำงาน นอกนี้จากงานวิจัยแนวทางการดำเนินงานอย่างยั่งยืนของธุรกิจบริการทางการเงินหลังมีการปรับใช้กฎหมาย GDPR ในสหราชอาณาจักร ยังชี้ให้เห็นถึงผลกระทบในสภาพแวดล้อมภายนอกองค์กรเพิ่มเติม ได้แก่ ลูกค้าและคู่ค้า จึงสามารถสรุปกรอบแนวคิดการวิจัยตามแผนภาพด้านล่างนี้



ภาพที่ 2.1 กรอบแนวคิดงานวิจัยเรื่องผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย

บทที่ 3 วิธีการวิจัย

การศึกษาลงพื้นที่จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) เพื่อมุ่งเน้นการสะท้อนให้เห็นถึงผลกระทบขององค์กรในภาคธุรกิจธนาคารพาณิชย์จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงแนวทางการบริหารจัดการขององค์กรและแนวทางการพัฒนาการบริหารองค์กรภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย โดยผู้วิจัยได้กำหนดหัวข้อระเบียบการวิจัยดังนี้

- 3.1 แหล่งข้อมูลที่ใช้ในการวิจัย
- 3.2 ลักษณะประชากร
- 3.3 กลุ่มตัวอย่างที่ใช้ในการวิจัย
- 3.4 เครื่องมือที่ใช้ในการวิจัย
- 3.5 การเก็บรวบรวมข้อมูลและการวิเคราะห์ข้อมูล

3.1 แหล่งข้อมูลที่ใช้ในการวิจัย

งานวิจัยฉบับนี้เก็บรวบรวมข้อมูลจาก 2 แหล่งข้อมูลหลักด้วยกัน ได้แก่

3.1.1 ข้อมูลปฐมภูมิ (Primary Source)

เป็นข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก (In-Depth Interview) จากผู้บริหาร (Executive Management) และเจ้าหน้าที่ผู้ปฏิบัติงานที่เกี่ยวข้องกับการดำเนินการปรับใช้กฎหมายดังกล่าวของธุรกิจธนาคารพาณิชย์ ผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร

3.1.2 ข้อมูลทุติยภูมิ (Secondary Source)

เป็นข้อมูลจากแหล่งข้อมูลที่มีความหลากหลาย อาทิเช่น บทความวิชาการที่เกี่ยวข้อง งานวิจัย อินเทอร์เน็ต โดยเก็บรวบรวมข้อมูลจากเอกสารที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นโยบายความเป็นส่วนตัว (Privacy Policy) ของแต่ละธนาคาร และหนังสือให้ความยินยอมในการเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคล (Letter of Consent) แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

3.2 ลักษณะประชากร

งานวิจัยฉบับนี้สามารถจำแนกลักษณะประชากรเป็น 2 กลุ่ม ดังนี้

3.2.1 กลุ่มผู้ปฏิบัติงานในอุตสาหกรรมธนาคารพาณิชย์ (Commercial Bank) ซึ่งเป็นกลุ่มผู้ให้ข้อมูลหลัก (Key Informants) ประกอบด้วย

(1) ผู้บริหารของธุรกิจธนาคารพาณิชย์ (Executive / Top Management) โดยเป็นธนาคารพาณิชย์ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย

(2) กลุ่มเจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Management/Staff) เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ฝ่ายกำกับดูแลกิจการ ฝ่ายรักษาความปลอดภัยของข้อมูล ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายกฎหมาย และฝ่ายบริหารความเสี่ยง เป็นต้น

3.2.2 กลุ่มผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร ซึ่งเป็นกลุ่มผู้ให้ข้อมูลทั่วไป (General Informants)

โดยเป็นผู้เชี่ยวชาญทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ปฏิบัติงานที่เกี่ยวข้องกับเรื่องดังกล่าวในหน่วยงานกำกับดูแล (ธนาคารแห่งประเทศไทย) และผู้เชี่ยวชาญด้านการบริหารจัดการข้อมูล

3.3 กลุ่มตัวอย่างที่ใช้ในการวิจัย

กลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ในครั้งนี้ ผู้ทำการวิจัยใช้วิธีการคัดเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) โดยกลุ่มตัวอย่างที่ใช้ในการวิจัยโดยการสัมภาษณ์เชิงลึกแบ่งเป็น 2 กลุ่ม มีรายละเอียด ดังนี้

3.3.1 กลุ่มผู้ปฏิบัติงานในอุตสาหกรรมธนาคารพาณิชย์ (Key Informants) โดยเลือกธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยจำนวน 14 แห่ง ซึ่งกลุ่มผู้ปฏิบัติงานดังกล่าวแบ่งออกเป็น 2 กลุ่ม ประกอบด้วย

(1) ผู้บริหารของธุรกิจธนาคารพาณิชย์ (Executive / Top Management) จำนวน 3-5 คน โดยการสัมภาษณ์จะเลือกสัมภาษณ์กลุ่มตัวอย่างผู้บริหารในตำแหน่งที่เกี่ยวข้อง เช่น ประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการ ผู้บริหารสายงานบริหารความเสี่ยง สายงานกำกับดูแลกิจการ สายงานกฎหมาย สายงานปฏิบัติการ เป็นต้น เพื่อให้เห็นภาพรวมและทิศทางขององค์กรในการปรับตัวต่อการคุ้มครองข้อมูลส่วนบุคคล

(2) เจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินการปรับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวน 5-7 คน โดยการสัมภาษณ์จะเลือกสัมภาษณ์ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เจ้าหน้าที่ฝ่ายรักษาความปลอดภัยของข้อมูล ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายกฎหมาย และฝ่ายบริหารความเสี่ยง เป็นต้น เพื่อให้เห็นมุมมองในการปฏิบัติงานจริง ปัญหา อุปสรรค แนวทางในการดำเนินงานและการพัฒนาในอนาคต

3.3.2 กลุ่มผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร (General Informants) จำนวน 3-5 คน ซึ่งเป็นกลุ่มผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร เช่น ผู้เชี่ยวชาญทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้ที่ปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลของหน่วยงานกำกับดูแล (ธนาคารแห่งประเทศไทย) บริษัทที่ให้บริการด้านการบริหารจัดการข้อมูลหรือการคุ้มครองข้อมูลส่วนบุคคล

ซึ่งจากกลุ่มตัวอย่างที่ใช้ในงานวิจัยถือเป็นกลุ่มตัวอย่างที่ดีของประชากรทำให้เกิดการตีความของข้อมูลครบตามวัตถุประสงค์ตามที่ Bertaux (1981) ได้เสนอแนะว่าขนาดของกลุ่มตัวอย่างสำหรับการวิจัยเชิงคุณภาพที่น้อยที่สุดที่สามารถยอมรับได้อยู่ที่ 15 คน แต่อย่างไรก็ตาม Romney, Batchelder, and Weller (1986) กล่าวว่ากลุ่มตัวอย่างที่เป็นผู้เชี่ยวชาญในอุตสาหกรรมเพียง 4 คนก็สามารถให้ความแม่นยำต่อผลงานวิจัยในระดับสูงและการเก็บข้อมูลจากกลุ่มตัวอย่างทั้ง 2 ประเภทนั้นทำให้ข้อมูลของงานวิจัยมีมิติมากขึ้น

3.4 เครื่องมือที่ใช้ในการวิจัย

เพื่อให้การเก็บรวบรวมข้อมูลสำหรับงานวิจัยมีความครบถ้วน และมีความน่าเชื่อถือ จึงได้กำหนดให้มีการเก็บข้อมูลจากหลายแหล่งข้อมูล (Data Source Triangulation) ซึ่งประกอบด้วยการเก็บข้อมูลจาก 2 แหล่งข้อมูลหลัก ดังนี้

3.4.1 การสัมภาษณ์เชิงลึก (In-Depth Interview)

ผู้วิจัยได้ทำการทบทวนทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อนำมาใช้เป็นแนวทางในการออกแบบคำถามในการสัมภาษณ์เชิงลึกกลุ่มตัวอย่างที่ได้มีการกำหนดหัวข้อศึกษาไว้ล่วงหน้า และนำมาใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลในการทำวิจัยครั้งนี้โดยชุดคำถามสำหรับใช้ในการสัมภาษณ์แบ่งออกเป็น 2 ส่วน ดังต่อไปนี้

ส่วนที่ 1 ชุดคำถามสำหรับกลุ่มผู้ให้ข้อมูลหลัก (Key Informants)

(1) คำถามเกี่ยวกับข้อมูลส่วนตัวทั่วไปของผู้ถูกสัมภาษณ์

- ชื่อ-สกุล ตำแหน่งงาน
- ความรับผิดชอบในส่วนงานที่ดูแล และความรับผิดชอบเกี่ยวกับการ

คุ้มครองข้อมูลส่วนบุคคล

(2) คำถามเกี่ยวกับภาพรวมของการคุ้มครองข้อมูลส่วนบุคคลในภาคธนาคารพาณิชย์ ก่อนและหลังการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ก่อนการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทได้มีการคุ้มครองข้อมูลส่วนบุคคลหรือไม่อย่างไร ภายใต้กฎหมายหรือหลักเกณฑ์ใด
- การคุ้มครองข้อมูลส่วนบุคคลก่อนและหลังการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความแตกต่างหรือมีการเปลี่ยนแปลงอย่างไรในภาคธุรกิจธนาคารพาณิชย์

(3) คำถามเกี่ยวกับผลกระทบที่เกิดขึ้นกับสภาพแวดล้อมทั้งภายในและภายนอกองค์กรจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- หลังจากที่มีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทได้มีการปรับเปลี่ยนโครงสร้างองค์กร กลยุทธ์/นโยบาย และ แนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอย่างไร
- การปรับเปลี่ยนกลยุทธ์/นโยบายและแนวทางปฏิบัติหลังจากมีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของบริษัท ส่งผลกระทบต่อกระบวนการปฏิบัติงานใดบ้าง (Process) และมีผลกระทบอย่างไร
- พนักงานในองค์กรได้รับผลกระทบจากการปรับใช้กฎหมายหรือไม่อย่างไร
- บริษัทได้ลงทุนเพิ่มเติมในเทคโนโลยีเพื่อการคุ้มครองข้อมูลส่วนบุคคลอย่างไร
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นอุปสรรค/โอกาส ต่อการพัฒนาเทคโนโลยีในภาคธุรกิจหรือไม่ เช่นการทำ Digital Banking หรือ Open Banking การประมวลผลด้วย Big Data AI หรือ API เป็นต้น
- การปรับเปลี่ยนกระบวนการทำงานทำให้ส่งผลกระทบต่อความพึงพอใจในการให้บริการและการเปิดเผยข้อมูลของของลูกค้าหรือไม่
- กิจกรรมที่เกี่ยวกับคู่ค้าของบริษัทตั้งแต่การสรรหา คัดเลือก บริหารจัดการ คู่ค้าได้รับผลกระทบจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่อย่างไร

- รายได้และค่าใช้จ่ายขององค์กรได้รับผลกระทบจากพ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 หรือไม่อย่างไร

(4) คำถามเกี่ยวกับมุมมองผู้บริหารต่อ พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 ที่ส่งผลกับธุรกิจธนาคารพาณิชย์

- ในมุมมองของผู้บริหารมีความคิดเห็นต่อ พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 ว่ามีการสร้างโอกาสหรืออุปสรรคต่อภาคธุรกิจอย่างไร

(5) คำถามเกี่ยวกับแนวทางการบริหารจัดการการเปลี่ยนแปลงองค์กรเพื่อตอบสนองต่อการคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລภายใต้ข้อกำหนดตามกฎหมาย

- บริษัทมีแนวทางการบริหารจัดการต่อสภาพแวดล้อมภายในและภายนอกองค์กรเพื่อตอบสนองต่อพ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 อย่างไร

(6) คำถามเกี่ยวกับแนวทางการพัฒนาองค์กรภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย

- บริษัทจะมีแนวทางพัฒนาการบริหารจัดการองค์กรภายใต้ พระราชบัญญัติ คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 อย่างไร

ส่วนที่ 2 ชุดคำถามสำหรับกลุ่มผู้เชี่ยวชาญเกี่ยวกับการคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລและหน่วยงานที่เกี่ยวข้องกับภาคธุรกิจธนาคาร (General Informants)

(1) คำถามเกี่ยวกับข้อมูลส่วนตัวทั่วไปของผู้ถูกสัมภาษณ์

- ประวัติโดยทั่วไปของผู้ถูกสัมภาษณ์และประสบการณ์เกี่ยวกับการคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ

(2) คำถามเกี่ยวกับการเปลี่ยนแปลงในการคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລในภาคธุรกิจก่อนและหลังการประกาศใช้ พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562

การคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລในภาคธุรกิจมีวิวัฒนาการอย่างไร

- หลังการประกาศใช้ พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 เกิดการเปลี่ยนแปลงการคຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລในภาคธุรกิจอย่างไร

- แนวโน้มในอนาคต พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562 จะมีการปรับปรุงแก้ไขเพื่อให้เข้ากับการบริหารงานในยุคปัจจุบันอย่างไร

(3) คำถามในประเด็นเกี่ยวกับมุมมองต่อผลกระทบที่จะเกิดขึ้นกับองค์กรจากการประกาศใช้ พ.ร.บ. คຸ້ມຄອງຂໍ້ມູນສ່ວນບຸກຄລ พ.ศ. 2562

- กฎหมายส่งผลกระทบต่อสภาพแวดล้อมภายในองค์กร เช่น โครงสร้างองค์กร กลยุทธ์ นโยบาย กระบวนการปฏิบัติงาน เทคโนโลยี และพนักงาน หรือไม่อย่างไร

- กฎหมายส่งผลกระทบต่อสภาพแวดล้อมภายนอกองค์กร เช่น ลูกค้า คู่ค้า หรือไม้อย่างไร

- รายได้และค่าใช้จ่ายขององค์กรได้รับผลกระทบจาก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของบริษัทหรือไม่อย่างไร

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อการพัฒนาเทคโนโลยีในภาคธุรกิจหรือไม่ เช่น การทำ Digital Banking หรือ Open banking เป็นต้น

- ในมุมมองของท่านมีความคิดเห็นต่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ว่าเป็นการสร้างโอกาสหรืออุปสรรคต่อภาคธุรกิจอย่างไร

(4) คำถามเกี่ยวกับประเด็นแนวทางการบริหารจัดการการเปลี่ยนแปลงและการพัฒนาองค์กรจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- บริษัทจะต้องมีการแนวทางการบริหารองค์กรและปรับตัวอย่างไรเพื่อให้การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นไปอย่างมีประสิทธิภาพ

- เทคโนโลยีสามารถเข้ามาช่วยให้การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นไปอย่างมีประสิทธิภาพหรือไม่

- บริษัทจะมีแนวทางการพัฒนาการบริหารองค์กรภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างไร

- บริษัทควรมีวิธีการสื่อสารกับบุคคลทั้งภายในและภายนอกองค์กรอย่างไร เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงาน และเป็นประโยชน์ต่อการได้มาซึ่งข้อมูลอันเป็นประโยชน์ต่อองค์กร

3.4.2 การศึกษาข้อมูลจากแหล่งข้อมูลทุติยภูมิ (Secondary Source)

การศึกษาข้อมูลจากแหล่งข้อมูลทุติยภูมิเพื่อบ่งเน้นการศึกษาแนวทางปฏิบัติขององค์กรตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผลกระทบและแนวทางการพัฒนาองค์กรจากการปรับใช้กฎหมายดังกล่าว และแนวทางการบริหารและพัฒนาองค์กร เพื่อใช้สนับสนุนและเป็นแนวทางในการวิเคราะห์ข้อมูลจากแหล่งข้อมูลปฐมภูมิ ผ่านแหล่งข้อมูลที่หลากหลายทั้งหนังสือ งานวิจัยอื่น ๆ ที่เกี่ยวข้อง บทความทางธุรกิจ นโยบายความเป็นส่วนตัว (Privacy Policy) ที่ธนาคารเผยแพร่สาธารณะ รวมถึงการจัดเสวนาออนไลน์ เกี่ยวกับการปรับใช้กฎหมายจากผู้เชี่ยวชาญในด้านต่าง ๆ

3.5 การเก็บรวบรวมข้อมูลและการวิเคราะห์ข้อมูล

การสัมภาษณ์เชิงลึก (In- depth Interview) แบบกึ่งมีโครงสร้าง (Semi-Structured Interview) โดยการสัมภาษณ์กลุ่มตัวอย่างเป็นรายบุคคล เพื่อให้ทราบถึงมุมมองของการบริหารจัดการ โอกาส ข้อจำกัด และข้อเท็จจริงที่เกี่ยวข้องกับผลกระทบจากการปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นการสัมภาษณ์แบบเผชิญหน้า (Face-to-Face Interview) หรือการสัมภาษณ์ทางโทรศัพท์ (Telephone Interview) ในกรณีที่ผู้ให้สัมภาษณ์ไม่สะดวกให้เข้าพบ หรือต้องการข้อมูลภายหลัง คำถามที่ใช้ในการสัมภาษณ์เป็นลักษณะคำถามแบบปลายเปิดที่สอดคล้องกับแนวคิดในการวิจัย โดยคำถามอาจถูกสลับลำดับ ปรับเปลี่ยนหรือเพิ่มเติมตามความเหมาะสมกับสถานการณ์ เน้นเปิดโอกาสให้ผู้สัมภาษณ์ได้แสดงความคิดเห็นในประเด็นต่าง ๆ และถามเพิ่มเติมในบางประเด็นเพื่อความครบถ้วนของข้อมูล

ทั้งนี้ในการสัมภาษณ์จะต้องขออนุญาตบันทึกเสียงจากผู้ถูกสัมภาษณ์ เพื่อนำมาถอดคำพูดและใช้ในการวิเคราะห์ข้อมูลต่อไป โดยรายละเอียดและข้อมูลส่วนตัวของผู้ถูกสัมภาษณ์จะเก็บไว้เป็นความลับ หรือใช้การจดบันทึกแทน ถ้าไม่อนุญาตและผู้วิจัยได้คำนึงถึงจริยธรรมกับผู้ให้สัมภาษณ์ โดยมีการติดต่อขอข้อมูลและความอนุเคราะห์ในการสัมภาษณ์ก่อนดำเนินการสัมภาษณ์จริง พร้อมกับแจ้งวัตถุประสงค์ของการวิจัยก่อนการสัมภาษณ์ทุกครั้ง โดยที่ผู้วิจัยได้เปิดเผยข้อมูลตามที่ผู้ให้สัมภาษณ์อนุญาตเท่านั้น ในส่วนของข้อมูลที่ไม่สามารถเปิดเผยได้นั้น ผู้วิจัยได้ทำการเก็บไว้เป็นความลับไม่ทำการเผยแพร่ โดยหลังจากวิจัยเสร็จสิ้นข้อมูลจากการวิจัยจะถูกสรุปและส่งกลับไปเพื่อประโยชน์แก่ผู้สัมภาษณ์

ภายหลังการสัมภาษณ์ นักวิจัยได้ดำเนินการถอดเทป ตรวจสอบความถูกต้อง น่าเชื่อถือของข้อมูลโดยวิธีการตรวจสอบสามเส้าด้านข้อมูล (Data Triangulation) โดยตรวจสอบแหล่งที่มาของข้อมูลที่แตกต่างกัน ประกอบไปด้วยข้อมูลจากการศึกษาแนวคิดและทฤษฎี รวมถึงงานวิจัยที่เกี่ยวข้อง และข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกจากกลุ่มตัวอย่าง ซึ่งถ้าข้อมูลจากทุกแหล่งข้อมูลได้ข้อค้นพบเหมือนกันนั้นแสดงให้เห็นว่าข้อมูลที่ได้รับมามีความถูกต้อง น่าเชื่อถือ ซึ่งการเก็บข้อมูลจากแหล่งข้อมูลที่แตกต่างกันจะช่วยตรวจสอบความถูกต้องและน่าเชื่อถือของข้อมูลก่อนนำไปวิเคราะห์ตามกระบวนการของงานวิจัยเชิงคุณภาพ คือวิเคราะห์ถึงประเด็นสำคัญที่ได้จากการสัมภาษณ์ (Major Themes) จากนั้นนำประเด็นสำคัญมาแยกเป็นประเด็นย่อย (Sub-Themes) และหัวข้อย่อย (Categories) ซึ่งเป็นการวิเคราะห์จากภาพรวมไปจนถึงวิเคราะห์ประเด็นย่อย ใช้การวิเคราะห์แบบตีความอุปนัย (Analytics induction) กล่าวคือ เป็นการตีความสร้างข้อสรุปข้อมูลจากสิ่งที่เป็นรูปธรรมจากการเก็บรวบรวมข้อมูล โดยเป็นการพิจารณาลักษณะร่วมกันของข้อมูลที่เป็นรูปธรรมเพื่อสรุปรวมลักษณะดังกล่าวและนำเสนอผลการวิจัยด้วยวิธีการเชิงบรรยาย (Descriptive Research)

บทที่ 4

ผลการวิจัย

ผลการศึกษาวิจัยและเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างผ่านการสัมภาษณ์เชิงลึก (In-Depth Interview) ด้วยช่องทางออนไลน์และออฟไลน์ ในระหว่างเดือน ตุลาคม-พฤศจิกายน 2563 จากกลุ่มตัวอย่างทั้งหมด 20 คน ประกอบด้วยตัวอย่างกลุ่มผู้ให้ข้อมูลหลัก (Key Informants) จำนวน 8 คน และกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants) จำนวน 12 คน โดยผู้วิจัยได้สรุปข้อมูลเป็นประเด็น ดังนี้

4.1 ข้อมูลเบื้องต้นของกลุ่มตัวอย่าง

4.2 ผลกระทบของธุรกิจธนาคารพาณิชย์จากราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3 แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคล ภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.4 แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.1 ข้อมูลเบื้องต้นของกลุ่มตัวอย่าง

จากการสัมภาษณ์กลุ่มตัวอย่างผู้บริหาร ผู้ปฏิบัติงานที่เกี่ยวข้องกับการดำเนินการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของธุรกิจธนาคารพาณิชย์ และผู้เชี่ยวชาญด้านกฎหมาย หน่วยงานกำกับดูแล และผู้เชี่ยวชาญด้านการบริหารจัดการข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล ในช่วงเดือน ตุลาคม-พฤศจิกายน 2563 ประกอบด้วย

4.1.1 ข้อมูลของกลุ่มตัวอย่างผู้ให้ข้อมูลหลัก (Key Informants)

กลุ่มผู้บริหาร (Executive Management) และผู้ปฏิบัติงาน (Management/Staff) ที่เกี่ยวข้องกับการดำเนินการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของธุรกิจธนาคารพาณิชย์ จำนวน 8 คน จาก 4 บริษัท ประกอบด้วยกลุ่มผู้บริหารจำนวน 3 คน และกลุ่มผู้ปฏิบัติงานจำนวน 5 คน โดยใช้รหัส RK1-RK8 แทนชื่อกลุ่มตัวอย่าง โดยมีรายละเอียดตามตารางที่ 4.1

ตารางที่ 4.1

ข้อมูลเบื้องต้นของกลุ่มตัวอย่างผู้ให้ข้อมูลหลัก (Key Informants)

บริษัท	รหัสและตำแหน่ง	ระดับ	แผนก/ฝ่าย
A	RK1: ผู้ช่วยกรรมการผู้จัดการใหญ่*	Executive Management	Governance Office and Corporate Secretary
	RK2: หัวหน้าหน่วยงาน	Management	Operation Risk
	RK3: หัวหน้าหน่วยงาน	Management	IT Risk
	RK4: เจ้าหน้าที่อาวุโส	Staff	Compliance
B	RK5: หัวหน้าหน่วยงาน	Management	Legal
C	RK6: หัวหน้าเจ้าหน้าที่บริหาร*	Executive Management	Compliance
	RK7: รองประธานกรรมการ	Executive Management	PDPA Compliance
D	RK8: ผู้จัดการอาวุโส*	Management	Legal

*หมายเหตุ: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ของบริษัท

4.1.2 ข้อมูลของกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants)

ผู้ปฏิบัติงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานกำกับดูแลภาคธุรกิจ ผู้เชี่ยวชาญด้านบริหารข้อมูล และกลุ่มผู้เชี่ยวชาญทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล จำนวน 12 คน จาก 7 องค์กร โดยใช้รหัส RGR1-5, RGC1-4, และ RGL1-3 ตามลำดับ โดยมีรายละเอียดตามตารางที่ 4.2

ตารางที่ 4.2

ข้อมูลเบื้องต้นของกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants)

บริษัท	รหัสและตำแหน่ง	ความรู้/ความเชี่ยวชาญ	รายละเอียดการให้บริการ
A	RGR1: ผู้อำนวยการอาวุโส	กลุ่มงานกลยุทธ์และธรรมาภิบาลข้อมูล	หน่วยงานกำกับดูแลภาคธุรกิจ
	RGR2: ผู้วิเคราะห์อาวุโส		หน่วยงานกำกับดูแลภาคธุรกิจ
	RGR3: ผู้วิเคราะห์อาวุโส	ฝ่ายบริหารความเสี่ยง	หน่วยงานกำกับดูแลภาคธุรกิจ
	RGR4: ผู้วิเคราะห์อาวุโส	ฝ่ายบริหารความเสี่ยง	หน่วยงานกำกับดูแลภาคธุรกิจ
	RGR5: ผู้วิเคราะห์อาวุโส	ฝ่ายบริหารความเสี่ยง	หน่วยงานกำกับดูแลภาคธุรกิจ

ตารางที่ 4.2

ข้อมูลเบื้องต้นของกลุ่มตัวอย่างผู้ให้ข้อมูลทั่วไป (General Informants) (ต่อ)

บริษัท	รหัสและตำแหน่ง	ความรู้/ ความเชี่ยวชาญ	รายละเอียดการให้บริการ
B	RGC1: กรรมการผู้จัดการ	การบริหารข้อมูล	บริหารข้อมูลทางการตลาด
C	RGC2: กรรมการผู้จัดการ*	การบริหารข้อมูล	บริหารข้อมูลทางการตลาด
D	RGC3: ผู้อำนวยการฝ่าย	การบริหารข้อมูล	หน่วยงานบริหารข้อมูลภาครัฐ
E	RGC4: กรรมการผู้จัดการ	การบริหารข้อมูล	ศูนย์ทดสอบทักษะทางด้าน ดิจิทัลเกี่ยวกับการป้องกันข้อมูล
F	RGL1: อาจารย์	กฎหมาย	คณะนิติศาสตร์
	RGL2: อาจารย์	กฎหมาย	คณะนิติศาสตร์
G	RGL3: อาจารย์	กฎหมาย	คณะนิติศาสตร์

*หมายเหตุ: Certified GDPR Data Protection Officer

4.2 ผลกระทบของธุรกิจธนาคารพาณิชย์จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หากกล่าวถึงข้อกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถือเป็นกฎหมายฉบับแรกที่ว่าด้วยเรื่องการคุ้มครองข้อมูลเป็นการเฉพาะและใช้กับทุกภาคธุรกิจ ก่อนหน้านั้นการรับรองสิทธิเรื่องการคุ้มครองข้อมูลส่วนบุคคลกระจายอยู่ในกฎหมายที่ต่าง ๆ อย่างในภาคธุรกิจธนาคารควบคุมโดย พ.ร.บ.ธุรกิจสถาบันการเงิน พ.ศ. 2551 เป็นหลัก ประกอบกับกฎหมายอื่น ๆ เช่น พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 และแนวปฏิบัติต่าง ๆ ซึ่งการควบคุมดูแลเกี่ยวกับการคุ้มครองข้อมูลของผู้บริโภคในภาคธุรกิจธนาคารถูกควบคุมโดยหน่วยงานกำกับดูแลอย่างธนาคารแห่งประเทศไทย แต่เดิมธนาคารสามารถทำธุรกิจโดยง่ายซึ่งอาจจะไม่ได้คำนึงถึงสิทธิของผู้บริโภคมากนักต่อมาในปี 2561 ทางธนาคารแห่งประเทศไทยได้ผลักดันการกำกับดูแลเรื่องการให้บริการแก่ลูกค้าอย่างเป็นธรรม โดยออกประกาศ เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ซึ่งองค์ประกอบหนึ่งของหลักเกณฑ์มีการกำหนดถึงมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลลูกค้าซึ่งสอดคล้องกับแนวทางของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงส่งผลให้ภาคธุรกิจธนาคารมีข้อได้เปรียบจากภาคธุรกิจอื่น เนื่องจากมีการปรับใช้หลักเกณฑ์ Market Conduct มาก่อนหน้านี้ แต่ก็เป็นหลักเกณฑ์เพียงบางส่วนของ การคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. 2562 อย่างไรก็ตามหลังจากมีการประกาศใช้ พ.ร.บ. คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562 และจากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า ผลกระทบของกฎหมายสามารถจำแนกออกเป็น 2 ประเด็น คือ 1) ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562 และ 2) ผลกระทบในระดับองค์กรต่อปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กรจากการปรับใช้ พ.ร.บ. คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562

4.2.1 ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562

4.2.1.1 ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงบวก

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า กฎหมายส่งผลกระทบในเชิงบวกกับภาคธุรกิจในเรื่องการสร้างมาตรฐานการปฏิบัติงานในระดับสากล เพิ่มโอกาสในการเข้าไปแข่งขันในตลาดโลก สร้างความแข็งแกร่งของภาคธุรกิจธนาคารในมุมของความมั่นคงปลอดภัยในข้อมูลและเป็นการสร้างความเชื่อมั่นให้กับผู้บริโภคในการคัดกรองข้อมูลส่วนบุคคล เพิ่มโอกาสทางการแข่งขัน รวมถึงข้อมูลส่วนบุคคลจะมีคุณภาพมากขึ้นและเป็นการเพิ่มประสิทธิภาพในการบริหารจัดการข้อมูลของธนาคารในยุคที่ข้อมูลมีค่ามากกว่าน้ำมัน

“มีการตกลงระหว่างประเทศที่จะต้องปรับใช้มาตรฐาน เรื่อง GDPR ไม่เช่นนั้นประเทศเราก็จะทำธุรกิจกับทางต่างประเทศลำบาก ดังนั้นธุรกิจที่จะทำธุรกิจกับประเทศยุโรป คุณต้องมีมาตรการคัดกรองข้อมูลส่วนบุคคล ในระดับเดียวกับ GDPR” (Executive Management, RK1)

“มันมีกฎหมายตัวหนึ่งของยุโรป คือ GDPR ซึ่งเป็นตัวสำคัญที่ทำให้บ้านเราอยากจะทำกฎหมายตัวนี้เพราะกลัวว่าเราจะได้มาตรฐานอะไรเลย ใน GDPR หลักการที่สำคัญอันหนึ่งเลยก็คือว่าเวลาที่เขาจะโอนข้อมูลออกนอกกลุ่มประเทศยุโรปมันต้องมั่นใจว่าประเทศปลายทางมีมาตรฐานเพียงพอ” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

“มันก็เสริมสร้างความแข็งแกร่งของธนาคารด้วยในมุมของความมั่นคงปลอดภัยในข้อมูล ต่อให้ไม่มีเรื่องของ Data เข้ามา ยังไงธนาคารก็ต้องลงทุนในเรื่องของ Cyber Security อยู่แล้ว อันนี้ก็คือลงทุนเพิ่มอีกนิดหนึ่งในมุมของการรักษาความปลอดภัยของข้อมูลส่วนบุคคล” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR5)

“ธนาคารเป็นธุรกิจของการสร้างความเชื่อมั่น (Truth) ถ้าเราทำได้ดี ซึ่งเราต้องทำได้ดี เราก็มีโอกาสที่จะสร้างความเชื่อมั่นให้กับลูกค้ามากขึ้น เกิดความได้เปรียบที่เหนือกว่าพวก Non-Bank ตรงที่เขาอาจจะไม่สามารถทำได้ดีเท่าเราธนาคารน่าจะดูแลข้อมูลลูกค้าได้ดีกว่า” (Executive Management, RK1)

“ข้อมูลที่น่ามาใช้ต้องถูกต้องครบถ้วนและเป็นปัจจุบันการที่จะเอามาจัดการหรือวิเคราะห์อะไรก็ตามมันอยู่บนพื้นฐานของข้อมูลที่มีคุณภาพและคนที่ได้ประโยชน์เมื่อข้อมูลถูกต้อง คือธนาคารได้ประโยชน์แน่ ๆ เพราะว่าสามารถนำเสนอข้อมูลหรือผลิตภัณฑ์ที่ตรงใจลูกค้าพอตรงใจลูกค้าเขาได้ในสิ่งที่อยากได้ก็อาจจะกลับมาซื้อซ้ำได้อีก” (Executive Management, RK7)

“ปัจจุบัน Data Base ของบริษัทที่มีอยู่ตอนนี้เป็นข้อมูลขยะค่อนข้างเยอะเพราะว่ามันไม่เคยมีกฎหมายข้อนี้และทุกคนกลัวการส่งเมลขยะมาเยอะ ๆ แล้วก็ทำให้เมลปลอม เบอร์ปลอม เปลี่ยนเบอร์แล้วไม่ยอมอัปเดต ดังนั้นการมี PDPA จะทำให้ข้อมูลมีคุณภาพมากขึ้น สะอาดและเป็นจริงมากขึ้น เพราะคนมั่นใจในการให้ข้อมูลกับบริษัทมากขึ้นเขาเต็มใจจะให้เต็มใจจะได้รับข่าวสารจากแบรนด์ต่าง ๆ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

4.2.1.2 ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงลบ

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า พ.ร.บ. คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อภาคธุรกิจ 2 เรื่อง ประกอบด้วย 1) เกิดการสร้างมาตรฐานการคัดกรองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาด 2) การใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม โดยมีรายละเอียดเพิ่มเติม ดังนี้

(1) เกิดการสร้างมาตรฐานการคัดกรองข้อมูลส่วนบุคคลโดยบริษัทใหญ่

ในตลาด

ทางสมาคมธนาคารไทยได้ดำเนินการร่วมกันกับกลุ่มสมาชิกและที่ปรึกษาเพื่อจัดทำแนวปฏิบัติ สำหรับภาคธุรกิจธนาคาร (Industry Guideline) อย่างไรก็ตามแนวปฏิบัติของภาคธุรกิจธนาคารก็อยู่ระหว่างการนำเสนอให้หน่วยงานกำกับดูแลพิจารณาแนวทางเพื่อจะปรับใช้แนวทางดังกล่าวกับภาคธุรกิจ อย่างไรก็ตามแม้ว่าจะมีการออกแนวปฏิบัติสำหรับภาคธุรกิจ แต่ในการปฏิบัติงานจริงในภาคธุรกิจธนาคารยังไม่สามารถทำให้เกิดการปฏิบัติเป็นมาตรฐานเดียวกันทั้งอุตสาหกรรมได้ เนื่องจากแต่ละธนาคารยังพิจารณาแนวทางปฏิบัติตามกลยุทธ์และนโยบายของบริษัท ซึ่งในปัจจุบันธนาคารแบ่งออกเป็น 2 กลุ่ม ได้แก่ 1) กลุ่มที่ตีความกฎหมายอย่างเคร่งครัด (Conservative) โดยจะเน้นการขอความยินยอม (Consent) และการปฏิบัติตามสัญญา (Contract) และ 2) กลุ่มที่ตีความกฎหมายโดยยึดประโยชน์ธุรกิจเป็นหลักเน้นใช้หลักการประโยชน์อันชอบธรรม (Legitimate Interest) เป็นหลัก ซึ่งหากบริษัทใหญ่ที่มีส่วนแบ่งทางการตลาดค่อนข้างสูงเลือกปฏิบัติไปในทิศทางใดก็จะเป็นการสร้างแนวปฏิบัติให้กับอุตสาหกรรม เพราะลูกค้าโดยส่วนใหญ่ของตลาดเกิดความคาดหวังและสร้างเป็นมาตรฐานของภาคธุรกิจซึ่งจะมีการเรียกร้องมาตรฐานตามการให้บริการของบริษัทใหญ่ซึ่งอาจเป็นภาระกับบริษัทขนาดกลางและขนาดเล็กในตลาด

“เมื่อมันกำหนดกติการ่วมกันไม่ได้ แนวปฏิบัติตัวนี้ถ้ามันไม่กลายเป็น เอกฉันท์ขึ้นมา ทุกคนไม่ได้ปฏิบัติเหมือนกัน มันมีคนปฏิบัติที่มากกว่า และมีคนปฏิบัติที่น้อยกว่า คนที่ได้รับสารไปคือผู้บริโภคก็คงงวามมาตรฐานมันอยู่ตรงไหนและจะเรียกร้องเอามาตรฐานตามคนที่ Conservative กว่าซึ่งก็จะเป็นปัญหาหลักเหมือนกัน โดยเฉพาะถ้าธนาคารที่ Conservative กว่า เป็นธนาคารที่ใหญ่ซึ่งมีส่วนแบ่งการตลาดเยอะ การสร้างแนวปฏิบัติก็แทบจะไม่มีประโยชน์ เพราะว่า ธนาคารใหญ่เขาได้สร้างมาตรฐานของเขามาแล้ว มันจะกลายเป็น Norm Over Market ไม่ใช่ Market Norm” (Executive Management, RK6)

“ธนาคารแบ่งเป็นสองค่าย ค่ายที่ Conservative เน้นสัญญา กับ การขอ ความยินยอม (Consent) เป็นหลักตรงไปตรงมาถ้าลูกค้ายินยอมคือไปต่อได้ ถ้าไม่ก็อย่าไปยุ่งกับ ลูกค้า ส่วนค่ายที่ใช้อีกฐานหนึ่งก็คือ Legitimate Interest ก็จะไม่บอกว่าถ้าเป็นสิ่งที่ทำแล้วธนาคารได้ ประโยชน์ Third party ได้ประโยชน์ ลูกค้าอาจจะได้รับผลกระทบไม่เยอะก็ไปใช้ Legitimate Interest ก็จะเป็นสองค่ายที่ยังเป็นคู่ขนานกันไปแบบนี้” (Executive Management, RK7)

(2) การใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า กฎหมายได้ให้การคุ้มครองข้อมูล ส่วนบุคคลและสิทธิของเจ้าของข้อมูลค่อนข้างมากซึ่งหากหน่วยงานกำกับตีความกฎหมายอย่าง เคร่งครัด ประกอบกับความรู้ความเข้าใจเกี่ยวกับกฎหมายและการคุ้มครองข้อมูลส่วนบุคคลของคน ไทยยังไม่เป็นที่แพร่หลายมากนัก จึงอาจทำให้เกิดการใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสมและเป็น ภาระแก่ภาคธนาคาร เช่น ลูกค้าต้องการให้ลบข้อมูลส่วนบุคคลโดยที่ไม่ทราบว่าการธนาคารสามารถเก็บ ข้อมูลส่วนบุคคลของลูกค้าได้บนฐานกฎหมายอื่น เกิดความเข้าใจที่ไม่ตรงกันกับธนาคารและเกิดการ ฟ้องร้อง ซึ่งทำให้ธนาคารต้องเสียเวลาในการตรวจสอบและจัดการกับข้อร้องเรียนต่าง ๆ ที่เกิดจาก ความไม่เข้าใจกฎหมายของลูกค้า หรือแม้กระทั่งหากเกิดกรณีลูกค้าเกิดความวิตกกังวลกับการแจ้ง เหตุข้อมูลรั่วไหล (Data Breach) ซึ่งหากหน่วยงานกำกับกำหนดเนื้อหาในการแจ้งที่ทำให้เกิดความ ตื่นตระหนกแก่ผู้บริโภคอาจเกิดเหตุการณ์ที่ผู้บริโภคระดมกันขอถอนความยินยอม ซึ่งทำให้ภาคธุรกิจ จะไม่มีข้อมูลลูกค้า เป็นต้น

“สิทธิต่าง ๆ ของผู้บริโภคที่มันมากขึ้นอาจจะมากเกินไปเสียด้วยซ้ำ ถ้า ตีความกันเข้ม ๆ กฎหมายนี้มันทำให้ประเทศไทยมันไม่พัฒนาเราเป็นประเทศไม่พัฒนาแต่เราเอา กฎหมายที่พัฒนาแล้วมาใช้ ถ้าเราเจอคนที่ตีความแบบเข้มมาก ๆ เราก็จะพัฒนาไม่ได้” (Management, RK8)

“แล้วถ้าเกิดว่ามันมีความพิกลพิการในความคิดของลูกค้าขึ้นมาแล้วเขา จะแหกกันถอนความยินยอม (Consent) โดยที่เขาไม่รู้ว่าจะผลที่ตามมาคืออะไร กลายเป็นว่าประเทศ เราไม่มีข้อมูลเลยนะ” (Management, RK8)

“ผู้บริโภคมิได้เข้าใจ PDPA ว่ามันมีเกณฑ์พิจารณาตัวหนึ่งที่ชื่อว่า *Legitimate Interest* ก็ไม่ต้องขอความยินยอม (*Consent*) เกิดความเข้าใจที่ขัดแย้งกันแล้ว ถ้าสมมติว่าหน่วยงานกำกับดูแลแล้วบอกว่าผู้บริโภคถูก มันจะกลายเป็นอุปสรรค เพราะเราที่เราทำการตลาดทำธุรกิจทั้งหมด เราไม่ได้ออกแบบมาเพื่อใครคนใดคนหนึ่งถ้ามีคนใดคนหนึ่งไม่ให้ความยินยอมขึ้นมา เราไม่สามารถใช้ข้อมูลของเขาไปทำอะไรได้หรือออกแบบผลิตภัณฑ์ให้กับเขาได้ วันที่มีความรู้สึกว่าเขาได้รับการให้บริการไม่เท่ากับคนที่ให้ความยินยอมเขาจะเริ่มโวยวายแล้ว” (Executive Management, RK6)

“คำว่าคุ้มครองไม่ได้แปลว่าสปอยล์ ทำอย่างไรให้ลูกค้ารู้ว่ามันมีกติกาหนึ่งที่เรารัดดลินใจร่วมกัน ไม่ใช่อะไรก็ฟ้อง วันหนึ่งต้องมานั่งรับเรื่องลูกค้าฟ้องร้องเรื่องที่เขาคิดว่าละเมิดข้อมูลส่วนบุคคลแต่จริง ๆ แล้วไม่ใช่ ผู้ประกอบการคงไม่ต้องการ วัน ๆ มานั่งทำเรื่องพวกนี้มันค่อนข้างจะเป็นต้นทุน” (Executive Management, RK6)

“อุปสรรคสำคัญของเรื่องข้อกำหนดเกี่ยวกับความชัดเจนว่าบริบทอะไรที่ต้องแจ้งข้อมูลรั่วไหลเราต้องแจ้งทุกเรื่องใหม่ เนื้อหาที่สมควรควรจะเป็นแบบไหนสร้างสรรค์หรือจะสร้างความหวาดกลัวให้กับตลาด ถ้าอิงตาม GDPR ค่อนข้างจะใช้ข้อความที่น่าจะตื่นตระหนก เกิดความวิตกกังวลที่มากเกินไป เกิดความหวาดระแวงขึ้นในตลาดสิ่งที่ตามมาคือลูกค้าเดินหน้าฟ้องผู้ประกอบการกระจายเลย ทั้ง ๆ ที่แจ้งตามที่หน่วยงานกำกับกำหนดไว้เรียบร้อยแล้วแต่กลายเป็นว่าผู้บริโภคมิชอบตรงนี้กลับมาฟ้องผู้ประกอบการ” (Executive Management, RK6)

นอกจากนี้ยังรวมไปถึงกลุ่มเจ้าของข้อมูลที่ไม่ประสงค์กับธนาคารใช้กฎหมายเป็นเครื่องมือในการโจมตีธนาคาร หลังจากที่มีการประกาศใช้กฎหมายกลุ่มธุรกิจธนาคารเริ่มมีกลุ่มคนที่มีพฤติกรรมสุ่มเสี่ยงที่ทำให้เกิดความเสียหายต่อการถูกฟ้องร้อง เช่น การส่งอีเมลเข้ามาแจ้งข้อมูลส่วนบุคคลกับธนาคารโดยไม่ได้เป็นลูกค้าหรือเข้ามาขอใช้สิทธิลบข้อมูลส่วนบุคคลโดยที่ธนาคารไม่มีข้อมูล เนื่องจากกฎหมายมีการกำหนดทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองที่ค่อนข้างหนัก กลุ่มคนเหล่านี้อาจจะใช้ข้อมูลส่วนบุคคลเป็นเครื่องมือในการโจมตีธนาคารเพื่อเรียกเงินตอบแทน รวมถึงเป็นเป้าหมายของอาชญากรไซเบอร์ (Hacker) ในการเรียกค่าไถ่เพิ่มขึ้นอีกด้วย

“เริ่มมีคนเข้ามาขอใช้สิทธิแต่ไม่ใช่ลูกค้าเข้ามาขอใช้สิทธิว่าให้ลบข้อมูลด้วยบริษัทก็ต้องมานั่งคิดว่าจะไปลบอะไร ในเมื่อไม่มีอะไรเลย ซึ่งเขาเขียนมาผ่านช่องทางการติดต่อเจ้าหน้าที่คุ้มครองส่วนบุคคล (DPO) ให้ข้อมูลมาจัดเต็มมาก” (Executive Management, RK7)

“ไม่ว่าจะเป็นลูกค้าหรือไม่แต่ไม่น่าใช่ หรืออาจเป็นนักศึกษา หรือคนที่ทำหน้าที่ NGO หรือถ้าเลวร้ายหน่อยก็อาจจะจะเป็นพวกที่พยายามมาเรียกค่าไถ่ (Ransom) เจตตั้งแต่ส่งชื่อส่งนามสกุลมาทั้งไว้ทางอีเมลแล้วก็ไม่ทำอะไร ก็ยังคิดไม่ออกว่าส่งมาทำไมแต่เรามองในภาพที่ว่า

มีข้อพวกนี้อยู่ในถึงข้อมูลเราแล้ว เราต้องประมวลผลว่าเราเก็บในฐานอะไร ถ้าเราไม่ระวังมันอาจจะเกิดผลที่ตามมาได้ มีประเภทเขียนเข้ามาเพื่อถามนั่นถามนี่เต็มไปหมด แต่จริง ๆ เราตรวจสอบแล้วไม่ใช่ลูกค้า มันกลายเป็นดาบอีกเล่มหนึ่งที่มาทำร้ายผู้ประกอบการ จริง ๆ” (Management, RK8)

“ธนาคารไหนกล้าบอกมัยว่าธนาคารเขาระบบความปลอดภัยข้อมูลดี ที่สุดไม่มีใครกล้าพูดและไม่ควรพูดด้วยมันเป็นการเรียกแขกแฮคเกอร์มาแน่” (Staff, RK4)

“ในต่างประเทศมันก็มีกลุ่มคนที่หาเงินกับเรื่องนี้โดยเฉพาะ มันจะมีกลุ่มคนที่หารูรั่วเพื่อจับให้ได้ เราก็ไม่รู้ว่บ้านเราจะมีมัย” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

4.2.2 ผลกระทบในระดับองค์กรจากการปรับใช้ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล พ.ศ. 2562

จากการสัมภาษณ์กลุ่มตัวอย่างและกรอบแนวคิดการวิจัย พบว่า จากการปรับใช้พระราชบัญญัติคຸ່ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบตຸ່งองค์กรภาคธุรกิจธนาคารพาณิชย์ทั้งปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กร โดยมีรายละเอียด ดังนี้

4.2.2.1 ผลกระทบตຸ່งปัจจัยสภาพแวดล้อมภายในองค์กร

(1) ผลกระทบตຸ່งโครงสร้างองค์กร

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า มีการแต่งตั้งเจ้าหน้าที่คຸ່ມครองข้อมูลส่วนบุคคล (Data Protection Office: DPO) เพื่อปฏิบัติหน้าที่ตามที่กฎหมายกำหนดและรายงานการดำเนินงานที่เกี่ยวกับหน้าที่ความรับผิดชอบในบทบาทของ DPO ตຸ່งผู้มีอำนาจสูงสุดขององค์กร และจัดให้มีทีมงานสนับสนุนการปฏิบัติงานของ DPO โดยผู้ที่ได้รับการแต่งตั้งเป็น DPO มาจากบุคลากรภายในองค์กรที่สังกัดอยู่ภายใต้ส่วนงานต่าง ๆ ที่เกี่ยวข้องกับการปรับใช้และควบคุมการปฏิบัติตามกฎหมาย เช่น ส่วนงานกำกับดูแลกิจการ ส่วนงานกฎหมาย เป็นต้น ซึ่งมีทั้งไม่แยกโครงสร้างส่วนงาน DPO ขึ้นมาใหม่อยู่ภายใต้สังกัดเดิมและแยกโครงสร้างส่วนงาน DPO ออกมาเป็นอีกหนึ่งส่วนงานเพื่อบริหารจัดการด้านข้อมูลโดยเฉพาะ

“เรามีการแต่งตั้งให้ Head of Compliance เป็น DPO” (Executive Management, RK1)

“มีการเพิ่มตำแหน่ง DPO ขึ้นมาโดย DPO เป็น Function ที่ตั้งขึ้นมาต่างหากแต่ถ้าถามว่า ณ วันนี้ DPO คือใคร ก็คือ Head of Compliance มาดูแลแทนก่อนใน Function นี้ก็อยู่ภายใต้ Governance Office และรายงานตรงผู้มีอำนาจสูงสุด” (Staff, RK4)

“มีการปรับโครงสร้างองค์กรโดยมีการแต่งตั้ง DPO และมีการตั้งทีม PDPA” (Executive Management, RK7)

“DPO เป็นตำแหน่งใหม่ ในบริษัทใหญ่ ๆ DPO มันไม่ใช่แค่ตำแหน่ง 1 ตำแหน่งมันกำลังพูดถึงโครงสร้างขององค์กรที่จำเป็นต้องมีตำแหน่งหนึ่งที่ทำหน้าที่ประสานงานกับ

คนทั้งหมดในเรื่องนี้มันต้องมีแผนหนึ่งขึ้นมาแล้วหัวหน้าของแผนนี้เรียกว่า DPO พุดง่าย ๆ เลย DPO ควรเป็น C level คือ เท่ากับ CFO CMO อย่างพวกธนาคารสามารถใช้โครงสร้างนี้ได้” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC4)

“DPO ควรจะมีแยกออกมาเป็นหน่วยงานหนึ่งอยู่ภายใต้ Data Governance ทั้งหมดแต่ไม่ควรจะไปแยกว่าเป็นข้อมูลส่วนบุคคลหรือไม่ใช่ข้อมูลส่วนบุคคล แล้วถ้าเป็นเรื่องของข้อมูลส่วนบุคคล DPO ก็รับไป” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR1)

(2) ผลกระทบต่อกลยุทธ์และนโยบายบริษัท

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า กลยุทธ์ของธนาคารพาณิชย์ มุ่งเน้นการปฏิบัติตามกฎหมายโดยให้ความสำคัญกับเรื่องกระบวนการควบคุม การรักษาความปลอดภัยของข้อมูลส่วนบุคคลมากขึ้น และมีความระมัดระวังเป็นพิเศษหรือเลือกที่จะไม่ปฏิบัติในกระบวนการที่มีความเสี่ยงสูง รวมถึงธุรกิจใดที่มีความเสี่ยงที่จะขัดต่อกฎหมายก็ต้องมาพิจารณาและหาวิธีจัดการกับความเสี่ยงนั้น โดยการตัดสินใจเชิงกลยุทธ์ทั้งหมดอยู่บนพื้นฐานของการหาสมดุลระหว่างผลประโยชน์ของลูกค้าและการปฏิบัติตามกฎหมายกับการดำเนินธุรกิจที่ไม่ได้รับผลกระทบมากเกินไป ซึ่งในกลุ่มของธนาคารพาณิชย์สามารถแบ่งกลุ่มของธนาคารออกเป็น 2 กลุ่มกลยุทธ์ตามมุมมองการตีความทางด้านกฎหมายของแต่ละธนาคาร ได้แก่ 1) กลุ่มที่ตีความกฎหมายอย่างเคร่งครัด (Conservative) โดยจะเน้นการขอความยินยอม (Consent) และการปฏิบัติตามสัญญา (Contract) 2) กลุ่มที่ตีความโดยมุ่งเน้นการดำเนินธุรกิจเป็นหลักเน้นใช้หลักการประโยชน์อันชอบธรรม (Legitimate Interest)

“ในแง่ของกลยุทธ์องค์กรก็เน้นเรื่องการควบคุมเรื่องของ Security เรียกว่าระมัดระวังมากขึ้น หรืออะไรบางอย่างที่มีความเสี่ยงสูงมาก ๆ ก็จะไม่ทำ มีการระมัดระวังเรื่องนี้เป็นพิเศษ ธุรกิจไหนที่มีความเสี่ยงที่จะขัดต่อกฎหมายสูงมาก ๆ ก็ต้องมาทบทวนแต่โดยส่วนใหญ่มันจัดการความเสี่ยงได้” (Executive Management, RK1)

“กลยุทธ์เราไปในแนวทางผลประโยชน์ของลูกค้า ในขณะที่เดียวกันเราก็ต้องทำให้ได้เต็มที่ ฝ่ายกฎหมายก็ไม่ได้ตีความตามตัวอักษร เราก็ต้องพยายามอย่างเต็มที่เพื่อไม่ให้ผิดกฎหมายและไม่ให้กระทบวิถีของธนาคารจนเกินไปจนไม่สามารถทำธุรกิจได้” (Management, RK5)

“ธนาคารแบ่งเป็นสองค่าย ค่ายที่ Conservative เน้นสัญญากับการขอความยินยอม (Consent) เป็นหลัก ส่วนอีกค่ายที่ใช้ฐาน Legitimate Interest ก็จะบอกว่าถ้าเป็นสิ่งที่ทำแล้วธนาคารได้ประโยชน์ Third party ได้ประโยชน์ ลูกค้าอาจจะได้รับผลกระทบไม่เยอะก็ไปใช้ Legitimate Interest ก็จะมีเป็นสองค่ายที่ยังเป็นคู่ขนานกันไปแบบนี้” (Executive Management, RK7)

ด้านนโยบายธนาคารได้ปรับปรุงนโยบายเดิมที่มีอยู่แล้วในองค์กรให้สอดคล้องกับเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล เพิ่มกระบวนการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเข้าไปในกระบวนการปฏิบัติงาน พิจารณาปรับปรุงนโยบายให้มีประสิทธิภาพในการควบคุมมากขึ้น พร้อมทั้งกำหนดบทลงโทษสำหรับบุคลากรในองค์กรที่กระทำผิด นอกจากนี้ยังมีการเพิ่มเติมในส่วนของการคุ้มครองข้อมูลส่วนบุคคลเข้าไปในนโยบายธรรมาภิบาลข้อมูล (Data Governance Policies) และการออกประกาศนโยบายใหม่สำหรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของบริษัทโดยเฉพาะพร้อมจัดทำนโยบายความเป็นส่วนตัว (Privacy Policy)

“เราปรับ Policy Guideline โดยเอาเรื่องการคุ้มครองข้อมูลส่วนบุคคลเข้ามาอยู่ในกระบวนการ” (Management, RK3)

“แต่เดิมเรื่องการรักษาความลับของข้อมูลลูกค้าเป็นนโยบายสำคัญของธนาคารอยู่แล้วพอมี PDPA เข้ามาเรื่องของ Action ต่าง ๆ มันเข้มข้นขึ้น เรื่องกระบวนการต่าง ๆ มาตรการต่าง ๆ ที่มันจำเป็นต้องมีก็มีความชัดเจนขึ้น เราก็ต้องมาคิดต่อมาปรับปรุงว่าเราจะทำไงให้มันรองรับตัวกฎหมายที่มันชัดเจนขึ้นตรงนี้” (Staff, RK4)

“เรื่องของข้อมูลมันมีมานานแล้วเพียงแต่ว่ามันอยู่กระจัดกระจายอยู่แล้วแต่ว่าอยู่ที่นโยบายในเรื่องไหน แต่ในส่วนของ PDPA ก็จะมีจะมีนโยบายอีก 1 เล่มที่บอกว่าในการที่จะปฏิบัติตามกฎหมาย PDPA จะต้องทำดังต่อไปนี้” (Executive Management, RK7)

“เรื่องของช่องทางออนไลน์อย่างเว็บไซต์มี Cookie Policy ใช่มั้ยถ้ามีแล้ว Cookie Policy มันครอบคลุมตามกฎหมายหรือไม่ก็ต้องไปทบทวนปรับปรุงดู” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

(3) ผลกระทบต่อกระบวนการปฏิบัติงาน

ในภาคธุรกิจธนาคารพาณิชย์ได้รับผลกระทบจากการปรับใช้ พ.ร.บ. ข้อมูลส่วนบุคคล พ.ศ. 2562 โดยส่งผลกระทบต่อการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลทั้งภายในและภายนอกองค์กร โดยจากผลการสัมภาษณ์กลุ่มตัวอย่างสามารถสรุปได้ว่าบริษัทมีการเปลี่ยนแปลงในกระบวนการปฏิบัติงานต่าง ๆ ทั่วทั้งองค์กรเพื่อให้การปฏิบัติงานเป็นไปตามกฎหมายซึ่งแบ่ง 2 ส่วน คือ 1) การปรับปรุงกระบวนการปฏิบัติงานเดิม 2) การเพิ่มกระบวนการปฏิบัติงานใหม่

1. การปรับปรุงกระบวนการปฏิบัติงานเดิม

กระบวนการทั้งภายในและภายนอกองค์กรจะถูกทบทวนทุกกระบวนการที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลเพื่อให้บริษัทมั่นใจได้ว่าทุกกระบวนการที่เกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดของกฎหมาย ข้อมูลถูกเก็บรวบรวมอย่างถูกต้องตามฐานการประมวลผลข้อมูล มีการใช้ข้อมูลอย่างถูกต้อง โปร่งใสเป็นไปตามวัตถุประสงค์ และมีการเปิดเผยข้อมูลตามที่กฎหมายกำหนดพร้อมทั้งมีกระบวนการรักษาความปลอดภัยข้อมูลที่เป็นมาตรฐาน มีการ

ออกแบบการควบคุมที่เหมาะสมตามความเสี่ยงของข้อมูลที่จะส่งผลกระทบต่อเสรีภาพของบุคคล ออกแบบการให้บริการและการสื่อสารกับลูกค้าอีกทั้งยังมีการปรับปรุงกระบวนการทางการตลาด กระบวนการจัดจ้าง และเพิ่มขอบเขตการตรวจสอบในกระบวนการตรวจสอบ โดยมีรายละเอียดดังนี้

ตารางที่ 4.3

สรุปการปรับปรุงกระบวนการปฏิบัติงานเดิม

กระบวนการ	การปรับปรุงและเปลี่ยนแปลงที่เกิดขึ้นในกระบวนการ
1. กระบวนการจัดการข้อมูล (เก็บรวบรวม ใช้และเปิดเผยข้อมูล)	- ต้อง Walk Trough กระบวนการปฏิบัติการใหม่ทั้งหมด และมีการจัดทำทะเบียนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROP) เพื่อให้ทราบว่าข้อมูลใดควรเก็บหรือลบ กระบวนการใดที่ขัดต่อกฎหมายต้องมีการปรับเปลี่ยนเพื่อให้เป็นไปตามกฎหมาย และ ปรับปรุงกระบวนการไหลของข้อมูล (Data Flow) - การเก็บรวบรวมข้อมูลจากเดิมสามารถเก็บ ใช้ และเปิดเผยข้อมูลได้อย่างเสรีแต่ปัจจุบันต้องระบุนานกฎหมายในการจัดเก็บ ใช้และเปิดเผยข้อมูลได้ หากไม่สามารถระบุได้จะมีการปรับเปลี่ยนกระบวนการอย่างไรให้สามารถทำได้ ซึ่งหากเป็นการปฏิบัติงานตามการให้บริการปกติของธนาคารข้อมูลส่วนบุคคลจะถูกเก็บตามฐานสัญญา (Contract) ยกเว้นการเก็บข้อมูลเพื่อใช้ในการตลาดที่จะเป็นฐานความยินยอม (Consent) ซึ่งต้องมีการขอความยินยอมจากเจ้าของข้อมูล แต่อย่างไรก็ตามเรื่องการขอความยินยอมจากลูกค้าธนาคารมี Market Conduct ซึ่งเป็นข้อกำหนดจากรบพ. ถือปฏิบัติมาก่อนหน้านี้แล้วอาจจะไม่มีผลกระทบมากนัก - ต้องมีการปรับปรุงเอกสารสัญญาและแบบฟอร์มต่าง ๆ ให้เป็นไปตามข้อกำหนดของกฎหมาย เช่น สัญญาจ้างพนักงาน สัญญาการให้บริการลูกค้า และสัญญาจ้างงานผู้รับเหมา เป็นต้น - ต้องวางแผนการใช้ข้อมูลส่วนบุคคลให้เกิดประโยชน์อย่างสูงสุดจากการเก็บข้อมูลส่วนบุคคลให้น้อยที่สุด

ตารางที่ 4.3

สรุปการปรับปรุงกระบวนการปฏิบัติงานเดิม (ต่อ)

กระบวนการ	การปรับปรุงและเปลี่ยนแปลงที่เกิดขึ้นในกระบวนการ
2. กระบวนการรักษาความปลอดภัยข้อมูล	- แต่เดิมธนาคารมีการให้ความสำคัญในเรื่องของการรักษาความปลอดภัยของข้อมูลลูกค้าอยู่แล้ว เพียงแต่ต้องเพิ่มความเข้มข้นมากขึ้นทำการวิเคราะห์ Gap Analysis เพื่อเพิ่มเติมมาตรฐานการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้ได้มาตรฐานมากขึ้น เช่น มีการกำหนดสิทธิการเข้าถึงข้อมูลตามการใช้งาน การใส่รหัสรักษาความปลอดภัยต่าง ๆ เช่น รหัสคอมพิวเตอร์ โน้ตบุ๊ก ไฟล์เอกสาร กำหนดสิทธิในการส่งออกข้อมูลไปยังบุคคลที่ 3 ต้องมีการกำหนดอำนาจในการอนุมัติ เป็นต้น
3. กระบวนการควบคุม	- ออกแบบกระบวนการควบคุมการปฏิบัติงานให้มีการคุ้มครองข้อมูลเป็นไปตามที่แนวทางที่บริษัทกำหนด และมีการปรับปรุงบทลงโทษและบังคับใช้สำหรับการกระทำผิดเกี่ยวกับเรื่องดังกล่าวให้เข้มข้นขึ้น
4. กระบวนการสื่อสารภายในองค์กร	- กระบวนการสื่อสารภายในองค์กรต้องเพิ่มเรื่องของการให้ความรู้เกี่ยวกับกฎหมาย และสร้างการตระหนักรู้เกี่ยวกับการใช้ข้อมูลส่วนบุคคลรวมถึงวิธีการทำงานที่มีการปรับเปลี่ยนไป ผ่านการฝึกอบรม การทำ Workshop และช่องทางการสื่อสารต่าง ๆ ขององค์กร
5. กระบวนการให้บริการและการสื่อสารกับลูกค้า	- ปรับปรุงกระบวนการการให้บริการลูกค้าซึ่งต้องเพิ่มกระบวนการขอความยินยอมลูกค้า (Consent) ต้องการปรับปรุงบทพูด (Script) การสื่อสารกับลูกค้าให้เหมาะสม และกระบวนการติดต่อกับลูกค้าจะถูกเปลี่ยนมาเป็นดิจิทัลมากขึ้น - ต้องมีการสื่อสารประชาสัมพันธ์ข้อมูลเกี่ยวกับความรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าตระหนักและทราบถึงประโยชน์ของกฎหมายฉบับนี้ ในทุกช่องทางการสื่อสาร และปรับช่องทางการสื่อสารให้สามารถเข้าถึงได้ง่ายทุกกลุ่มลูกค้าและเป็นเนื้อหาที่สามารถเข้าใจได้ง่ายเหมาะกับกลุ่มลูกค้า

ตารางที่ 4.3

สรุปการปรับปรุงกระบวนการปฏิบัติงานเดิม (ต่อ)

กระบวนการ	การปรับปรุงและเปลี่ยนแปลงที่เกิดขึ้นในกระบวนการ
6. กระบวนการทางการตลาด	- ต้องปรับกระบวนการใช้ข้อมูลลูกค้าในการทำกิจกรรมทางการตลาดที่ระมัดระวังมากขึ้น คัดกรองมากขึ้น และต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งต่อลูกค้า - ปรับกลยุทธ์ กระบวนการทำงานออกแบบการขอความยินยอม (Consent) ทั้งเนื้อหาและรูปแบบที่สามารถจูงใจลูกค้าในการให้ความยินยอมกับบริษัทมากที่สุด
7. กระบวนการจัดจ้าง	- ปรับเกณฑ์การพิจารณาคัดเลือกผู้รับเหมารายใหม่และต่ออายุรายเก่าโดยเพิ่มเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล - ปรับสัญญาการให้บริหารระหว่างผู้รับเหมารายเดิมที่เกี่ยวข้องการใช้ข้อมูลส่วนบุคคลเป็นสัญญาประมวลผล - หากเป็น Outsource ที่เป็นตลาดผูกขาดหรือเป็นรายใหญ่อำนาจในการต่อเรื่องมาตรฐานการบริการก็เป็นไปได้ยาก ซึ่งอาจจะเพิ่มความเสี่ยงให้กับองค์กรได้จึงอาจจะพิจารณาเรื่องกระบวนการบริหารจัดการความเสี่ยงเพิ่มเติม
8. กระบวนการตรวจสอบ	- หน่วยงานตรวจสอบภายใน (Internal Audit/IT Audit) จะเพิ่มขอบเขตการตรวจสอบโดยต้องวางแผนและออกแบบการตรวจสอบเกี่ยวกับกระบวนการคุ้มครองข้อมูลส่วนบุคคลเพิ่มขึ้น - ส่วนงานกำกับดูแลกิจการ (Compliance) ต้องเข้าตรวจสอบการปฏิบัติงานของพนักงานภายในบริษัทว่ามีการปฏิบัติตามระเบียบนโยบายที่บริษัทกำหนดหรือไม่ - ทีมบริการข้อมูล (Data Steward Council) ปรับปรุงกระบวนการปฏิบัติงานการตรวจสอบโดยเพิ่มเรื่องของการใช้ข้อมูลส่วนบุคคลซึ่งจะประสานงานร่วมกับ DPO - มีการจัดตั้งทีมงานอาสาสมัครลับ (Spy) เพื่อช่วยกันตรวจสอบการปฏิบัติตามระเบียบนโยบายที่บริษัทกำหนดเกี่ยวกับข้อมูลส่วนบุคคล

“การได้มาซึ่งข้อมูลของลูกค้าได้มาในฐานใดของกฎหมาย เป็นไปตามกฎหมายกำหนดมัย ถ้าไม่ได้เราจะปรับเปลี่ยนมันอย่างไรบ้าง รวมถึงกระบวนการจัดเก็บข้อมูลต่าง ๆ แต่เดิมในแต่ละ Business เก็บข้อมูลกันกระจัดกระจาย ไม่เคยรู้เลยว่าเขาเก็บข้อมูลอะไรบ้าง แต่พอกฎหมายออกมาเราต้องรู้ว่าเรามีข้อมูลส่วนบุคคลเก็บไว้ที่จุดไหนบ้าง มันก็ต้องปรับ Process ต้องทำทะเบียนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROP) ในแต่ละจุดว่ามีใครบ้าง อย่างไรบ้าง” (Management, RK3)

“มีกระบวนการทำงานที่เพิ่มมากขึ้นได้ อย่างเช่น เรื่องการขอความยินยอมเดิมก็มีประกาศออกมาแล้วเรื่อง Market Conduct ธนาการก็อาจจะคุ้นเคย ในระดับหนึ่งอยู่แล้ว แต่ว่าเพิ่มในเรื่องของการแจ้งประกาศความเป็นส่วนตัว (Privacy Notice)” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR5)

“ถ้าเกิดว่ามันมีอะไรที่ต้องปรับปรุงโดยกฎหมายก็จะทำให้ Data Flow มันเปลี่ยน ใน General Banking คิดว่าไม่ได้เปลี่ยนเยอะขนาดนั้นในส่วนที่เป็น กิจกรรมการให้บริการแต่ส่วนที่จะเปลี่ยนเยอะคือส่วนการตลาดส่วนที่เอาข้อมูลไปทำอย่างอื่นซึ่งต้องขอความยินยอม (Consent) อันนี้มันจะเป็นความยาก” (ผู้เชี่ยวชาญกฎหมาย, RGL2)

“ใช้ข้อมูลน้อยที่สุดแต่เกิดประสิทธิภาพมากที่สุดจะต้องทำไง เพราะฉะนั้นการที่จะรู้ว่าต้องใช้ข้อมูลอะไรเราก็คิดมาแล้วทำการบ้านมาแล้วว่าต้องการอะไร ไปทำอะไร ข้อมูลมันเหมือนวัตถุดิบในการทำอาหาร เหมือนเอามาปรุงออกเป็นเมนูใหม่ๆ ได้ เช่น อายุ เพศ Location รวมกัน สามารถแตกข้อมูลไปในมุมต่าง ๆ ได้” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“การเปิดบัญชีใหม่จะมีค่าขอเปิดบัญชี คราวนี้จะเพิ่มมากับหนังสือขอความยินยอม (Contract Application Form) โปะไปคู่กันแต่ถ้าลูกค้าไม่เซ็นก็ไม่ใช่ไรนี่แหละเป็นกระบวนการที่เพิ่มขึ้นจากเดิม Contract Application Form ก็พอ จริง ๆ ต้องใช้วาทศิลป์ของสาขาเพราะว่าถ้ามีของใหม่มาให้ทำลูกค้าก็จะงงว่าจะมาทำธุรกรรม ก แต่ได้ทำ ข ด้วยเขาก็จะงง ๆ เราก็ต้องสื่อสารให้เข้าใจ จะถ่ายทอดให้ลูกค้าอย่างไรให้ลูกค้าเห็นว่ามันเป็นประโยชน์” (Executive Management, RK7)

“การปฏิสัมพันธ์กับลูกค้ามันจะเป็นดิจิทัลมากขึ้นอาจจะไม่ใช่คนอย่างเดียวอาจจะเป็นระบบ (System) ด้วย” (ผู้เชี่ยวชาญกฎหมาย, RGL2)

“เรามีการจัดอบรมเกือบทุกระดับในองค์กรตั้งแต่ บอร์ด ผู้บริหาร พนักงาน ในบางระดับก็จะเป็นทางสื่อคอมพิวเตอร์ การเรียนออนไลน์ มีการพูดซ้ำแล้วซ้ำอีก ย้ำแล้วย้ำอีก มีการเรียกประชุมคุยกัน ก็เล่าเรื่องเดิม จนเข้าใจจากเข้าใจก็เริ่มซีเรียส เราให้ความสำคัญกับเรื่องพวกนี้ เรามีการสื่อสารทุกระดับจริง ๆ ตัวเนื้อหาที่ให้ตรงตามแต่ละส่วนงานที่เขาทำงาน” (Executive Management, RK1)

“มุมมองตลาดถ้าได้ข้อมูลมาแล้วคนที่จะทำแคมเปญในลักษณะนี้ได้จะต้องเป็นคนที่ให้ความยินยอม (Consent) เท่านั้นมันก็จะเพิ่มกระบวนการคัดกรองมากขึ้น” (Executive Management, RK7)

“นักการตลาดจะออกแบบการขอการขอความยินยอม (Consent) ยังไงให้ไม่กระทบกับกระบวนการทำงานทั้งหมดให้ได้ นั่นคือสิ่งที่ต้องไปนั่งแก้กัน” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“เราก็ต้องการทำสัญญาประมวลผลข้อมูลเพิ่มเติมในกรณีที่เราเป็น Outsource รายเดิมส่วนรายใหม่ ๆ เราก็พิจารณาว่าเรามีมาตรการในการควบคุมดูแลข้อมูลส่วนบุคคลของเราเพียงพอ เป็นไปตามกฎหมาย รวมไปถึงการทบทวนคุณสมบัติของผู้รับเหมาที่จะมีการเอาเรื่องของ PDPA มาพิจารณาเพิ่มด้วยก็คือเอาเข้ามาพิจารณาร่วมด้วยทั้งเรื่องของการจ้างรายใหม่ และต่ออายุรายเก่า” (Staff, RK4)

“มีการสื่อสารว่าแผนของ PDPA เรามีการควบคุมอะไรบ้าง Internal Audit จะรับทราบแล้วเขาก็จะออกแบบการตรวจสอบและมีการรายงานความคืบหน้าคณะกรรมการตรวจสอบอยู่เรื่อย ๆ” (Executive Management, RK7)

“เรามีทีมบริหารข้อมูล (Data Steward Council) ในเรื่องของการใช้ข้อมูลด้วย เราก็มาดูว่าข้อมูลที่เอาไปใช้ต่าง ๆ มันมีฐานกฎหมายรองรับหรือไม่เพื่อให้ข้อมูลมันใช้อย่างถูกต้องตามกฎหมายแล้วทำให้เกิดประโยชน์สูงสุดกับองค์กรแยกจากทีม DPO เลย” (Management, RK8)

“ตอนนี้ Compliance ยังเดินเองตรวจเองกันอยู่สองสามคน เดียวเราก็จะเริ่มมี Spy อยู่ตามจุดต่าง ๆ ซึ่งกลุ่มคนพวกนี้ก็ต้องปิดตัวเองว่าทำงานให้กับ PDPA เราก็จะมีกลุ่มคนเหล่านี้ช่วยกันตรวจสอบ โดยจะเป็นกลุ่มคนจากแผนกต่าง ๆ เจตตรงไหนก็ถ้ารู้อยู่แล้วแจ้งกันมา” (Executive Management, RK7)

“สัญญา Vendor Partner พนักงานด้วยต้องปรับหมดเมื่อก่อนจะเป็น การขอความยินยอม (Consent) ในสัญญาก็ต้องปรับข้อความให้มันดูเป็นสัญญาจากคำว่ายินยอมเป็นตกลงหรือเงื่อนไขบางอันที่มันไม่จำเป็นก็เอาออกอาจจะเพิ่มเรื่องลูกค้ารับทราบ ประกาศความเป็นส่วนตัว (Privacy Notice) เข้าไป” (Management, RK8)

2. การเพิ่มกระบวนการปฏิบัติงานใหม่

หลังจากการปรับใช้พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลต้องมีกระบวนการปฏิบัติงานใหม่ ๆ ที่เพิ่มขึ้นหลัก ๆ 3 กระบวนการ ได้แก่ 1) กระบวนการบริหารจัดการการขอความยินยอม (Consent Management) 2) กระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล (Data

Subject Right Management) 3) กระบวนการแจ้งการรั่วไหลของข้อมูล (Data Breach Notification) โดยมีรายละเอียดตามตาราง

ตารางที่ 4.4

สรุปกระบวนการปฏิบัติงานใหม่

กระบวนการ	รายละเอียดกระบวนการ
1. กระบวนการบริหารจัดการการขอความยินยอม (Consent Management)	- บริษัทต้องกำหนดได้ว่าข้อมูลส่วนบุคคลใดที่บริษัทจำเป็นต้องจัดเก็บ ใช้ และเปิดเผยภายใต้ฐานความยินยอม (Consent) และจัดให้มีกระบวนการขอความยินยอมและการแจ้งประกาศความเป็นส่วนตัว (Privacy Notice) ที่มีความชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิด - จัดให้มีกระบวนการถอนความยินยอมที่สามารถทำได้โดยง่าย เนื่องจากเจ้าของข้อมูลถอนความยินยอมเมื่อใดก็ได้ (เว้นแต่มีข้อจำกัดตามที่กฎหมายกำหนด)
2. กระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right Management)	- ต้องมีการออกแบบกระบวนการทำงานและช่องทางรองรับการเข้ามาใช้สิทธิของเจ้าของข้อมูลตามที่กฎหมายกำหนด - อย่างไรก็ตามสิทธิบางอย่างของเจ้าของข้อมูลก็เป็นเรื่องยากในการจัดการสำหรับองค์กร เช่น สิทธิในการลบ (Right to be Forgotten) ซึ่งในทางปฏิบัติสามารถทำได้ยากโดยเฉพาะข้อมูลเก่า ๆ เพราะข้อมูลกระจายอยู่ทั่วองค์กร หรือ สิทธิในการโอนย้ายข้อมูล (Right to Data Portability) เนื่องจากยังต้องอาศัยความพร้อมในหลาย ๆ ด้านทั้งภาครัฐและเอกชน ซึ่งมีการลงทุนที่ค่อนข้างสูง - ต้องออกแบบกระบวนการพิสูจน์และแก้ปัญหาข้อร้องเรียนจากเจ้าของข้อมูล
3. กระบวนการแจ้งการรั่วไหลของข้อมูล (Data Breach Notification)	- จัดให้มีการกระบวนการตรวจสอบสาเหตุการรั่วไหลของข้อมูลที่มีความรวดเร็ว - ออกแบบกระบวนการแจ้งเหตุการณ์รั่วไหลข้อมูลต่อหน่วยงานกำกับและเจ้าของข้อมูลที่สามารถแจ้งเหตุการณ์ได้ภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด

“การขอความยินยอม (Consent) ของเรามีหลักๆ มี 4 แบบ คือ 1. ตาม Market Conduct คือเปิดเผยข้อมูลให้คนอื่น 2. เรื่องของการทำ Profiling 3. เรื่อง Data Sharing ภายในกลุ่มธุรกิจ ที่ไม่ใช่เพื่อวัตถุประสงค์ทางการตลาด แต่เป็นเพื่อวัตถุประสงค์หลาย ๆ อย่าง เพื่อให้บริการลูกค้าซึ่งลูกค้าจะเห็นบัญชีทุกบัญชีของลูกค้าในกลุ่มการเงินเรา 4. ไบโอมเมตริกซ์ (Biometrics) ด้วยอุตสาหกรรมธนาคารมันจะมีโครงการระบบการพิสูจน์และยืนยันตัวตนรูปแบบดิจิทัล (National Digital ID: NDID) ด้วย Biometric Face Recognition (FR) การทำตัว FR มันต้องทำการขอความยินยอมแบบชัดแจ้ง (Explicit Consent) แยกออกมา” (Management, RK8)

“สิ่งที่อาจจะเพิ่มเข้ามาเยอะคือเรื่องการเข้ามาใช้สิทธิของเจ้าของข้อมูล ที่อาจจะทำให้นาการเหมือนมีภาระเพิ่มนอกเหนือจาก Core Business ที่ธนาคารทำก็เป็นกระบวนการที่เพิ่มขึ้น” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR5)

“เรื่องข้อมูลรั่วไหล ต้องมีรายงานให้กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบภายใน 72 ชม. แต่เราก็บอกว่าเราอยากให้มีกระบวนการภายในคือเกิดเหตุแล้วแจ้งทันทีและภายใน 24 ชม. เจ้าของข้อมูลที่เกิดเหตุขึ้นต้องบอกได้ว่าสาเหตุที่เกิดคืออะไร แล้วมีมาตรการอย่างไรไม่ให้อันเกิดขึ้นอีก พร้อมกับมาตรการเยียวยา” (Executive Management, RK7)

“สิ่งหนึ่งที่น่ากังวลในอนาคต บรรดาสิทธิต่าง ๆ ที่ผู้บริโภคจะมีสิทธิในการถูกลืมหรือสิทธิในการลบ(Right to be Forgotten/Right to Erasure) กับสิทธิในการโอนย้ายข้อมูล (Right to Data Portability) อันนี้สำคัญ สิ่งหนึ่งที่จะสร้างต้นทุนให้กับเราก็คือการที่เราไม่สามารถทำได้ด้วยตัวเองเราต้องทำตามมาตรฐานต้องเชื่อมกับคนอื่น ไม่ใช่ธนาคารกับธนาคารอย่างเดียว ธนาคารกับโรงแรม กับโรงพยาบาลแล้วจะทำอย่างไร ข้อมูลมันคนละแบบเพราะมันต่างวัตถุประสงค์กันจะต้องโอนให้กันมากน้อยแค่ไหน Data portability นี่สำคัญกฎหมายยังไม่ชัดเจนซึ่งถ้าตรงนี้มันยังไม่ชัดเจน เราไม่รู้ว่ามันต้องทำขนาดไหนเป็นแบบยุโรปเลยหรือไม่” (Executive Management, RK6)

“ระบบบริหารจัดการการขอความยินยอม (Consent Management) ถ้าหน่วยงานไหนที่ใช้เยอะๆ ก็จะเหนื่อยเพราะว่าการให้ความยินยอมมันพามาซึ่งภาระทั้งในการเก็บ และการต้องมีระบบให้เขาถอนได้ด้วย แล้วระบบการถอนกฎหมายก็เขียนว่าห้ามยากไปกว่าตอนที่ขอข้อมูล จากเดิมการขอความยินยอมไม่เคยมีการถอน” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

(4) ผลกระทบต่อทรัพยากรบุคคล

จากการสัมภาษณ์พบว่า การปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นส่งผลกระทบต่อทรัพยากรบุคคลภายในองค์กรแบ่งเป็น 4 ประเด็น ได้แก่ 1) ภาระงานที่เพิ่มขึ้น 2) เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้านข้อมูล (Data Literacy)

3) มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 4) เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

1. ภาระงานที่เพิ่มขึ้น

ทรัพยากรบุคคลภายในธนาคารได้รับผลกระทบในเรื่องภาระงานที่เพิ่มมากขึ้นจากการปรับปรุงกระบวนการทำงานให้เป็นไปตามกฎหมายกำหนด ทั้งส่วนงานสนับสนุนและส่วนงานปฏิบัติการ โดยส่วนงานสนับสนุน (Back Office) ก็จะมีภาระที่เพิ่มขึ้นจากการที่ต้องวางแผนและออกแบบการปฏิบัติงานในการปรับใช้กฎหมายกับกระบวนการทางธุรกิจซึ่งจะมีการแต่งตั้ง DPO และคณะทำงาน (Working Team) จากส่วนงานต่าง ๆ และยังคงต้องรับผิดชอบหน้าที่ในส่วนงานเดิมและเพิ่มเติมหน้าที่งานใหม่ในการปรับใช้กฎหมาย แต่อย่างไรก็ตามในอนาคตอาจมีการพิจารณาสรรหาพนักงานเพิ่มหากมีปริมาณงานที่มากขึ้น

ส่วนงานปฏิบัติการ (Staff) พนักงานธนาคารที่ให้บริการลูกค้าก็จะมีขั้นตอนการปฏิบัติงานที่เพิ่มมากขึ้น ต้องมีการสื่อสารสร้างความเข้าใจกับลูกค้าเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะการขอความยินยอม (Consent) จากลูกค้า รวมถึงต้องเรียนรู้กระบวนการทำงานที่เปลี่ยนแปลงไป

“มี Working Team ในการทำ Project PDPA ประกอบด้วยหน่วยงานบริหารความเสี่ยงด้านปฏิบัติการ ด้านไอที หน่วยงานกำกับดูแล และฝ่ายกฎหมายมาทำงานร่วมกัน ดังนั้นคนในองค์กรงานเพิ่มอย่าง Compliance ก็ต้องประสานงานเรื่องนี้ทั้งภายนอกภายในเรา Implement เอง 100%” (Staff, RK4)

“ขั้นตอนการปฏิบัติงานเพิ่มขึ้นต้องให้ลูกค้าเซ็นให้ความยินยอม (Consent) สิ่งที่เพิ่มขึ้นคือบทพูดธนาคารจะเอาทั้ง ๆ ที่รู้ว่าไม่ให้ก็ไม่ใช่ไรก็ยังไม่ทำธุรกรรมปกติได้แต่จะทำยังไงที่จะหว่านล้อมให้ลูกค้ายินยอมให้ข้อมูลเห็นประโยชน์ของการให้แต่ไม่ให้ก็ไม่ใช่ไรแต่เราก็ต้องแจ้งว่าสิ่งที่ลูกค้าจะได้ผลกระทบคืออะไร” (Executive Management, RK7)

“ช่วงนี้ไม่มีการสรรหาเพิ่ม ก็ผมนี้แหละทำ ตอนนี้นั้นอยู่ในช่วงลดคนไม่รับเพิ่ม เราก็ Allocate คนทำ เพราะฉะนั้นก็ไม่ต้องจ้างคนอื่นแล้ว อย่างตัวผมเองเป็น DPO ก็ต้องทำงานอย่างอื่นด้วย ในทีมกฎหมายมีคนหนึ่งทำด้านนี้โดยเฉพาะ Compliance มีคนหนึ่ง Allocate 90% ทำด้านนี้โดยเฉพาะ อีก 4 คน 50% หลังกฎหมายมีผลแล้วเราจะมาประเมินอีกทีว่าควรต้องตั้งฝ่ายมัย จ้างเพิ่มมัย” (Management, RK8)

“ตำแหน่ง DPO ก็ไม่ค่อยมีคนอยากทำหรอก เป็นตำแหน่งที่น่ากลัวมาก จริง ๆ แล้วมันก็เหมือนเป็นการไปเพิ่มงานให้เขาจากงานเดิมที่รับผิดชอบ ถ้าไม่สรรหาคนใหม่เข้ามา ใช้คนเก่าก็จะเป็นประมาณนี้ แต่ก็มีคนอยากสรรหาเหมือนกันนะ ใครจะไปอยากทำ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

2. เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้านข้อมูล (Data Literacy)

พนักงานทุกคนในองค์กรควรมีการเพิ่มทักษะในการทำความเข้าใจข้อมูล (Data Literacy) ซึ่งสำคัญมากในยุคที่ข้อมูลมีอยู่มากมาย พนักงานจึงต้องมีความเข้าใจกับข้อมูลที่ใช้ทั้งในแง่ของกฎหมายและการใช้ให้เกิดประโยชน์อย่างสูงสุด และที่สำคัญต้องได้รับการอบรมความรู้เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงทัศนคติต่อข้อมูลส่วนบุคคลต้องเปลี่ยนแปลงไปจากเดิมที่มองว่าข้อมูลเป็นสินทรัพย์ของบริษัทแต่ปัจจุบันนั้นเป็นสินทรัพย์ของเจ้าของข้อมูล

“เราก็เชิญอาจารย์ผู้มีความรู้เรื่อง PDPA มาให้ความรู้เรื่องเกี่ยวกับ พ.ร.บ. กับบอร์ดโดยเฉพาะให้รู้เลยว่าหน้าที่ของคุณคืออะไรคุณมีหน้าที่อย่างไร พนักงานทุกคนตั้งแต่ CEO ลงมาพนักงานปฏิบัติการทุกคนต้องเรียน E-Learning ของ PDPA มี Roadshow ที่เราจะไปหา Target Group ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล” (Executive Management, RK7)

“ในยุคของเทคโนโลยีทุกคนทุกบริษัทต้องมีในเรื่องของ Data Literacy ความรู้ความเข้าใจเรื่องข้อมูลขั้นพื้นฐาน เหมือนที่ทุกวันนี้ใช้คอมพิวเตอร์เป็น ใช้อินเทอร์เน็ต ใช้โซเชียลมีเดียเป็น ดังนั้นเรื่องการใช้ข้อมูลคุณต้องรับรู้เข้าใจได้โดยไม่ต้องมานั่งสอนเรื่องนี้ ทุกคนต้องรู้แล้วว่าเราอยู่ในกระบวนการไหน ติดตรงไหนของกฎหมายข้อนี้บ้าง นั่นหมายถึงการให้ความรู้กับคนในองค์กรก็ต้องเพิ่มขึ้นด้วย ส่วนการสร้างทีมจากข้างในต้องมีการสรรหาคนเพิ่มเติมยังงี้ก็ต้องมี” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“จุดเปลี่ยนของ PDPA มันเปลี่ยนแค่แนวคิด จากที่ธนาคารคิดมาเสมอว่าข้อมูลลูกค้าเป็นสินทรัพย์ของธนาคาร เพราะฉะนั้นก็มาเปลี่ยนความคิดใหม่ ข้อมูลพวกนี้มันเป็นสินทรัพย์ของลูกค้า ลูกค้าเอามาฝากไว้กับธนาคาร ธนาคารสามารถใช้ได้อย่างจำกัดตามที่เขาฝากไว้หรืออนุญาต” (Executive Management, RK6)

3. มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

พนักงานภายในองค์กรต้องได้รับบทลงโทษจากการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทกำหนดเพื่อเป็นการควบคุมการปฏิบัติตามกฎหมายและกฎระเบียบของคนในองค์กร รวมถึงผู้บริหารที่มีโทษทางอาญาตามกฎหมายอีกด้วย

“โทษทางอาญามาถึงบอร์ด มาถึงผู้บริหาร ส่วนพนักงานของเราตอนนี้ใครมีบัตรประชาชนของลูกค้าในลิ้นชักโต๊ะนี้ โทษมีการตักเตือนเป็นลายลักษณ์อักษร สำเนาเหมือนกันถ้าใบเดียวก็จะตักเตือนด้วยวาจา 3 ใบ เป็นลายลักษณ์อักษร ถ้าเจอเป็นปึก ไล่ออกเลย” (Executive Management, RK1)

“เรื่องของ KPI เมื่อเรามีเป้าให้เขาถ้าเขาทำผิดมันคือตัวที่ไปลดคะแนนของเขาบางครั้งคุณมีเป้าสูงแต่บังเอิญว่าคุณผิดในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเยอะกลายเป็นว่าเดือนนั้นคุณอาจจะไม่ได้อะไรเลยก็ได้ ประเด็นที่ 1 คุณจะไม่ได้ค่าคอมมิชชั่นอะไรเลยคือสิ่งที่เราทำโทษเขา 2 ถ้าคุณทำผิดเยอะตามเกณฑ์ที่เรากำหนดไว้คุณก็ไม่สามารถขายของต่อได้นะนั่นก็แปลว่าเขาขาดรายได้” (Executive Management, RK6)

“เรามีการควบคุมอยู่แล้วตาม Code of Conduct เพียงแต่ว่าเราอาจจะต้องมาปิดฝุ่น จากที่ไม่เคยลงโทษ มันถึงเวลาแล้วหรือยัง ก็ต้องลงโทษกันสักทีมัย เพราะว่าสุดท้ายถ้าเหตุมันเกิดแล้วธนากรรมมันเสียหายทุกกรณี” (Executive Management, RK7)

4. เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

ถือว่าเป็นผลกระทบในเชิงบวกแก่บุคลากรในองค์กรในการเพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path) เพื่อดำรงตำแหน่ง DPO หรือทีมงานสนับสนุน DPO ในหลาย ๆ สายงาน เช่น สายงานบริหารความเสี่ยง สายงานกำกับดูแลกิจการ สายงานกฎหมาย สายงานเทคโนโลยีสารสนเทศ และสายงานตรวจสอบ เป็นต้น

“พอมีตำแหน่ง DPO ขึ้นมาเหมือนเป็นอีก Career Part ในสายงานกฎหมาย IT Compliance หรือ Audit” (Management, RK5)

“จริง ๆ มันเป็นกฎหมายสร้างงานสร้างโอกาสเหมือนกันนะ ตำแหน่งใหม่ก็มี Job ใหม่ก็มี Software Consult ต่าง ๆ ก็ทำเรื่องนี้เพิ่ม” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

(5) ผลกระทบต่อเทคโนโลยี

จากการสัมภาษณ์ พบว่า ผลกระทบจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อเทคโนโลยีมีผลกระทบใน 2 ส่วน ได้แก่ 1) การลงทุนในเทคโนโลยีใหม่ 2) การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร โดยมีรายละเอียด ดังนี้

1. การลงทุนในเทคโนโลยีใหม่

การลงทุนในเทคโนโลยีใหม่เพื่อรองรับการปฏิบัติตามกฎหมายนั้น ไม่ได้เป็นการลงทุนในซอฟต์แวร์สำเร็จรูปสำหรับ PDPA เป็นการเฉพาะ เนื่องจากผู้ประกอบการเห็นว่ายังไม่มีซอฟต์แวร์สำเร็จรูปใดที่จะใช้งานได้กับกระบวนการปฏิบัติงานของทุกองค์กร แต่จะลงทุนในเทคโนโลยีใหม่ ๆ เกี่ยวกับระบบบริหารจัดการการให้ความยินยอม (Consent Management) และระบบการบริการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) โดยเฉพาะอย่างยิ่งในเรื่องสิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to Data Portability) ที่ต้องมีการลงทุนสูงแต่อย่างไรก็ตามต้องรอความชัดเจนของข้อกำหนดถึงขอบเขตที่ต้องปฏิบัติ

นอกจากนี้ยังมีการเปลี่ยนซอฟต์แวร์บางรุ่นที่ไม่สามารถพัฒนาได้หรือต้นทุนในการพัฒนาสูงเพื่อให้รองรับกับกฎหมาย ส่วนเทคโนโลยีทางด้านการรักษาความปลอดภัย

ธนาคารให้ความสำคัญและลงทุนในเรื่องนี้มาระยะหนึ่งแล้วจึงไม่ได้รับผลกระทบมากนักแต่ก็ยังมีการเพิ่มความเข้มข้นในการรักษาความปลอดภัยเพิ่มขึ้นและมองหาเครื่องมือใหม่ ๆ ที่จะเข้ามาช่วยในเรื่องของการป้องกันข้อมูลเพิ่มขึ้น อย่างไรก็ตามการใช้เทคโนโลยีเข้ามาช่วยในการปฏิบัติตามกฎหมายก็ต้องแลกมาด้วยความเสี่ยงทางด้านความปลอดภัยยิ่งใช้เทคโนโลยีมากขึ้นเท่าไรก็ต้องลงทุนในการรักษาความปลอดภัยเพิ่มมากขึ้น

“พวกซอฟต์แวร์ที่เราไม่ได้พัฒนาเองที่ซื้อมาจาก Third Party เราไปสั่งให้ทำนั่นนี่เขาไม่ทำเราจะไป Modify ก็เหนียวยากมันจะเกิดการเปลี่ยนเวอร์ชัน” (Executive Management, RK1)

“ในภาคธนาคารไม่ได้มีผลกระทบมากแบบมีนัยสำคัญ แต่มันอาจทำให้ต้องมีกระบวนการในการควบคุมเพิ่มขึ้นกับการทำตัวระบบบริหารจัดการการขอความยินยอม (Consent Management)” (Management, RK3)

“จะมีเพิ่มเติมในส่วนของระบบการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล ที่มันจะต้องเพิ่มขึ้นมาหลักๆ ช่องทางที่มันจะต้องปลอดภัยทั้งหมดมันก็จะต้องเพิ่มความเข้มข้นมากขึ้นในช่องทางเหล่านั้น ก็จะมาพิจารณาช่องทางที่เราใช้ในการสื่อสารกับบุคคลคนภายในภายนอกว่าปลอดภัยเพียงพอมั้ยถ้าไม่พอก็ต้องมีการลงทุนตรงนี้ที่เพิ่มขึ้นมา” (Staff, RK4)

“มีการลงทุนในเรื่องของการใช้ระบบการหาเครื่องมือเข้ามาช่วยในเรื่อง การป้องกันการสูญหายของสารสนเทศที่มีความสำคัญ Data Leak Prevention (DLP)” (Executive Management, RK7)

“ตอนนี้ยังไม่มีการลงทุนเพิ่มไม่ใช่ไม่มีแต่เรากำลังสำรวจอยู่ หลาย ๆ ครั้งที่เราฟังเซลล์มาขายของแล้วไม่คิดว่าจะช่วยได้ มันไม่มีซอฟต์แวร์อะไรที่มาปักแล้วมันดีอย่างที่เขามโนะ มันดีเพราะว่าเขาถืออัปขึ้นมาแล้ว แต่ถ้าเอามาใช้งานจริงมันไม่น่าจะได้ แต่ถ้ามันมีอะไรที่มันว้าว ก็พร้อมที่จะลงทุนนะ ผู้บริหารไม่ติดอะไรในเรื่องของการลงทุน ตอนนี้เทคโนโลยีที่เราลงทุนไปก็มีระบบบริหารจัดการการขอความยินยอม (Consent Management)” (Management, RK8)

“ต้องแยกเป็นสองส่วน ส่วนแรกที่เกี่ยวข้องกับคุ้มครองข้อมูลส่วนบุคคล เพื่อไม่ให้เกิดการรั่วไหลอันนั้นต่อให้ไม่มีกฎหมายตัวนี้ก็ต้องคุ้มครองกันอยู่แล้ว แต่สิ่งที่ต้องลงทุนเพิ่มคือลงทุนเพื่อให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลของตัวเอง เข้ามาจัดการข้อมูลของตัวเอง ขอยกเลิกได้ ตรวจสอบได้” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC4)

“ต้องมีระบบบริหารจัดการการขอความยินยอม (Consent Management) เพราะจากเดิมไม่เคยมีกระบวนการถอนข้อมูลของลูกค้า” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

“เทคโนโลยีมันไม่ได้ตอบโจทย์ทุกเรื่องแต่ถามว่ามันมาช่วยได้มั้ย เทคโนโลยีช่วยได้ทุกเรื่องและก็ไม่สามารถช่วยได้ทุกเรื่องเหมือนกัน เทคโนโลยีอาจจะช่วยในเรื่องของความเร็ว เรื่องของ *Economy of speed* กับ *Economy of Scale* แต่ไม่ได้ช่วยเรื่อง *Security* แน่ ๆ ยิ่งใช้เทคโนโลยีมากขึ้นเท่าไร *Security* ยิ่งต้องสูงตามมากขึ้นเท่านั้น” (Executive Management, RK6)

2. การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร

ถือว่าเป็นโอกาสในการพัฒนาและผลักดันเทคโนโลยีในภาคธุรกิจให้เป็นธนาคารยุคดิจิทัลมากขึ้น (Digital Banking) เนื่องจากกฎหมายเข้ามาเสริมความเชื่อมั่นในการปกป้องข้อมูลส่วนบุคคลให้กับลูกค้า เพียงแค่ในช่วงแรกของการปรับใช้กฎหมายอาจจะทำให้การพัฒนาเทคโนโลยีชะลอตัวลงเท่านั้น

“ไม่ได้คิดว่ามันเป็นปัญหาอะไรกับการพัฒนาเทคโนโลยีในธุรกิจธนาคาร มันน่าจะเป็นโอกาสสำหรับคนที่สามารถทำได้ดี คนที่ทำได้ปลอดภัย แต่ถ้าใครที่จะทำ Digital Banking หรือ Digital Business แต่ว่าดูแลข้อมูลของลูกค้าไม่ดี ก็น่ากลัวมาก” (Executive Management, RK1)

“ไม่เรียกว่าเป็นการ Disrupt นะ มันเหมือนเบรคให้ช้าลง เพราะว่าการใช้ IT มันเป็นแค่ในมุมของช่องทางในการรับข้อมูลต่าง ๆ หรือเป็นการรับส่ง Order จากลูกค้าแต่ธุรกิจหลักเรายังอยู่ด้านหลัง” (Management, RK3)

“ธนาคารก็เป็นอีกภาคหนึ่งที่มองว่าเราต้องเป็น Digital เรามองมาตั้ง 10 ปีที่แล้วจะอย่างไรให้เกิด Digital Eco System ให้ได้ ดังนั้นเรื่องของ Data Security เลยเป็นเรื่องสำคัญเพียงแต่ว่า PDPA มาเสริมไม่ได้พูดถึงเรื่องของ Data Security แยกเดียวเรื่องของการใช้ข้อมูลของลูกค้าในการทำธุรกิจต่างหากเป็นเรื่องสำคัญที่เพิ่มขึ้นมา (Executive Management, RK6)

“ช่วงสั้น ๆ จะกระทบการพัฒนาเทคโนโลยีแต่ในระยะยาวมันจะส่งผลให้ธุรกิจใช้ข้อมูลได้อย่างคุ้มค่าและมีประสิทธิภาพมากขึ้น” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ถึงตอนนี้มันจะเริ่มมีพวกเรื่อง M Banking หรือ I Banking Digital Banking แต่มันก็เป็นช่วงเริ่มต้น หลัก ๆ อะไรที่มันเป็นการออกแบบเพื่อการรักษาความเป็นส่วนตัวมันเป็นแนวปฏิบัติที่ดีอยู่แล้วที่คุณจะต้องมีอะไรกับเรื่องพวกนี้ มันไม่ได้เป็นอุปสรรคและที่สำคัญมันเป็นประโยชน์ด้วย” (ผู้เชี่ยวชาญกฎหมาย, RGL3)

(6) ผลกระทบรายได้และต้นทุนขององค์กร

จากการสัมภาษณ์ พบว่า ในปัจจุบันกฎหมายไม่ได้ส่งผลกระทบทำให้รายได้ของธนาคารเพิ่มขึ้นหรือลดลง แต่หากบริษัทสามารถทำได้ดีกว่าบริษัทอื่น ๆ อาจจะเป็นโอกาสดึงดูดเข้ามาเป็นของบริษัท เพิ่มความสัมพันธ์กับลูกค้าในระยะยาว ทั้งนี้ขึ้นอยู่กับว่าลูกค้าให้คุณค่ากับการคุ้มครองข้อมูลส่วนบุคคลมากน้อยแค่ไหน แต่อย่างไรก็ตามการดำเนินการในภาคธุรกิจธนาคารมักจะมีแนวปฏิบัติที่เป็นมาตรฐานเป็นไปในทิศทางเดียวกันจึงทำให้การสร้างแตกต่างในเรื่องของการปฏิบัติตามกฎหมายเพื่อสร้างความได้เปรียบในการแข่งขันเป็นไปได้ยาก

“เราจะได้รายได้จากไหนไม่คิดว่าจะมีได้นะ” (Management, RK3)

“ถ้าในภาคธุรกิจธนาคารคิดว่าไม่สร้างโอกาสในการแข่งขัน เพราะเราตั้งสมาคมเพื่อให้การปฏิบัติงานเป็นมาตรฐานเดียวกัน เราจะไม่พยายามทำให้มันเด่นกว่า จริง ๆ แข่งกันแบบนั้นก็ดีนะอุตสาหกรรมมันจะดีขึ้นแต่ทุกวันนี้แค่ทำตามกฎหมายยังยากเลย คงไม่ใช่จุดเด่นในการขายของเราแน่นอน” (Staff, RK4)

“ณ ตอนนี้อย่างไม่มีผล อย่างที่บอกว่าเรามี Legitimate Interest เป็นผ้ายันต์กันเหนียวอยู่ตอนนี้เราก็ก๊อให้ได้มากที่สุดก่อน แต่อยู่บนพื้นฐานที่ว่าเราต้องไม่ละเมิดการตกลงลูกค้า” (Management, RK5)

“ตัวผู้ให้บริการที่มีอยู่ในตลาดถ้ารายไหนไม่ follow กฎหมายมันก็แข่งขันไม่ได้ ใครทำได้ดี ลูกค้าก็เชื่อมั่นลูกค้าก็จะไหลไปที่นั่นซึ่งทั้งหมดทั้งมวลลูกค้าจะต้องเห็นคุณค่ากับข้อมูลนี้ด้วยคือถ้าไม่สนใจก็จะไม่เกิดปรากฏการณ์ไหล” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC3)

“ในขณะที่เดียวกันก็ลดความเสี่ยงในเรื่องของความเชื่อมั่นเกี่ยวกับลูกค้าหรือผู้ใช้บริการเพราะฉะนั้นในการลดความเสี่ยงหรือความเสียหายที่เกิดขึ้นในทางกลับกันก็เป็นการเพิ่มความเชื่อมั่นแน่นอนว่าผลกระทบของมันก็คือมันอาจจะเพิ่มปริมาณของธุรกรรมและเพิ่มความสัมพันธ์กับลูกค้าในระยะยาว” (ผู้เชี่ยวชาญกฎหมาย, RGL3)

แน่นอนว่าสิ่งที่บริษัทหลีกเลี่ยงไม่ได้คือต้นทุนของการบริหารจัดการข้อมูลที่เพิ่มขึ้นจากต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) ซึ่งต้นทุนจะแบ่งออกเป็น 2 ช่วง คือ ต้นทุนช่วงแรกจะเป็นต้นทุนเริ่มต้นเพื่อปรับใช้กฎหมาย และต้นทุนหลังการปรับใช้กฎหมายนอกจากนี้ยังมีเรื่องของต้นทุนจากการจ้างงานคนภายนอก (Outsource) ที่เพิ่มสูงขึ้นอีกด้วย

ต้นทุนในช่วงแรกเพื่อที่จะปรับใช้กฎหมาย PDPA นั้นโดยหลัก ๆ จะประกอบด้วย ต้นทุนทรัพยากรบุคคล (Manhours) ที่ต้องใช้ในการวางแผนและออกแบบปรับปรุงเปลี่ยนแปลงกระบวนการทำงานทั้งองค์กรเพื่อรองรับกับกฎหมาย ต้นทุนในการปรับเปลี่ยนเอกสาร

แบบฟอร์มต่าง ๆ และการเปลี่ยนแปลงระบบการทำงานให้รองรับกฎหมาย ต้นทุนในการปรับปรุงระบบการรักษาความปลอดภัยของข้อมูล (Security System) ให้มีความปลอดภัยเพิ่มขึ้น ต้นทุนในการซื้อเทคโนโลยีใหม่ ๆ ตามที่ได้กล่าวไปแล้วข้างต้นรวมถึงต้นทุนในการติดตั้งและปรับแต่งเพื่อให้สามารถใช้งานเชื่อมต่อกับระบบเก่าต่าง ๆ ในองค์กรได้ นอกจากนี้ยังมีต้นทุนในการฝึกอบรมให้ความรู้ สร้างการตระหนักรู้ให้พนักงานภายในองค์กรทุกระดับ และต้นทุนจากการจ้างที่ปรึกษาภายนอกอีกด้วย

ส่วนต้นทุนในช่วงหลังการปรับใช้กฎหมายนั้นจะเป็นต้นทุนจากการปรับปรุงกระบวนการงานหากเมื่อปรับใช้จริงแล้วมีปัญหาที่อาจจะไม่สะดวก ไม่เป็นที่พอใจของลูกค้า หรือเสี่ยงต่อการไม่ปฏิบัติตามกฎหมายก็จะมีต้นทุนในการตรวจสอบ ประเมินผลและออกแบบการควบคุมใหม่ รวมถึงค่าบำรุงรักษาระบบต่าง ๆ

“ในภาพรวมการ Modify ระบบนี้แหละเป็นต้นทุนที่ใหญ่ที่สุดการที่มานั่งคุย มานั่งจิกนั่งติดตามพวกนี้ก็ใช้เวลา เสีย man-days ไปมหาศาลมันเป็นการออกแบบกระบวนการใหม่ ๆ มันเป็นความพยายามในการที่แต่ละคนลงไปศึกษาในงานของตัวเองแต่จริง ๆ เราก็คงไม่ได้เคยนับต้นทุนมันออกมา เรื่องของ PDPA มันก็จะไปถูกรวม ๆ อยู่กับเรื่องอื่น ๆ อย่างเช่น เรื่องการทบทวนกระบวนการก็มีการทบทวนอยู่แล้วเพียงแค่เพิ่ม PDPA เข้าไป” (Executive Management, RK1)

“การมี Consent Management ไม่ใช่ว่ามีระบบนี้แล้วมันจบระบบอื่น ๆ มันก็ต้องมาเชื่อมกันด้วยมันก็จะมาใช้จ่ายเหล่านี้ค่อนข้างจะเยอะ” (Management, RK3)

“ค่าใช้จ่ายเพิ่มขึ้นมาก ธนาครมีหลายระบบ ก็หมดไปกับค่าพัฒนาระบบ แล้วก็ค่าใช้จ่ายเกี่ยวกับการบริหารการเปลี่ยนแปลง (Change Management) มันรวมหมดเลย ไม่ว่าจะเป็น Training พนักงาน ผู้บริหาร เรื่องการแจ้งลูกค้า” (Management, RK5)

“ต้นทุนก็เป็นเรื่องของคนกับการปรับกระบวนการทำงานส่วนเทคโนโลยีอาจจะยังไม่ชัดมาก เพราะยังไม่อยากจะลงทุนโดยที่ยังไม่มั่นใจ การทำ Implementation เพิ่มเพื่อให้มันเข้ากับระบบที่ผ่านมา 70-80 ปี ค่า Implementation บานเลยแล้วยังมีค่าบริการดูแลและบำรุงรักษาต่อปีอีกมหาศาล” (Management, RK8)

“ต้นทุนในการบริหารจัดการข้อมูลสูงขึ้นจากเทคโนโลยีในวันนี้อาจจะแค่ส่วนหนึ่ง เพราะเทคโนโลยีในวันนี้ยังมีราคาแพง ต้นทุนในการเพิ่มทักษะและความรู้พนักงาน ซึ่งต้องตระหนักถึงความปลอดภัยของข้อมูลมากกว่า” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ต้นทุนมี 3 อย่าง คือ เทคโนโลยีต้องมีแน่ ๆ บุคลากรก็ต้องมีความรู้และเรื่องบริหารจัดการ (Management) เรื่องนโยบายและการจัดการ ระเบียบใหม่ ๆ ในการปฏิบัติงานและการใช้งานข้อมูล” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC3)

“ต้นทุนจะเป็นไปตามการไหลของข้อมูล (Data Flow) ที่ปรับเปลี่ยนอีกส่วนหนึ่งคือด้านความปลอดภัย ซึ่งต้นทุนมันจะมีสองแบบต้นทุนตั้งต้นตอนที่เปลี่ยนระบบ กับต้นทุนที่ต้องบำรุงรักษา ส่วนของทรัพยากรบุคคล ก็มีต้นทุนในการฝึกอบรม” (ผู้เชี่ยวชาญกฎหมาย, RGL2)

นอกจากนี้ยังมีต้นทุนที่เพิ่มสูงขึ้นจากการจ้างงานคนภายนอก (Outsource) ที่จะมีการคิดอัตราค่าบริการที่สูงขึ้นจากต้นทุนการปฏิบัติตามกฎหมาย (Compliance Cost) ที่เพิ่มขึ้น โดยเฉพาะรายที่มีการผูกขาดรวมถึงต้นทุนที่บริษัทต้องปรับตัวเพื่อเป็นมาตรฐานให้บริษัทสามารถใช้บริการได้

“สุดท้าย PDPA Compliance มันจะเกิดต้นทุนจากที่เราเคยจ่าย Outsource 10 บาท มันจะเป็น 150 250 อันนั้นมันเป็นความท้าทายของธนาคารที่ต้องมาพิจารณาด้วยนะว่าฉันยอมจ่ายสูงขึ้นเพื่อการป้องกันความเสี่ยงที่สูงขึ้น” (Management, RK8)

“ทุกครั้งที่มันมีกฎหมายหรือมีระเบียบ มันไม่สามารถออกแบบให้เหมาะกับทุกคนได้ เราต้องปรับตัวของเราเพื่อจะเข้ากับมาตรฐานกลางของเขา ต้นทุนมันเกิดขึ้นตรงนั้นแหละ ทุกการปฏิบัติตามกฎระเบียบคือต้นทุน” (Executive Management, RK7)

แต่อย่างไรก็ตามในอีกมุมหนึ่งก็มองว่ากฎหมายสามารถช่วยในการลดต้นทุนจากการที่จัดเก็บข้อมูลน้อยลง เก็บเฉพาะข้อมูลที่จำเป็นเท่านั้น ทำให้ประหยัดพื้นที่ในการจัดเก็บทั้งในรูปแบบของ Hard Copy และ Soft File และการลดความเสี่ยงจากการกระทำผิดกฎหมายที่เกิดค่าปรับจำนวนมากมหาศาล

“ถ้าเรามีที่เก็บของอยู่จำกัดจะเก็บข้อมูลที่ไม่ได้ใช้ไว้ทำไมเอาที่ไปเก็บข้อมูลที่จะเกิดขึ้นมากมายในอนาคตดีกว่า พื้นที่จัดเก็บประหยัดขึ้นทั้ง Physical ทั้ง Storage” (Management, RK5)

“ต้นทุนลดมัยก็มีนะเพราะว่าหลักการของ PDPA จริง ๆ แล้วคือการพูดถึงเรื่องของ Data Minimization ใช้ข้อมูลให้น้อยที่สุดเพื่อให้บรรลุวัตถุประสงค์” (ผู้เชี่ยวชาญกฎหมาย, RGL3)

“แน่นอนว่ามันมีประโยชน์ในเรื่องของการลดต้นทุนในเรื่องของการลดความเสี่ยง เช่น ความเสี่ยงทางด้านกฎหมายจากการที่ต้องไปจ่ายค่าเสียหายจากการรับผิดชอบต่าง ๆ” (ผู้เชี่ยวชาญกฎหมาย, RGL3)

สุดท้ายแล้วก็ยังไม่ได้มีการวัดผลกระทบที่แน่นอนสำหรับรายได้และต้นทุนแน่นอนว่ามันเกิดเป็น Compliance Cost ที่สามารถวัดเป็นตัวเงินได้แต่ก็ยังไม่เคยมีการคำนวณอย่างชัดเจน และในขณะเดียวกันถ้าบริษัทปฏิบัติตามกฎหมายก็จะมี Compliance Benefit เกิดขึ้นด้วย เช่น ไม่ต้องเก็บข้อมูลมากมายที่เป็นความเสี่ยง ประหยัดพื้นที่การจัดเก็บ ลดความเสี่ยง

จากการถูกปรับและเสียชื่อเสียงองค์กรซึ่งไม่สามารถวัดเป็นตัวเงินได้ ดังนั้นจึงไม่สามารถทราบได้แน่ชัดว่าระหว่าง Compliance Cost และ Compliance Benefit สุดท้ายแล้วผลจะเป็นต้นทุนที่เพิ่มขึ้นหรือประโยชน์ที่มากกว่า

4.2.1.2 ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร

(1) ผลกระทบต่อลูกค้า

จากการสัมภาษณ์ พบว่า ลูกค้าได้รับผลกระทบจาก พ.ร.บ. คื้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งผลกระทบในเชิงบวกและผลกระทบในเชิงลบ โดยผลกระทบในเชิงบวก คือ ลูกค้าได้สิทธิในการคื้มครองข้อมูลส่วนบุคคลตามกฎหมายและมาตรฐานการคื้มครองข้อมูลส่วนบุคคลจากธนาคาร สร้างความมั่นใจให้กับลูกค้าว่าข้อมูลส่วนบุคคลจะไม่ถูกนำไปใช้นอกเหนือวัตถุประสงค์ที่ได้แจ้งไว้และมีความปลอดภัย ส่วนผลกระทบในเชิงลบ คือ ลูกค้าจะมีต้นทุนค่าบริการเพิ่มขึ้นในรูปแบบของต้นทุนแฝงจากอัตราดอกเบี้ยเงินกู้ที่เพิ่มขึ้นหรือปรับลดอัตราดอกเบี้ยเงินฝากเพื่อที่ธนาคารจะสามารถชดเชยต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามกฎหมาย นอกจากนี้ยังมีผลกระทบต่อประสบการณ์การใช้บริการของลูกค้า (Customer Experience) เช่น ขั้นตอนการทำธุรกรรมที่มากขึ้น ลูกค้ารู้สึกเสียเวลา ไม่อยากทำความเข้าใจเรื่องใหม่ๆ มากนัก หรือการใช้บริการเว็บไซต์ ที่จะมีการขออนุญาตเก็บ Cookies ทำให้ไม่สะดวกในการใช้งาน เป็นต้น แต่ทั้งนี้ก็ขึ้นอยู่กับการตระหนักถึงการคื้มครองข้อมูลส่วนบุคคลของลูกค้าแต่ละรายด้วย

“ในมุมมองของผู้ใช้งานผลกระทบน่าจะเป็นพวกดิจิทัล Platform เวลาคุณเข้าเว็บไซต์จะเริ่มเจอถามเรื่อง Cookie มันไม่ได้บังคับให้ตอบยินยอมหรอกแต่มันก็จะแจ้งเตือนในทุกหน้า ถ้าไม่ยินยอมจะสร้างความรำคาญก็จะตอบยินยอมไป” (Management, RK3)

“ในมุมมองลูกค้าเขาได้รับสิทธิในการคื้มครองข้อมูลมากขึ้นเป็นประโยชน์มากกว่า แต่ว่าขั้นตอนการให้บริการก็จะมากขึ้น เพราะฉะนั้นมันก็จะกระทบในมุมมอง ประสบการณ์การใช้บริการของลูกค้า (Customer Experience) เช่นว่ามันต้องเซ็นอะไรเยอะขึ้น ซึ่งมันก็ขึ้นอยู่กับลูกค้ามีความตระหนัก (Aware) แะไหนด้วย” (Management, RK5)

“Compliance Cost มันจะถูกผลักไปหาผู้บริโภคเป็นต้นทุนแฝงที่เราไม่รู้ เช่น การลดอัตราดอกเบี้ยเงินฝาก ดอกเบี้ยการให้สินเชื่อเพิ่มขึ้นเพื่อเอามาชดเชยค่าใช้จ่ายพวกนี้ พี่มองว่ามันไม่ยุติธรรม เพราะว่า PDPA คนที่ได้รับประโยชน์คือลูกค้าส่วนบุคคล แต่ลูกค้ากลุ่มนี้ต้องรับต้นทุนเพิ่มขึ้น ลูกค้า Corporate เราต้องดึงลูกค้ากลุ่มนี้ไว้ต้องขายของถูกให้เขา แปลว่าเราต้องไปเก็บผู้บริโภคให้แพงขึ้น ตามหลักการทำธุรกิจปกติอยู่แล้ว ดังนั้นถ้ากฎหมาย Require มาขึ้นเรื่อย ๆ มากกว่าสิ่งที่ธนาคารมี นั่นคือต้นทุนจะไปหาผู้บริโภค” (Executive Management, RK6)

“ลูกค้ายกลุ่ม Wealth เป็นเจ้าของกิจการใหญ่ ๆ เขาไม่มาเสียเวลาเซ็นต์ให้ความยินยอม (Consent) นะ เขาต้องการผลตอบแทนลูกค้าย Wealth เซ็นเปิดบัญชี ไม่เกิด 2 ลายเซ็นหรอก เกินกว่านี้เขาต่ำแล้ว” (Management, RK8)

“ก็มีเป็นไปได้ว่าลูกค้ายจะรำคาญขั้นตอนที่เยอะขึ้น” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

(2) ผลกระทบต่อคู่ค้า

จากการสัมภาษณ์ พบว่า คู่ค้า (Vendor) ได้รับผลกระทบในเรื่องของโอกาสในการได้รับงานจากธนาคารมากขึ้นหรืออาจลดลง เนื่องจากการปรับเปลี่ยนกระบวนการคัดเลือกคู่ค้าทั้งการพิจารณาคัดเลือกคู่ค้ารายใหม่และการต่อสัญญารายเก่าของธนาคารจะต้องเพิ่มหลักเกณฑ์เกี่ยวกับการให้บริการที่ได้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายกำหนด หากคู่ค้ารายใดไม่สามารถปฏิบัติตามหลักเกณฑ์และกระบวนการที่ธนาคารกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลก็จะเสียโอกาสในการรับงานและถึงแม้ว่าคู่ค้าบางรายที่ปรับตัวได้ก็ต้องมีต้นทุนที่เพิ่มมากขึ้น แต่หากเป็นผู้ประกอบการรายเล็กธนาคารมีอำนาจต่อรองสูงกว่าก็จะไม่สามารถเพิ่มอัตราการให้บริการได้ส่งผลกระทบต่อกำไรในการดำเนินงานลดลง รวมถึงอาจถูกตรวจสอบกระบวนการทำงานว่าเป็นไปตามเกณฑ์มาตรฐานที่ธนาคารกำหนดหรือไม่ อีกทั้งธนาคารจะใช้บริการ Outsource ที่เกี่ยวกับข้อมูลส่วนบุคคลน้อยลง โดยจะพยายามดึงกลับมาทำเองให้ได้มากที่สุด

นอกจากนี้สิ่งหนึ่งที่เปลี่ยนแปลงไปในภาพของอุตสาหกรรมจากกฎหมายฉบับนี้ คือ ในเรื่องของการประมวลผลข้อมูลมีการกำหนด ผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor) ซึ่งแต่เดิมเราจะมักจะเรียกกันว่า Outsource มีการควบคุมเรื่องข้อมูลกันผ่านสัญญาการรักษาความลับ (Confidential Agreement) ระหว่างกัน แต่ตามกฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องมีการควบคุมระหว่างกันด้วยสัญญาประมวลผล (Data Processing Agreement)

ดังนั้นเมื่อมีหลักการเรื่องของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลก็ส่งผลให้เกิดการแย่งชิงข้อมูลกันขึ้น เนื่องจากหากตีความว่าผู้ให้บริการเป็นผู้ประมวลผลข้อมูลซึ่งโดยหน้าที่ตามกฎหมายผู้ประมวลผลข้อมูลจะต้องเก็บ ใช้ และเปิดเผยตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้นไม่สามารถกระทำการนอกเหนือคำสั่งได้ ซึ่งบริษัทที่มีอำนาจในการต่อรองมากกว่าก็จะผลักดันให้อีกฝั่งเป็นผู้ประมวลผลข้อมูล โดยที่แท้จริงแล้วตามกฎหมายอาจจะเป็นผู้ควบคุมข้อมูลได้ทั้ง 2 ฝั่ง จึงเกิดเป็นภาพของการแย่งชิงข้อมูลกันแบบปลาใหญ่กินปลาเล็ก

“เราต้องทำสัญญาประมวลผลข้อมูลเพิ่มเติมในกรณีที่เขาเป็น Outsource รายเดิมส่วนรายใหม่ๆ เราก็พิจารณาว่าเขามีมาตรการในการควบคุมดูแลข้อมูลส่วนบุคคลของเราเพียงพอ เป็นไปตามกฎหมาย รวมไปถึงการทบทวนคุณสมบัติของ Vendor ก็จะมีการ

เอาเรื่องของ PDPA มาพิจารณาเพิ่มด้วย ก็คือเอาเข้ามาพิจารณาร่วมด้วยทั้งเรื่องของการจ้างรายใหม่ และต่ออายุรายเก่า” (Staff, RK4)

“พอมีเรื่อง Concept ของผู้ประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคล มันก็จะเป็นคิกระหว่างผู้ให้บริการ ฝ่ายที่เป็นใหญ่กว่าในตลาดก็จะพยายามผลักให้อีกฝ่ายเป็นผู้ประมวลผลข้อมูล โดยการส่งสัญญามาให้เราเป็นผู้ประมวลผล ถ้าเราเอาหลักของความเป็นเหตุเป็นผลมาวางเราจะเห็นว่ามันไม่ใช่แบบนั้นทั้งสองคนเป็นผู้ควบคุมข้อมูลด้วยกันทั้งคู่ทำไมต้องให้เป็นผู้ประมวลผลล่ะ เพราะการเป็นผู้ควบคุมข้อมูลสามารถบอกว่า คุณจะทำอะไรกับข้อมูลไม่ได้ละ ถ้าฉันไม่ยินยอมมันเลยกลายเป็นคิกระหว่างข้อมูลโดยปริยาย ซึ่งถ้าปลาใหญ่ปีบบังคับปลาน้อยมันก็จะกลายเป็นภาพนั้น” (Management, RK8)

“เข้าใจว่าเรื่องนี้จะทำให้เขามีต้นทุนที่สูงขึ้นแต่มันเป็นแค่ครั้งเดียว แต่ถ้าเขาไม่มีเลยก็จะไม่สามารถรับงานของธนาคารใหญ่ ๆ ได้ มันก็คือการลงทุนของเขา” (Management, RK8)

“ธนาคารพยายามดึงกลับมาทำเอง พยายามไม่จ้างคนนอกถ้าไม่จำเป็น เพราะว่าข้อมูลธนาคารเป็นข้อมูลที่มีความอ่อนไหว เช่น สมมติมีข้อมูลแล้วแบ่ง Segmentation แล้วจ้าง Outsource ไปทำ Marketing ต่อให้ แต่คนที่ทำหน้าที่ให้การวิเคราะห์ข้อมูลทั้งหมดเป็นธนาคารเขาพยายามควบคุมข้อมูลเขาให้ได้มากที่สุด” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“เราควรจะต้องตรวจสอบถ้าผู้ประมวลผลข้อมูลเอาข้อมูลของเราไป เช่น ว่ามีการคัดลอกไปอีก cloud หนึ่ง มีการทำ Firewall อย่างไรใน Cloud นั้นใครเข้าถึงได้บ้างมีต่อต่อไปที่ไหนอีกหรือไม่ ควรจะตรวจสอบค่ะ ถ้าไม่มีการตรวจสอบความเสี่ยงของธนาคารเต็ม ๆ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

4.3 แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การบริหารจัดการองค์กรเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลควบคู่กับการดำเนินธุรกิจได้นั้นต้องมีการบริหารจัดการทั้งปัจจัยภายในและภายนอกองค์กร โดยปัจจัยภายในองค์กรมีองค์ประกอบสำคัญ 3 องค์ประกอบ ได้แก่ คน (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) ซึ่งบริษัทจะต้องบริหารทุกองค์ประกอบให้มีความสอดคล้องซึ่งกันและกัน และจะขาดองค์ประกอบใดองค์ประกอบหนึ่งไม่ได้ ที่สำคัญอีกประการคือเรื่องของ Tone at the Top จากผู้บริหารก็เป็นส่วนสำคัญในการผลักดันทั้ง 3 องค์ประกอบให้มีประสิทธิภาพ นอกจากนี้ก็ยังมีปัจจัยต่าง ๆ ที่ช่วยในการสนับสนุนให้เกิดการปฏิบัติที่เป็นไปตาม

กฎหมาย เช่น การวางกลยุทธ์นโยบาย การออกแบบโครงสร้างองค์กรที่เหมาะสม วิธีการสื่อสารวัฒนธรรมองค์กร เป็นต้น อย่างไรก็ตามก็ต้องคำนึงถึงปัจจัยภายนอกองค์กรร่วมด้วย ได้แก่ ลูกค้า และคู่ค้า โดยมีรายละเอียดเพิ่มเติม ดังนี้

4.3.1 ปัจจัยสภาพแวดล้อมภายในองค์กร

ประกอบไปด้วย 3 องค์ประกอบหลัก ดังนี้

4.3.1.1 คน (People)

จากการสัมภาษณ์ พบว่า คนเป็นองค์ประกอบที่มีความเสี่ยงและสามารถควบคุมได้ยากที่สุดในทั้งหมด 3 ปัจจัย ซึ่งเรื่องของคนต้องเริ่มตั้งการมี Tone at the Top จากผู้บริหารก่อน อันดับแรกผู้บริหารต้องให้ความสำคัญ มีความเอาใจจริงเอาใจและทำให้เห็นเป็นแบบอย่างในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล มีการออกแบบโครงสร้างองค์กรให้เหมาะสมโดยมีการแต่งตั้ง DPO โดยส่วนใหญ่จะเป็นหัวหน้างานของหน่วยงานกำกับดูแลกิจการ หน่วยงานบริหารความเสี่ยง และหน่วยงานกฎหมาย เป็นต้น ส่วนทีมงานที่เข้ามาสนับสนุนการทำงานของ DPO ก็จะเป็นบุคคลที่มีทักษะทางด้านกฎหมาย ไอที หรือกระบวนการธุรกิจ โดยควรแยกออกมาเป็นอีกหนึ่งส่วนงานที่ดูแลด้านข้อมูลส่วนบุคคลและมี DPO เป็นผู้บังคับบัญชาของส่วนงานในระดับผู้บริหารระดับสูง (Top Management) หรืออาจจะตั้งแผนกงานที่ดูแลข้อมูลทั้งองค์กรและกำหนดให้ DPO และทีมงานเป็นส่วนงานหนึ่งในแผนกที่ดูแลเรื่องข้อมูลส่วนบุคคลโดยเฉพาะ และกำหนดให้ DPO สามารถรายงานตรงต่อผู้มีอำนาจตัดสินใจสูงสุดขององค์กร

แต่อย่างไรก็ตามสิ่งที่สำคัญที่สุดเรื่องของคน คือ การสื่อสารและการให้ความรู้แก่คนในองค์กรทุกระดับตั้งแต่คณะกรรมการบริษัทไปจนถึงพนักงานปฏิบัติการ โดยให้เข้าใจเกี่ยวกับบทบาทหน้าที่ของแต่ละระดับในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล หลังจากมีความรู้แล้วก็ต้องควบคู่ไปกับการสร้างความตระหนักรู้ (Awareness) ถึงมุมมอง ความเสี่ยง หลักการใช้ข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมาย ผ่านช่องทางการสื่อสารต่าง ๆ เช่น การอบรมที่มีการออกแบบอย่างเหมาะสมกับแต่ละระดับทั้งเนื้อหาและรูปแบบรวมถึงการวัดและประเมินผล การทำ Work Shop เพื่อให้เห็นภาพการปฏิบัติงานจริงหรือช่องทางสื่อสารอื่น ๆ ขององค์กร เป็นต้น

ปัจจัยอีกประการที่สำคัญคือการสร้างวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคลให้กับคนในองค์กร (Protection Culture) ให้คนในองค์กรรู้ว่าอะไรเป็นสิ่งที่ควรทำหรือไม่ควรทำ ค่อยบอกค่อยเตือนกันภายในองค์กร หากพนักงานคนไหนทำดีก็ให้คำชื่นชมและจะกลายเป็นตัวอย่างให้คนอื่น ๆ ในองค์กร ดีกว่าการลงโทษเลยในครั้งแรกมันจะกลายเป็นความกดดัน เป็นบรรยากาศที่น่ากลัวในการทำงานแต่หากมีการปฏิบัติที่ผิดระเบียบจริง ก็ต้องมีการลงโทษตามระเบียบเพื่อให้เกิดการบังคับใช้ที่จริงจัง นอกจากนี้ยังสามารถกำหนดการควบคุมลงใน KPI โดย

หากปฏิบัติไม่เป็นไปตามระเบียบที่บริษัทกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะมีผลลบต่อ KPI ซึ่งจะทำให้กระบวนการควบคุมเข้มข้นขึ้น

“อีกตัวหนึ่งที่สำคัญมาก ๆ คือ Tone at The Top เราเริ่มตั้งแต่ให้ความรู้กับคณะกรรมการบริษัทที่ใช้ที่ปรึกษามาสรุบให้ฟังว่าคืออะไร นิ่งคุยกับท่านก่อนการประชุม ลัก 20 นาทีท่านก็จะเข้าใจแล้วว่าคืออะไร จากนั้นเวลามีสื่อสารกันภายในองค์กรผมก็จะแจ้ง CEO ช่วยให้ Tone กับคนในองค์กร” (Executive Management, RK1)

“DPO ควรจะมีแยกออกมาเป็นหน่วยงานหนึ่งและไปอยู่ภายใต้ Data Governance ทั้งหมดแต่ไม่ควรจะไปแยกว่าเป็นข้อมูลส่วนบุคคลหรือไม่ใช่ข้อมูลส่วนบุคคล แล้วถ้าเป็นเรื่องของข้อมูลส่วนบุคคล DPO ก็รับไป” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR1)

“เราต้องสื่อสารให้ชัดเจนว่าผลกระทบจากการทำผิด ตัวคุณก็กระทบนะ ในมุมของผู้บริหารกระทบอย่างไร มุมของคนปฏิบัติงานกระทบอย่างไรมันมีระดับความซีเรียสของมันอยู่แล้ว ไม่มีระดับไหนไม่ซีเรียส เครียดไปคนละมุม” (Staff, RK4)

“สิ่งหนึ่งที่ต้องทำให้เกิด คือวัฒนธรรมการคุ้มครองข้อมูล (Data Protection Culture) ทำยังไงก็ได้ที่เจอ จับ ทำโทษ แล้วต้องจำ และไม่ทำอีก หลาย ๆ ครั้งพวก Policy หรือ Code of Conduct ที่เขียนมาเป็นเล็กระดาษ ไม่เคยเอามาใช้จริง เพราะงั้น PDPA อาจจะเป็นตัวกระตุ้น” (Executive Management, RK7)

“พนักงานทุกคนตั้งแต่ CEO เลย ลงมายันพนักงานปฏิบัติการทุกคนต้องเรียน E-Learning ของ PDPA มี Roadshow เราจะไปหากกลุ่มเป้าหมายซึ่งเป็นคนในองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล” (Executive Management, RK7)

“ธนาคารเราเริ่มจากการให้แครอตก่อน คนไหนทำดี คุณต้องชื่นชมนะ ตัวอย่างคนทำดีมันจะสร้างให้คนอื่นเห็นแล้วอยากทำตามมากกว่าที่เราจะลงโทษเลยครั้งแรก พอลงโทษแล้วมันเกิดบรรยากาศแห่งความกลัว คนก็จะมองเรื่องพวกนี้เป็นเรื่องน่ากลัวจริง ๆ เรื่องนี้มันไม่ใช่เรื่องน่ากลัว” (Executive Management, RK6)

“ความตระหนักรู้ (Awareness) ของคนสำคัญเพราะว่าความเล็งที่ละเกิดขึ้นก็จะเกิดขึ้นจากคนนี่แหละ” (Management, RK8)

“แต่สิ่งที่เราให้ความสำคัญคือการประเมินผลเรื่องความตระหนักรู้มันยาก เพราะงั้นสิ่งที่เราพยายามต้องทำ ก็คือต้องดูกลุ่มเป้าหมายเพื่อปรับเนื้อหาให้เหมาะกับกลุ่มเป้าหมาย แล้วช่องทางไหนดี เราก็มียุทธศาสตร์แล้วก็ส่งเป็นซีรีย่อออกไป” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ต้องมีการอบรมทุกคนในบริษัทต้องรู้ว่ากฎหมายครอบคลุมเรื่องอะไรบ้าง เกี่ยวข้องกับบริษัทเรา เกี่ยวข้องกับเขายังไง บริษัทเรามีการป้องกันอย่างไรบ้าง เพื่อให้

พนักงานเป็นตัวแทนบริษัทพูดคุยกับลูกค้าได้ เพราะว่าพอเขาเข้าใจและมั่นใจ และตัวจรรยาบรรณของพนักงานเองจะช่วยให้บริษัทผ่านจุดนี้ไปได้จริง ๆ ถ้าบริษัทจริงจังพนักงานก็จะจริงจัง แต่ว่าถ้าบริษัทบอกว่าเราจะทำนิดหน่อยมันก็ทำให้พนักงานรู้สึกว่าได้จริงจัง” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

“ต้องอบรมพนักงาน ให้ความรู้ในการปฏิบัติตน มี Code of Conduct เราควรให้ความรู้บุคลากรภายในให้มีความรู้ ความเชี่ยวชาญ สามารถตอบคำถามลูกค้าให้ได้เป็นอย่างดีเสียก่อน เพราะถ้าลูกค้ามีความรู้มากขึ้น การทำงานของพนักงานก็จะลำบากขึ้นเช่นกัน” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC3)

4.3.1.2 กระบวนการ (Process)

จากการสัมภาษณ์ พบว่า ด้วยแนวคิดของกฎหมายฉบับนี้เป็นเรื่องของการจัดการข้อมูลส่วนบุคคล ซึ่งต้องมีการทบทวนกระบวนการปฏิบัติงานทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและกระบวนการไหลของข้อมูล เพื่อออกแบบกระบวนการทำงานที่เป็นไปตามข้อกำหนดของกฎหมาย โดยจะทำการเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นให้น้อยที่สุดเพื่อลดความเสี่ยงและสามารถออกแบบการประมวลผลข้อมูลโดยใช้ข้อมูลให้น้อยลงแต่ได้ผลลัพธ์ที่มากขึ้น ซึ่งข้อมูลที่บริษัทเก็บ ใช้และเปิดเผยต้องมีฐานกฎหมายรองรับการเก็บนั้น ๆ ขึ้นอยู่กับบริษัทที่อาจจะเน้นไปทางฐานสัญญา (Contract) และฐานความยินยอม (Consent) หรือเน้นไปทางฐานประโยชน์อันชอบธรรม (Legitimate Interest) แต่โดยส่วนมากแล้วจะเน้นไปที่ฐานกฎหมายอื่นก่อนเลือกระบุเป็นฐานความยินยอม (Contract) เนื่องจากบริษัทจะมีภาระที่เพิ่มมากขึ้น

นอกจากนี้ยังมีกระบวนการประเมินความเสี่ยงของข้อมูลเพื่อออกแบบการควบคุมข้อมูลให้เหมาะสมกับความเสี่ยง รวมถึงมีการจำกัดการเข้าถึงข้อมูลส่วนบุคคลให้เฉพาะผู้ที่มีความจำเป็นเท่านั้นสามารถเข้าถึงได้และเข้าถึงในข้อมูลที่มีความจำเป็นเท่านั้น และจัดให้มีมาตรฐานการรักษาความปลอดภัยของข้อมูลแต่เนื่องจากกฎหมายไม่ได้กำหนดมาตรฐานที่ชัดเจน ในปัจจุบันจึงยึดมาตรฐานของทางไอที ตาม ISO 27001 เป็นหลัก รวมถึงออกแบบส่วนงานหลังบ้านคือระบบที่คอยดูแลเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูล และการแจ้งเหตุการรั่วไหลภายใน 72 ชั่วโมง อีกทั้งต้องจัดให้มีกระบวนการตรวจสอบการปฏิบัติตามแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบขององค์กร เช่น หน่วยงานตรวจสอบภายใน หน่วยงานกำกับดูแลกิจการ หรือทีมตรวจสอบการปฏิบัติตามกฎหมายที่บริษัทตั้งขึ้น

ส่วนเรื่องการขอความยินยอมจากลูกค้าเป็นหน้าที่ของการตลาดที่จะออกแบบการให้บริการและเนื้อหาของการขอความยินยอม (Consent) ที่จงใจให้ลูกค้ารู้สึกว่าได้ประโยชน์จากการให้ข้อมูลหรือหากจะมีการจูงใจด้วยสิ่งของอื่นใดต้องพิจารณาถึงต้นทุนที่ต้องจ่ายว่าคุ้มหรือไม่เพราะลูกค้าสามารถถอนความยินยอมได้

“ตอนนี้คุณมีข้อมูลของลูกค้าเยอะต้องทบทวนว่าในนี้มีข้อมูลที่ไม่จำเป็นรึป่าวในข้อมูลส่วนบุคคลเพราะว่าถ้าคุณเก็บข้อมูลที่ไม่จำเป็นคุณก็ตกอยู่ในความเสี่ยง ถ้าคุณจะเก็บข้อมูลที่มันเป็นข้อมูลอ่อนไหวหรือป่าว ถ้าใช้คุณต้องขอความยินยอม ” (Executive Management, RK1)

“การทำการประเมินความเสี่ยงข้อมูล (Data Risk Assessment) ข้อมูลแต่ละประเภทที่เก็บระดับความเสี่ยงของมันมีประมาณไหน เพื่อที่จะดูมาตรการของการควบคุมว่าเราควรจะมีระดับการควบคุมของเอกสารพวกนั้นอย่างไรบ้าง ” (Management, RK2)

“เจ้าหน้าที่ธนาคารมีการติดต่อกับลูกค้าก็ต้องเห็นข้อมูลลูกค้า เพราะฉะนั้นก็ต้องมีมาตรการดูแล ก็ต้องตรวจสอบติดตามให้ดีกว่าใครเข้าถึงข้อมูลอะไร ไม่เกินเลย ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC3)

“ทำยังไงก็ได้ให้ใช้ข้อมูลน้อยกว่าที่เคยใช้แต่ได้ผลลัพธ์มากกว่าที่เคยได้ ให้มันมีประสิทธิภาพมากขึ้น ไม่ใช่เก็บไว้ 8 อย่าง ใช้ 3 อย่าง ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ดังนั้นมันจะเป็นเรื่องการออกแบบการให้บริการ (Service Design) บริษัท องค์กร นักการตลาด จะออกแบบการขอการขอความยินยอม (Consent) ที่ไม่กระทบกับกระบวนการทำงานทั้งหมดให้ได้ นั่นคือสิ่งที่ต้องไปนั่งแก้กัน จะทำยังไงให้คนอยากให้ข้อมูล ง่ายที่สุด เร็วที่สุด แม่นยำที่สุด ด้วยตัวเองให้ได้ ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ก็ต้องมีศิลปะ ถ้าอย่างได้ข้อมูลเขามาทำอะไรที่เป็นประโยชน์กับตัวเอง แล้วเจ้าของข้อมูลในหลายกรณีที่ให้ความยินยอม (Consent) เขาก็ไม่ได้ประโยชน์อะไรเลย เราจะสนใจเขาด้วยอะไร การมีสิ่งของของใจในการให้ลูกค้าให้ความยินยอม ก็ต้องยอมรับต้นทุนตรงนั้นด้วย เพราะข้อมูลมันก็ถอนได้ ” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

ท้ายที่สุดแล้วกระบวนการปฏิบัติการทั้งหมด ขึ้นอยู่กับหลักการ 3 ประการ คือ 1) ความจำเป็น (Necessity) ข้อมูลใช้ได้ต่อเมื่อมีความจำเป็นเท่านั้น 2) ความโปร่งใส (Transparency) คือ ใช้อย่างโปร่งใส สามารถแจ้งได้ว่าเอาข้อมูลไปใช้ประโยชน์อย่างไร และเป็นธรรมในส่วนที่ให้ผู้บริโภคให้ความยินยอมด้วย 3) ความปลอดภัย คือ ระบบต้องมีความปลอดภัย เพราะไม่เช่นนั้นกระบวนการทุกอย่างที่ออกแบบมาก็จะไม่เกิดประโยชน์ถ้าข้อมูลหลุดออกไป

4.3.1.3 เทคโนโลยี (Technology)

จากการสัมภาษณ์ พบว่า เทคโนโลยีเป็นปัจจัยหนึ่งที่เข้ามาช่วยในการปรับใช้พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ในเรื่องต่าง ๆ เช่น ช่องทางการขอความยินยอม ลดความผิดพลาดจากการปฏิบัติงานของคน (Human Error) Tracking ข้อมูลได้ เรียกดูกิจกรรมการไหลของข้อมูล (Data Log Activity) และตรวจสอบการรั่วไหลของข้อมูลได้ง่ายกว่าข้อมูลที่เป็น Hard Copy ปัจจุบันบริษัทมีการลงทุนในเทคโนโลยีในส่วนที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล การ

บริหารจัดการการขอความยินยอม (Consent Management) และเตรียมลงทุนในส่วนของการบริหารจัดการเกี่ยวกับสิทธิของเจ้าของข้อมูล ซึ่งจะต้องรอความชัดเจนของกฎหมายอย่างเรื่องของสิทธิในการโอนข้อมูล (Right to Data Portability) ว่ากฎหมายมีความมุ่งหวังให้บริษัทดำเนินการในลักษณะใดจึงจะมีการลงทุนครั้งใหญ่เกี่ยวกับเรื่องดังกล่าว ส่วนในปัจจุบันก็ยังไม่เห็น Software ใดที่ธนาคารเห็นว่าการครอบคลุมการปฏิบัติงานตาม PDPA ได้อย่างสมบูรณ์จึงยังไม่มีการลงทุนในส่วนนี้ แต่หากเห็นว่า Software ใดมีประสิทธิภาพมากพอบริษัทก็พร้อมที่จะลงทุน

แต่อย่างไรก็ตามการใช้เทคโนโลยีเข้ามาช่วยในการปฏิบัติงานก็ต้องพิจารณาถึงการดำเนินงานขององค์กรด้วยว่าเป็นไปในทิศทางมุ่งเน้นในเทคโนโลยีหรือไม่ หากไม่ได้เป็นไปในทิศทางเทคโนโลยีมากนักก็สามารถใช้กระบวนการอื่นเข้ามาทดแทนการให้เทคโนโลยีได้และอีกปัจจัยที่สำคัญคือเรื่องงบประมาณของบริษัทที่จะลงทุนในเรื่องเหล่านี้ด้วย เนื่องจากธนาคารมีประเด็นปัญหาและความเสี่ยงที่หลากหลายอาจจะต้องพิจารณาจัดลำดับความสำคัญในการลงทุนด้วย อีกทั้งต้องพิจารณาเพิ่มด้วยว่าการใช้เทคโนโลยีเข้ามาช่วยในการทำงานให้มีความสะดวกมากขึ้นก็จริง แต่ก็แลกมาด้วยความเสี่ยงจากการรั่วไหลของข้อมูลที่มีผลกระทบมหาศาล ดังนั้นเพื่อบริหารความเสี่ยงนี้จึงต้องมีการลงทุนทางด้านการรักษาความปลอดภัยเพิ่มขึ้นตามความเสี่ยงที่เพิ่มมากขึ้น

“มันขึ้นอยู่กับขนาดขององค์กรด้วย และวัฒนธรรมขององค์กรว่าเขาใช้ระบบงานหรือว่า IT มากน้อยแค่ไหน แต่ละที่ก็มีความแตกต่างในเรื่องของ Operation เช่น บางธนาคารที่ไปทางด้านดิจิทัลเยอะ ๆ อันนั้นเขาก็จะกระทบการลงทุนในเทคโนโลยีเยอะ ของเราอาจจะมีการเพิ่มขึ้นของระบบ อย่างระบบบริหารจัดการการขอความยินยอม (Consent Management) และระบบการบริหารจัดการสิทธิของเจ้าของข้อมูลมากกว่า (Data Subject Right Management)” (Staff, RK4)

“พัฒนาแอปให้ก็ต้องเรียกไอทีมาคุยทำได้มัยยังงี้ เสร็จก็ต้องมาดูว่าบริษัทมีงบประมาณสำหรับ PDPA มัย ก็ต้องมาจัดลำดับความสำคัญหรือพิจารณาแล้วกลุ่มลูกค้ากลุ่มนี้ไม่น่าจะฟ้องร้องธนาคารก็พักไปก่อน ความเสี่ยงต่ำก็อาจจะไปทำให้ที่หลังแต่อาจจะไปรวมกับเรื่องอื่น ๆ” (Executive Management, RK1)

“ยังใช้ เทคโนโลยีมากขึ้นเท่าไรความปลอดภัยก็ต้องสูงตามมากขึ้นเท่านั้น นั่นแหละคือต้นทุนที่จะเกิดขึ้น” (Executive Management, RK6)

“อันนี้ขึ้นอยู่กับงบประมาณ คือถ้าอยากสบายก็ไปใช้เทคโนโลยี Automate ถ้าไม่มีเงินก็ Manual มันทำได้หมด ขึ้นอยู่กับความยุ่งยากและเงินในกระเป๋า ถ้ามีเงิน Automate มันดีอยู่แล้ว เทคโนโลยีมันก็เข้ามาช่วยได้นั้น ถ้ามีเงินก็ดีเลย” (Management, RK5)

“เทคโนโลยีทำให้การที่จะปฏิบัติตาม PDPA เป็นเรื่องที่ยง่ายขึ้น แน่แน่นอน เพราะถ้าไม่มีเรื่องของเทคโนโลยีนะ ตัวกฎหมายนี้ไม่เกิด มันมาพร้อมกับเทคโนโลยี” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC4)

ท้ายที่สุดแล้วการทำงานแบบสอดประสานกันไปได้ทั้ง 3 องค์ประกอบในองค์ประกอบที่สำคัญที่สุดก็คือเรื่องของคนที่ต้องเน้นย้ำอย่างหนัก แม้ว่าจะมีการวางแผนและออกแบบกระบวนการมาอย่างดีและมีการลงทุนในเทคโนโลยีที่เหมาะสมอย่างเต็มที่แล้วซึ่งเป็นจุดที่บริษัทสามารถควบคุมได้ทั้ง 2 องค์ประกอบแต่องค์ประกอบสุดท้ายอย่างคนซึ่งเป็นองค์ประกอบที่ควบคุมได้ยากที่สุด ดังนั้นจึงต้องอาศัยการให้ความรู้ จนเกิดความตระหนักรู้ และเกิดเป็นวัฒนธรรมแห่งการคุ้มครองข้อมูลส่วนบุคคลควบคู่กับการควบคุมตรวจสอบจากหน่วยงานภายในองค์กรจึงจะทำให้บริษัทบรรลุวัตถุประสงค์การปฏิบัติตามกฎหมายอย่างแท้จริง แต่อย่างไรก็ตามทั้ง 3 องค์ประกอบนี้ควรอยู่บนหลักของการหาแนวทางที่ใช้ต้นทุนน้อยที่สุดแต่สามารถปฏิบัติตามที่กฎหมายกำหนดอย่างน้อยที่สุดหากไม่ได้เป็นการสร้างรายได้เพิ่มก็ถือว่าไม่ทำให้เกิดค่าใช้จ่ายที่มากเกินไปจากค่าปรับและที่มากไปกว่านั้นคือชื่อเสียงของบริษัทที่ไม่สามารถประเมินมูลค่าได้ แต่หากจะเหนือไปกว่านั้นคือการนำเรื่องมาตรฐานการคุ้มครองข้อมูลของบริษัทไปสร้างโอกาสในการแข่งขันได้

“ความเสี่ยงที่ข้อมูลรั่วไหลมันก็ตั้งแต่ พันล้าน ถึง ห้าพันล้าน นั่นคือการเกิดครั้งเดียวแต่ถ้ามันเกิดถี่ ๆ คุณไปกี่ครั้ง เมื่อธนาคารรู้แล้วมีโอกาสมันจะสูญเสียค่าใช้จ่ายและในส่วนรายรับเราก็รู้การแข่งขันในตลาดสูงส่วนแบ่งการตลาดเราอยู่ตรงไหนเราอาจจะเดินได้เสียใหญ่แต่มันอาจจะไม่พอมารอดเซย์ค่าใช้จ่ายเหล่านั้น เพราะฉะนั้นเรารู้ว่าลูกบอลสองก้อนมันไม่เท่ากัน การป้องกันสำคัญที่สุดกันให้ได้มากที่สุด เพื่ออย่างน้อยรายได้ที่มีมันจำกัด มันจะได้ไม่ต้องเจียดมาจ่ายค่าใช้จ่ายอะไรแบบนี้ เพราะฉะนั้นการสร้างการตระหนักรู้ในคนสำคัญที่สุด” (Executive Management, RK7)

“แน่นอนว่า ณ วันนี้ทุกคนมีต้นทุนที่เพิ่มขึ้นใครเริ่มหาทางปรับให้ต้นทุนตรงนี้ให้ต่ำลงเกิดรายได้หรือกำไรขึ้นตามมา โดยการใช้ข้อมูลให้เป็นประโยชน์ในการเพิ่มโอกาสการแข่งขัน ซึ่งเป็นการใช้ข้อมูลตามกฎหมายใหม่ด้วย” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“ถ้าเราจะมองให้เรื่องนี้เป็นอาวุธในการแข่งขันได้ มันน่าจะต้องไปในทิศทางที่เราต้องได้ Consent มากกว่าคนอื่น ยังไม่นับว่าเราจะสามารถ PR ลูกค้าถ้าลูกค้ายืนยันในตัวเรา ลูกค้านี้แหละที่จะเป็นอาวุธของเราบอกว่าป็นลูกค้าของเจ้านี้ไม่เห็นเคยโดนแบบนี้เลยเขาไม่เคยโทรมารบกวนฉันเลยแค่นี้ก็ถือว่าเป็นอาวุธแล้ว” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

“โจทย์ของธุรกิจก็คือเราจะปรับใช้กฎหมายยังไงให้ต้นทุนมันต่ำที่สุด อยู่ในระดับที่ทำตามกฎหมาย มันมีทั้งภาระที่ต้องทำ บางอันมันเป็นโจทย์ให้บริษัทเลือกว่าแบบไหนดีที่สุดสำหรับองค์กรแล้ว ต้นทุนต่ำสุด” (ผู้เชี่ยวชาญกฎหมาย, RGL1)

“การแปลงเอาเรื่องนี้มาเป็นประโยชน์ธุรกิจ เช่น พวกที่เอาเรื่องนี้ไปโปรโมทว่ามีการคุ้มครองข้อมูลส่วนบุคคลอย่างดี พวกนี้มันจะเกิดขึ้นในช่วงต้น ๆ ของการบังคับใช้กฎหมาย ช่วงที่มาตรฐานมันยังไม่ถึงตอนที่มันยังไม่รู้ว่าแต่ละบริษัทเป็นยังไง เราก็ต้องวิ่งไปเคลมมาตรฐานก่อนคนที่ไปก่อนก็มีโอกาสมากกว่า” (ผู้เชี่ยวชาญกฎหมาย, RGL2)

4.3.2 ปัจจัยสภาพแวดล้อมภายนอกองค์กร

4.3.2.1 ลูกค้า (Customer)

จากการสัมภาษณ์ พบว่า ณ ปัจจุบันกลุ่มลูกค้าส่วนใหญ่ยังไม่ตื่นตัวกับกฎหมายเท่าไรนักหรือยังอาจจะมีเข้าใจที่ไม่ครบถ้วนหรือไม่ตรงกันกับบริษัทในบางส่วน เนื่องจากการให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยที่ยังไม่มากนัก ไม่ได้มีการปลูกฝังกันมาอย่างยาวนานเหมือนในต่างประเทศ จึงเป็นเรื่องที่ใหม่สำหรับคนไทย แต่อย่างไรก็ตามลูกค้า คือ หัวใจสำคัญของการทำธุรกิจให้ประสบความสำเร็จ ดังนั้นจึงมีแนวทางในการปฏิบัติต่อลูกค้าที่สำคัญคือ การสื่อสาร (Communication)

โดยมีการออกแบบการขอความยินยอม (Consent) ซึ่งมีเนื้อหา (Content) ที่ทำให้ลูกค้ารู้สึกถึงประโยชน์ของการให้ความยินยอมและเข้าใจสิทธิของลูกค้าในฐานะเจ้าของข้อมูลพร้อมกับสิทธิของบริษัทในการเก็บข้อมูลของลูกค้าตามฐานการประมวลอื่น ๆ ที่ได้รับยกเว้นไม่จำเป็นต้องขอความยินยอมเพื่อความเข้าใจที่ตรงกันระหว่างบริษัทและลูกค้าลดการฟ้องร้องซึ่งจะทำให้ลูกค้ามีความเต็มใจและยินยอมที่จะให้ข้อมูลแก่บริษัท นอกจากนี้ยังต้องสื่อสารถึงมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความเชื่อมั่นให้กับลูกค้าในการใช้บริการและการยินยอมให้ข้อมูล อีกทั้งยังต้องสื่อสารให้ลูกค้าตระถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูล

“ทำอย่างไรให้ลูกค้ามองว่าการให้ความยินยอม (Consent) เป็นสิ่งที่ดี มองว่า Consent เป็นเพื่อนเพราะว่าจะมาช่วยสกรีนนำผลิตภัณฑ์ที่เหมาะสมไปหาคุณได้” (Executive Management, RK6)

“สำคัญที่สุดคือโทนของคนที่ให้บริการ หรือ Sales ทำยังไงที่จะสามารถสื่อสารไปได้ว่าการขอความยินยอม (Consent) เป็นเพื่อน ซึ่งมันก็เป็นความท้าทายที่เราต้องพัฒนากันต่อมันขึ้นอยู่กับความตระหนักรู้ (Awareness) ของลูกค้าด้วยก็ต้องใช้วาทศิลป์ของสาขา เราก็ต้องสื่อสารให้เข้าใจเพราะขึ้นอยู่กับการรับรู้ของลูกค้าเหมือนกัน ถ้าเขาเข้าใจก็จะให้แต่ถ้าคนที่ไม่เข้าใจเขาก็จะตั้งการ์ดเลยไม่เอา” (Executive Management, RK7)

“ผู้บริโภคไม่ได้เข้าใจว่ากฎหมายมันมีเกณฑ์พิจารณาตัวหนึ่งที่ชื่อว่า Legitimate Interest อะไรก็ตามถ้าตีว่าเป็นฐานนี้ก็ไม่ต้องขอความยินยอมเพราะมันความเข้าใจที่ขัดแย้งกันมันเกิดขึ้นแล้ว ทำอย่างไรให้ลูกค้ารู้ว่ามันมีกติกาหนึ่งนะที่เราตัดสินใจร่วมกัน ไม่ใช่อะไรก็

ฟ้อง หรือมองว่าคำว่าคุ้มครองมันแปลว่าใครไม่สามารถทำอะไรกับฉันได้ ฉันสามารถฟ้องได้ กลายเป็นว่าบริษัทต้องมาจัดการกับเรื่องลูกค้าฟ้องร้องเรื่องละเมิดที่เขาคิดว่าละเมิดข้อมูลส่วนบุคคล แต่จริง ๆ แล้วไม่ใช่” (Executive Management, RK6)

“ตอนนี้เราสร้างความเชื่อมั่นไปแล้วว่าทุกคนมีสิทธินี้เหมือนเป็นการสร้างความคาดหวังใหม่ที่เกิดขึ้นกับลูกค้าที่มาใช้บริการพอมันเป็นเรื่องของความคาดหวังมันก็จะส่งผลต่อเรื่องของความยินดีที่จะจ่ายกับยินดีที่จะให้ข้อมูล” (ผู้เชี่ยวชาญกฎหมาย, RGL3)

4.3.2.2 คู่ค้า (Supplier/Vendor)

การพิจารณาคัดเลือกผู้ให้บริการรายใหม่และการต่อสัญญาเก่าของธนาคารจะต้องเพิ่มหลักเกณฑ์เกี่ยวกับการให้บริการที่ได้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายกำหนดพร้อมจัดทำสัญญาการประมวลผลข้อมูล รวมถึงมีการตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการรายนั้น ๆ ด้วย นอกจากนี้การจ้างงานในลักษณะที่เกี่ยวข้องกับข้อมูลส่วนบุคคลธนาคารจะดึงกลับมาทำเองให้มากที่สุดให้ข้อมูลส่วนบุคคลไหลออกไปนอกธนาคารให้น้อยที่สุดเพื่อเป็นการลดความเสี่ยง

“Partner ที่ไม่สามารถทำตาม PDPA เราก็จะไม่ทำธุรกรรมด้วย” (Executive Management, RK1)

“เราก็ต้องมั่นใจว่าตั้งแต่วันแรกที่เรามีสัญญากับ Vendor เขามี PDPA DNA อยู่แล้ว ตั้งแต่นั้นมันเป็นการลดความเสี่ยง” (Executive Management, RK7)

“ธนาคารพยายามดึงกลับมาทำเอง พยายามไม่จ้างคนนอกถ้าไม่จำเป็น เพราะว่าข้อมูลธนาคารเป็นข้อมูลที่มีความอ่อนไหว เช่น สมมุติมีข้อมูลแล้วแบ่ง segmentation จ้าง Outsource ไปทำการตลาดต่อให้ แต่คนที่ทำหน้าที่ให้การวิเคราะห์ข้อมูลทั้งหมดเป็นธนาคาร” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC1)

“เราควรจะต้องตรวจสอบ ถ้าผู้ประมวลผลข้อมูลเอาข้อมูลของเราไปแล้ว เช่นว่ามีการคัดลอกไปอีก Cloud หนึ่ง มีการทำ Firewall อย่างไรใน Cloud นั้นใครเข้าถึงได้บ้าง มีต่อต่อไปที่ไหนอีกหรือไม่ ควรจะตรวจสอบค่ะ ถ้าไม่มีการตรวจสอบความเสี่ยงของธนาคารเต็ม ๆ” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC2)

4.4 แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตาม ข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า กลุ่มธุรกิจธนาคารพาณิชย์และผู้เชี่ยวชาญมองว่าแนวทางการพัฒนาองค์กรเพื่อตอบรับกับการปฏิบัติตามข้อบังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. 2562 ซึ่งเป็นการหาจุดสมดุลในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เป็นภาระของภาคธุรกิจมากเกินไป โดยต้องเป็นความร่วมมือกันทั้งภาครัฐและเอกชนในการช่วยกันผลักดันให้เกิดการบังคับใช้กฎหมายที่เป็นประโยชน์อย่างสูงสุดทั้งฝั่งของผู้บริโภคและตัวองค์กรเอง โดยมีประเด็นแนวทางการพัฒนา 3 ประเด็น ดังนี้

4.4.1 มีแนวทางการปฏิบัติงานที่ชัดเจนสำหรับภาคธุรกิจ

จากการสัมภาษณ์ พบว่า เนื่องจากปัญหาการปรับใช้กฎหมายในปัจจุบันเป็นเรื่องของการตีความและรอความชัดเจนจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งในบางเรื่องต้องมีการรอกฎหมายในลำดับรองออกมาจึงจะมีความชัดเจน และมีหลายประเด็นที่ภาคธุรกิจกังวลในวิธีการปฏิบัติงานจริง เช่น เรื่องของสิทธิของเจ้าของข้อมูล (Data Subject Right) โดยเฉพาะเรื่องสิทธิการโอนข้อมูล (Right to Data Portability) ซึ่งจะสามารถปฏิบัติได้จริงอย่างมีประสิทธิภาพก็ต่อเมื่อเรามีการผลักดันให้ประเทศเข้าสู่ดิจิทัลอย่างแท้จริง เรื่องของบริบทของการแจ้งเหตุการณ์ข้อมูลรั่วไหลและเนื้อหาที่เหมาะสมที่บริษัทควรสื่อสารออกไปควรเป็นอย่างไร และมาตรฐานการรักษาความปลอดภัยที่เพียงพอตามข้อกำหนดของกฎหมายควรเป็นอย่างไร เป็นต้น และเนื่องจากกฎหมายฉบับนี้ออกมาเพื่อปรับใช้กับทุกภาคธุรกิจซึ่งในแต่ละธุรกิจก็มีลักษณะการประกอบธุรกิจที่มีความเฉพาะเจาะจงและเงื่อนไขการปฏิบัติงานที่แตกต่างกัน

ดังนั้นจึงควรมีการจัดทำแนวปฏิบัติกลางสำหรับภาคธุรกิจเพื่อให้เป็นมาตรฐานและแนวทางการปฏิบัติงานสำหรับภาคธุรกิจ ที่ได้รับความเห็นชอบจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหน่วยงานกำกับดูแล

นอกจากนี้เห็นควรว่าให้หน่วยงานกำกับดูแลภาคธุรกิจโดยตรงซึ่งหมายถึงธนาคารแห่งประเทศไทย เป็นผู้กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลของธนาคารโดยตรง ส่วนสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหน่วยงานกำกับดูแลของกฎหมายฉบับนี้จะเข้ามากำกับดูแลเพิ่มเติมผ่านธนาคารแห่งประเทศไทย เพื่อสะดวกต่อการกำกับดูแลในภาคธุรกิจและเป็นการลดภาระของหน่วยงานกำกับดูแลที่ต้องดูแลทุกภาคธุรกิจซึ่งมีหลายภาคธุรกิจที่ยังไม่มีหน่วยงานกำกับดูแลโดยตรง

“ความเป็นไปได้ในเชิงปฏิบัติบางเรื่องมันก็ยากต้องรอแนวทางการปฏิบัติมาให้ชัดเจน ซึ่งของธนาคารเราก็มีสมาคมธนาคารไทยที่พยายามทำแนวปฏิบัติออกมาในเชิงภาพรวมของอุตสาหกรรมภาคการเงินว่าจะปฏิบัติอย่างไร หลาย ๆ เรื่องมันก็รอความชัดเจนจากแนวปฏิบัติ พอมันไม่ออกมาก็จะมีปัญหาลักษณะแบบนี้ ดีความเอง ประเมินเอง คิดว่าแบบนั้นใช่ แบบนี้ไม่ใช่” (Management, RK3)

“เรื่องสิทธิในการโอนย้ายข้อมูล (Data Portability) น่าจะเป็นอุปสรรคสำคัญ เมื่อกฎหมายมีผลบังคับใช้แล้ว เผลอ ๆ ผ่านไปอีก 3 -5 ปีเมืองไทยอาจจะยังไม่ได้เกิดสิทธิในการโอนย้ายข้อมูล ในวงการธุรกิจมันจะมีประโยชน์ก็ต่อเมื่อทุกคนเปลี่ยน Identity ของตัวเองจาก Analog เข้าเป็น Digital การทำสิทธิในการโอนย้ายข้อมูลมันจะง่าย อยู่ธนาคารไหนเราส่งข้อมูลกันทางดิจิทัลทั้งหมด พิสูจน์ตัวตนกันที่ธนาคารหนึ่ง อีกธนาคารหนึ่งมาทำข้อมูลต่อเล็กน้อยเท่านั้น ” (Executive Management, RK6)

“ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (Three Regulator) ก็มีการทำงานร่วมกัน แล้วก็กลุ่มสมาคมธนาคารไทยก็ทำเป็นแนวปฏิบัติ (Guideline) เพื่อสุดท้ายแล้วในธุรกิจธนาคารเขาก็จะมี Guideline เป็นแกนกลาง ใครจะปลีกย่อยอะไรก็เป็นอีกเรื่องหนึ่ง แต่ Three Regulator ก็คุยกัน ไม่เฉพาะเรื่องของ PDPA โดยตรงเราคุยกันเรื่อง Data Governance ในขณะที่ PDPA ก็เป็นส่วนหนึ่ง” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR1)

“แบบค์ชาติก็จะเป็นตัวช่วยในการที่ว่าเราตกผลึกแล้วว่าอันไหนที่จะเป็นภาระหรืออุปสรรคต่อภาคธุรกิจธนาคารในการพัฒนาต่อไปเราก็จะไปหารือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและทำเป็นแนวทางปฏิบัติของภาคอุตสาหกรรม เพราะว่าแบบค์ชาติก็มีวิสัยทัศน์ว่าจริง ๆ แล้วการคุ้มครองข้อมูลมันก็โอเคในระดับหนึ่งแต่ก็ต้องไม่ปิดกั้นให้เราไม่สามารถทำธุรกิจได้เลย” (หน่วยงานกำกับดูแลภาคธุรกิจ, RGR5)

“สิ่งหนึ่งที่พยายามจะผลักดันเรื่องนี้ไปที่หน่วยงานกำกับว่าบริบท (Context) คืออะไรที่ต้องแจ้งเหตุ เพื่อจะจำกัดให้มันมีนัยสำคัญจริง ๆ ให้เราสามารถทำงานได้ภายใน 72 ชม. เนื้อหา (Content) แจ้งยังงี้ให้ไม่สร้างความตื่นตระหนกให้กับตลาด” (Executive Management, RK6)

“ในโลกดิจิทัลมันจะปรับปรุง (Stream Line) ได้ดีกว่านี้ มันมีโปรเจกต์หนึ่งของพอคุณจะไปเปิดบัญชีธนาคารนี้แล้วจะไปเปิดบัญชีอีกธนาคารหนึ่งหรือไปขอสินเชื่ออีกธนาคารหนึ่งคุณแค่กดใช้สิทธิโอนบัญชีจากธนาคารหนึ่งไปอีกธนาคารหนึ่งได้ ข้อมูลมัน กรอกให้เรียบร้อยแล้วไม่ต้องมานั่งกดซ้ำ” (Management, RK8)

“เราก็เคยคุยกับสมาคมธนาคารไทย แล้วก็หน่วยงานกำกับดูแลเราโดยตรงอย่างแบบค์ชาติและกลต.ว่าให้เรามี สคส. เข้ามาดูแลกำกับเราเพิ่มเติม เรียกว่าเข้ามาเป็น Super Supervisor ที่กำกับหน่วยงานกำกับเราอีกทีหนึ่ง แปลว่าถ้าหน่วยงานที่กำกับดูแลเรามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของแต่ละภาคธุรกิจแล้ว เขาไม่จำเป็นต้องลงมากำกับดูแลเราโดยตรงเพราะเขาคงไม่สามารถกำกับได้ทุกรูปแบบ เขาก็จะไปกำกับธุรกิจที่ไม่มีผู้กำกับดูแล ในอนาคตทุกธุรกิจจะมี Self Regulatory Organization คือ เรามีมาตรฐานขึ้นมาแล้วทุกคนปฏิบัติตามมาตรฐาน

แล้วกฎหมายที่ออกมาบังคับมันจะน้อยลงเรื่อย ๆ แนวทางในอนาคตมันควรจะเป็นแบบนี้ซะมากกว่า” (Executive Management, RK6)

4.4.2 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริหารและพนักงานภายในองค์กร

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า เรื่องของความรู้ ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จนเกิดความตระหนักรู้ (Awareness) เป็นปัจจัยพื้นฐานสำคัญที่จะทำให้กฎหมายฉบับนี้เกิดประโยชน์อย่างแท้จริงกับผู้บริโภคและภาคธุรกิจ

ในส่วนของผู้บริโภคภาครัฐ หน่วยงานกำกับดูแล และธนาคาร ควรออกมาสื่อสารความเข้าใจเกี่ยวกับกฎหมาย สร้างความตระหนักรู้ (Awareness) เกี่ยวกับข้อมูลส่วนบุคคล รวมถึงสิทธิและประโยชน์ของผู้บริโภคในทิศทางเดียวกัน เพื่อให้ผู้บริโภคเข้าใจถึงสิทธิที่แท้จริงของตน และสิทธิของธนาคารซึ่งจะทำให้เกิดความเข้าใจที่ตรงกันกับธนาคารถึงการใช้สิทธิในข้อมูลส่วนบุคคล ในปัจจุบันผู้บริโภคมักถูกสื่อสารกันถึงสิทธิของลูกค้าในมุมเดียวแต่ไม่ได้สื่อสารถึงสิทธิในฝั่งธนาคาร และในภาคธนาคารเองก็ต้องมีการสื่อสารความรู้ความเข้าใจและสร้างการตระหนักรู้ภายในองค์กรอย่างต่อเนื่องและเพิ่มความเข้มข้นขึ้นให้เกิดเป็นวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคล

“เราบอกออกไปตามสื่อออนไลน์ต่าง ๆ ถึงความหมายของ PDPA สิทธิของเจ้าของข้อมูลคืออะไรและจะได้ประโยชน์อะไรจาก PDPA ถ้าคุณไม่ให้คืออะไร ธนาคารทำอะไรคุณได้มัย รวมถึงสิทธิของสาขาก็จะให้ข้อมูลประมาณนี้ ซึ่งเราก็ต้องมีการสื่อสารเรื่อย ๆ เราก็มีการคุยกับแบงค์ชาติว่าถ้าแต่ละธนาคารต่างคนต่างพูดมันก็จะไม่ชัด ให้หน่วยงานกำกับดูแล นำร่องมาก่อน ดบด้วยแบงค์ชาติ พูดให้เหมือนกัน พอธนาคารพูดเขาก็จะเคยได้ยินมาแล้วมันไม่ใช่เรื่องใหม่ ความกลัว ความแพนิคมันก็จะน้อยลง การให้ความร่วมมือเป็นเรื่องปกติมันก็จะเกิดขึ้นได้เร็วกว่าให้ต่างคนต่างพูด” (Executive Management, RK7)

“เรามองว่ามันเกี่ยวข้องกับประชาชน ประชาชนทุกคนควรที่จะต้องเข้าใจผ่านกลไกอะไรบ้าง ผ่านกลไกการศึกษา ตั้งแต่ประถม มัธยม” (ผู้เชี่ยวชาญด้านบริหารข้อมูล, RGC4)

“ทางภาครัฐจะต้องให้ความรู้กับผู้บริโภคด้วยเราพูดไปในมุมมองของผู้ประกอบธุรกิจเขาก็ต้องมองว่าเราต้องการจะเอาข้อมูลเขาไปทำอะไรสักอย่างแหละ คนที่พูดละมีน้ำหนักที่สุดก็คือหน่วยงานกำกับต้องมาบอกแล้วว่าการให้ข้อมูลพวกนี้มันไม่ใช่เรื่องเสียหายมันเป็นเรื่องดีเสียมากกว่า ทำยังไงให้มันดูแล้วไม่น่ากลัว ให้เป็นเรื่องของการให้ความร่วมมือ” (Executive Management, RK6)

“ยุโรปคนเขาได้รับการให้ความรู้ความเข้าใจถึงสิทธิของเจ้าของข้อมูลยุโรปเขามี Directive มาเป็น 20 ปี ก่อนที่เขาจะขยับมาเป็น GDPR” (Management, RK8)

“บทบาทของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่หนึ่งคือ ส่งเสริมให้ประชาชนตระหนักถึงข้อมูลส่วนบุคคล เพราะฉะนั้นเขาอาจจะมีการบอกของการให้ความรู้ ในภาคประชาชนว่าสิทธิของตนเองเป็นอย่างไรจะปกป้องอย่างไร จะใช้อย่างไร” (ผู้เชี่ยวชาญด้าน บริหารข้อมูล, RGC4)

“ใช้ว่าส่วนหนึ่งคนไทยไม่ได้ตระหนักถึงแต่อีกส่วนก็เพราะมันไม่มีการปูพื้นมา ด้วย หลังจากนั้นไปอีกสัก 20 ปี คนไทยอาจจะมองว่า PDPA เป็นส่วนหนึ่งของชีวิตก็เป็นไปได้” (Management, RK5)

4.4.3 การควบคุม ติดตาม และประเมินผลการปฏิบัติงานหลังมีการปรับใช้จริงเพื่อ ปรับปรุงกระบวนการอย่างต่อเนื่อง

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า หลังจากมีการปรับใช้กฎหมายอย่างเต็ม รูปแบบและธนาคารได้ดำเนินการตามกระบวนการที่ได้ออกแบบไว้แล้วจะต้องมีกระบวนการ ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติงาน เพื่อให้ทราบว่ากระบวนการที่วางไว้มีปัญหา อุปสรรคในการปฏิบัติงานหรือไม่ ทั้งในมุมของการปฏิบัติตามกฎหมายและความพึงพอใจของลูกค้า นอกจากนี้ยังเป็นการควบคุมการปฏิบัติงานให้เป็นไปตามกระบวนการที่ออกแบบไว้และเพื่อให้เกิด การปรับปรุงกระบวนการอย่างต่อเนื่อง โดยปรับปรุงและพัฒนาควบคู่ไปกับธรรมาภิบาลข้อมูล (Data Governance)

“DPO เขาก็สามารถบอกได้ว่ามันควรจะมียอดดีทิลโปรแกรมแบบนี้ในแต่ละพื้นที่ นั้น แล้วเขาก็ส่งต่อให้ฝ่ายกำกับดูแล ให้ตรวจสอบภายในได้ถึงเวลาจริง ๆ ที่จะตรวจสอบเรื่อง PDPA ก็ต้องเป็น Risk Base ที่ไหนความเสี่ยงมากก็ตรวจสอบมากที่ไหนความเสี่ยงน้อยก็อาจจะไม่ต้อง ตรวจสอบอะไร” (Executive Management, RK1)

“หลังจากปรับใช้จริงประเด็นเรื่อง PDPA เวลาที่ออกดีทิลลงไปตรวจสอบก็จะเป็น ส่วนหนึ่งของการตรวจสอบเป็นความเสี่ยงหนึ่งที่เขาจะลงไปดู กระบวนการกำหนดไว้แบบนี้ แล้วคุณ ทำตามนั้นรึป่าว” (Staff, RK4)

“เราเตรียมพร้อมไว้แล้วแต่ในแง่ของการใช้จริงก็ยังไม่รู้ว่ามันจะเกิดปัญหาอะไร หลักจากการที่ใช้จริงไปแล้ว 6 เดือน ปีหนึ่งมันอาจจะต้องมาปรับ ต้องมาประเมินว่าต้องปรับแก้ ตรงไหนทั้งในมุมของการปฏิบัติตามกฎหมาย ทั้งความพึงพอใจของลูกค้า แล้วก็รอกฎหมายลูกด้วย ถ้าเราทำไปตามนี้ แล้วกฎหมายลูกออกมาผ่อนคลายนั่นที่เราทำมันมากไปเราก็มารับ” (Management, RK5)

“การทำเรื่อง PDPA มันก็จะถูกปรับใช้ไปกับเรื่องจำแนกประเภทข้อมูล (Data Classification) กับธรรมาภิบาลข้อมูล (Data Governance) ด้วย เรียกว่าเป็นการเปลี่ยนครั้งใหญ่ ในเรื่องของข้อมูล ซึ่งถ้าเรารักษาระบวนการและความเร็ว (Speed) แบบนี้ไปได้เรื่อย ๆ มันจะเป็น

ข้อดีเวลาเราจะทำอะไรใหม่ ๆ ในเรื่องที่เกี่ยวข้องกับข้อมูล เช่น เรื่องดิจิทัลมันจะช่วยในเรื่องของการสร้างมาตรฐานของทุกฟังก์ชันเข้าด้วยกัน” (Executive Management, RK1)

ดังนั้นสรุปได้ว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะเป็นประโยชน์ต่อทั้งผู้บริโภคและภาครัฐกิจเพียงแค่การออกกฎหมายอย่างเดียวไม่เพียงพอต้องมีความตระหนักรู้ของทั้งคนในองค์กรและผู้บริโภค ภาครัฐและภาคเอกชนได้ให้ความรู้แก่กลุ่มคนเหล่านั้นอย่างเพียงพอเหมาะสม เกิดการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชนอย่างแท้จริง มีแนวปฏิบัติในภาครัฐกิจที่เป็นมาตรฐานเดียวกัน และมีกระบวนการควบคุม ติดตาม และประเมินผลเพื่อปรับปรุงกระบวนการภายในองค์กรอย่างต่อเนื่อง



บทที่ 5

สรุปผลวิจัย อภิปรายผลและข้อเสนอแนะ

การสรุปและอภิปรายผลการวิจัยเรื่องผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศไทย เป็นการอภิปรายผลการวิจัยเชิงคุณภาพโดยการสัมภาษณ์เชิงลึกกับผู้บริหารและผู้ปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคารและผู้เชี่ยวชาญในการด้านกฎหมาย ด้านบริหารจัดการข้อมูล หน่วยงานกำกับดูแลภาคธุรกิจ โดยเนื้อหาจะครอบคลุมประเด็นหลัก ดังนี้

- 5.1 การสรุปและอภิปรายผลการวิจัย
- 5.2 ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์
- 5.3 ข้อจำกัดของงานวิจัย
- 5.4 ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

5.1 การสรุปและอภิปรายผลการวิจัย

การวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อศึกษาผลกระทบจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีต่อธุรกิจธนาคารพาณิชย์ในประเทศพบประเด็นสำคัญต่าง ๆ ตามวัตถุประสงค์งานวิจัยดังต่อไปนี้

- (1) ผลกระทบของธุรกิจธนาคารพาณิชย์จากข้อบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (2) แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคล ภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (3) แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5.1.1 ผลกระทบของธุรกิจธนาคารพาณิชย์จากข้อบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผลกระทบของธุรกิจธนาคารพาณิชย์สามารถจำแนกออกเป็น 2 ประเด็น คือ

- 1) ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ
- 2) ผลกระทบในระดับองค์กรจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5.1.1.1 ผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อภาพรวมของภาคธุรกิจธนาคารพาณิชย์ทั้งในเชิงบวกและเชิงลบ โดยมีรายละเอียด ดังนี้

(1) ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงบวก

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมีความเห็นเป็นไปในทิศทางเดียวกันถึงผลกระทบเชิงบวกต่อภาคธุรกิจธนาคารพาณิชย์จาก พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือ การเพิ่มโอกาสการแข่งขันในระดับสากล เสริมสร้างความเชื่อมั่นและความแข็งแกร่งให้กับภาคธุรกิจและคุณภาพของข้อมูลส่วนบุคคลที่เพิ่มขึ้น

โดยเห็นว่าการเพิ่มโอกาสการแข่งขันในระดับสากลนั้นเกิดจากกฎหมายสร้างให้เกิดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามมาตรฐานในระดับสากล เนื่องจากการโอนข้อมูลออกนอกประเทศต้องสามารถมั่นใจได้ว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลในระดับเดียวกัน รวมถึงการสร้างความแข็งแกร่งของภาคธุรกิจธนาคารในมุมของความมั่นคงความปลอดภัยในข้อมูลและเป็นการสร้างความเชื่อมั่นให้กับผู้บริโภคในการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ข้อมูลส่วนบุคคลจะมีคุณภาพมากขึ้นจากการที่ผู้บริโภคยินยอมที่จะเปิดเผยข้อมูลที่แท้จริงและถูกต้อง ซึ่งเป็นการเพิ่มประสิทธิภาพในการบริหารจัดการข้อมูลของธนาคารในยุคที่ข้อมูลมีค่ามากกว่าน้ำมัน

(2) ผลกระทบต่อภาคธุรกิจธนาคารพาณิชย์ในเชิงลบ

พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบในเชิงลบต่อภาคธุรกิจ 2 เรื่อง ประกอบด้วย 1) เกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาด 2) การใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม โดยมีรายละเอียด ดังนี้

1. เกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาด

กลุ่มผู้ปฏิบัติงานภาคธนาคารมองว่าเนื่องจากแต่ละธนาคารมีการพิจารณาแนวปฏิบัติตามกลยุทธ์และนโยบายของบริษัท ซึ่งในปัจจุบันธนาคารถูกแบ่งออกเป็น 2 กลุ่ม คือ 1) กลุ่มที่ตีความกฎหมายอย่างเคร่งครัด (Conservative) โดยจะเน้นการขอความยินยอม (Consent) และการปฏิบัติตามสัญญา (Contract) และ 2) กลุ่มที่ตีความโดยยึดประโยชน์ธุรกิจเป็นหลักเน้นใช้หลักการประโยชน์อันชอบธรรม (Legitimate Interest) ซึ่งหากบริษัทใหญ่ที่มีส่วนแบ่งทางการตลาดค่อนข้างสูงเลือกปฏิบัติไปในทิศทางใดก็จะกลายเป็นการสร้างแนวปฏิบัติให้กับอุตสาหกรรม เพราะลูกค้าโดยส่วนใหญ่ของตลาดเกิดความคาดหวังและสร้างเป็นมาตรฐานของภาค

ธุรกิจซึ่งจะมีการเรียกร้อยมาตรฐานตามการให้บริการของบริษัทใหญ่และอาจเป็นภาระกับบริษัทขนาดกลางและขนาดเล็กในตลาด

2. การใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมองว่ากฎหมายจะกลายเป็นอุปสรรคต่อการดำเนินธุรกิจหากเจ้าของข้อมูลใช้สิทธิที่ไม่เหมาะสม ซึ่งเกิดจากปัจจัย 2 ประการ ได้แก่ การใช้สิทธิของเจ้าของข้อมูลอย่างรู้เท่าไม่ถึงการณ์จากความไม่เข้าใจกฎหมาย และการใช้กฎหมายเป็นเครื่องมือโจมตีธนาคาร

- การใช้สิทธิของเจ้าของข้อมูลอย่างรู้เท่าไม่ถึงการณ์จากความไม่เข้าใจกฎหมายเนื่องจากกฎหมายให้การคุ้มครองข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูลค่อนข้างมากซึ่งหากหน่วยงานกำกับดูแลตีความกฎหมายอย่างเคร่งครัดเกี่ยวกับสิทธิของเจ้าของข้อมูล ประกอบกับความรู้ความเข้าใจเกี่ยวกับกฎหมายและการคุ้มครองข้อมูลส่วนบุคคลของคนไทยยังไม่เป็นที่แพร่หลายมากนัก จึงอาจทำให้เกิดการใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสมและเป็นภาระแก่ภาคธนาคาร เช่น ลูกค้านำข้อมูลส่วนบุคคลโดยที่ไม่ทราบว่าธนาคารสามารถเก็บข้อมูลส่วนบุคคลของลูกค้าบนฐานกฎหมายอื่นได้ เกิดความเข้าใจที่ไม่ตรงกันกับธนาคารและเกิดการฟ้องร้อง ซึ่งทำให้ธนาคารต้องเสียเวลาในการตรวจสอบและจัดการกับข้อร้องเรียนต่าง ๆ ที่เกิดจากการความไม่เข้าใจกฎหมายของลูกค้า หรือแม้กระทั่งหากเกิดกรณีลูกค้าเกิดความวิตกกังวลกับการแจ้งเหตุข้อมูลรั่วไหล (Data Breach) ซึ่งหากหน่วยงานกำกับดูแลกำหนดเนื้อหาในการแจ้งที่ทำให้เกิดความตื่นตระหนกแก่ผู้บริโภคอาจเกิดเหตุการณ์ที่ผู้บริโภคระดมกันขอถอนความยินยอม ซึ่งทำให้ภาคธุรกิจจะไม่มีข้อมูลลูกค้า เป็นต้น

- การใช้กฎหมายเป็นเครื่องมือโจมตีธนาคาร จากกลุ่มเจ้าของข้อมูลที่ไม่ประสงค์ดีกับธนาคาร หลังจากที่มีการประกาศใช้กฎหมายกลุ่มธุรกิจธนาคารเริ่มมีกลุ่มคนที่พฤติกรรมสุมเสี่ยงที่ทำให้เกิดความเสี่ยงต่อการถูกฟ้องร้อง เช่น การส่งอีเมลเข้ามาแจ้งข้อมูลส่วนบุคคลกับธนาคารโดยไม่ได้เป็นลูกค้าหรือเข้ามาขอใช้สิทธิลบข้อมูลส่วนบุคคลโดยที่ธนาคารไม่มีข้อมูลเนื่องจากกฎหมายมีการกำหนดทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองที่ค่อนข้างหนัก กลุ่มคนเหล่านี้อาจจะใช้ข้อมูลส่วนบุคคลเป็นเครื่องมือในการโจมตีธนาคารเพื่อเรียกร้อยเงินตอบแทนรวมถึงเป็นเป้าหมายของอาชญากรไซเบอร์ (Hacker) ในการเรียกค่าไถ่เพิ่มขึ้นอีกด้วย

ดังนั้นสามารถสรุปได้ว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบในเชิงบวกต่อภาพรวมของภาคธุรกิจธนาคารพาณิชย์ คือ การเพิ่มโอกาสการแข่งขันในระดับสากล เสริมสร้างความเชื่อมั่นและความแข็งแกร่งให้กับภาคธุรกิจ ในมุมของความเชื่อมั่นจากผู้บริโภค และคุณภาพของข้อมูลส่วนบุคคลที่เพิ่มขึ้นทำให้เกิดการประมวลผลอย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับบทความวิจัยของ กิตติพงศ์ กมลธรรมวงศ์ (2563) กล่าวว่า การสร้างมาตรฐานในการ

คุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ด้อยไปกว่าประเทศอื่น ๆ และสอดคล้องกับมาตรฐานสากลเป็นพื้นฐานที่จำเป็นต่อการพัฒนาธุรกิจบริการในอนาคตให้มีความสามารถแข่งขันกับนานาชาติรวมทั้งช่วยสร้างความตระหนักรู้ในสิทธิที่จะเข้าถึง ปกป้อง และควบคุมข้อมูลส่วนบุคคลของเอกชนให้เกิดขึ้น ทำให้เกิดความเข้าใจระหว่างผู้ประกอบการและผู้บริโภค เพิ่มความน่าเชื่อถือให้ผู้ประกอบการ และมีความคล่องตัวในการใช้ข้อมูลที่เกิดขึ้นมาเป็นประโยชน์อย่างแท้จริง แต่อย่างไรก็ตามจากการวิจัยได้พบประเด็นเพิ่มเติมจากองค์ความรู้เดิมในส่วนของผลกระทบในเชิงลบต่อภาคธุรกิจหากเกิดความไม่ชัดเจนให้แนวทางปฏิบัติและความรู้ของผู้บริโภคที่ไม่เพียงพอ คือ เกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาดซึ่งอาจเป็นภาระกับบริษัทขนาดกลางและขนาดเล็กและการใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม เนื่องจากความไม่เข้าใจในตัวกฎหมายของเจ้าของข้อมูลรวมถึงมีการใช้สิทธิจากกลุ่มเจ้าของข้อมูลที่ใช้กฎหมายเป็นเครื่องมือในการโจมตีธนาคารเพื่อเรียกร้องค่าตอบแทน

ตารางที่ 5.1

สรุปผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
จากบทความวิจัยของ กิตติพงศ์ กมลธรรมวงศ์ (2563) เรื่อง ประสพการณ์ของกฎหมาย คุ้มครองข้อมูลส่วนบุคคลในประเทศ สาธารณรัฐสิงคโปร์: บทเรียนสำหรับประเทศไทย กล่าวว่า การสร้างมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ด้อยไปกว่าประเทศอื่น ๆ และ สอดคล้องกับมาตรฐานสากลเป็นพื้นฐานที่จำเป็นต่อการพัฒนาธุรกิจบริการในอนาคตให้มีความสามารถแข่งขันกับนานาชาติรวมทั้ง ช่วยสร้างความตระหนักรู้ในสิทธิที่จะเข้าถึง ปกป้อง และควบคุมข้อมูลส่วนบุคคลของเอกชนให้เกิดขึ้น ทำให้เกิดความเข้าใจระหว่างผู้ประกอบการและผู้บริโภค เพิ่มความน่าเชื่อถือให้ผู้ประกอบการ และมีความคล่องตัวในการใช้ข้อมูลที่เกิดขึ้นมาเป็นประโยชน์อย่างแท้จริง	ผลกระทบในภาพรวมของอุตสาหกรรมจากการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นได้ส่งผลกระทบทั้งในเชิงบวกและเชิงลบ ดังนี้ 1) ผลกระทบเชิงบวก: เพิ่มโอกาสการแข่งขันในระดับสากล เสริมสร้างความเชื่อมั่นและความแข็งแกร่งให้กับภาคธุรกิจ และคุณภาพของข้อมูลส่วนบุคคลที่เพิ่มขึ้นทำให้เกิดการประมวลผลอย่างมีประสิทธิภาพ

ตารางที่ 5.1

สรุปผลกระทบในภาพรวมของอุตสาหกรรมจาก พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	2) ผลกระทบเชิงลบ: เกิดการสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลโดยบริษัทใหญ่ในตลาด ซึ่งอาจเป็นภาระกับบริษัทขนาดกลางและขนาดเล็กและการใช้สิทธิของเจ้าของข้อมูลที่ไม่เหมาะสม เนื่องจากความไม่เข้าใจในตัวกฎหมายของเจ้าของข้อมูลและมีการใช้สิทธิจากกลุ่มเจ้าของข้อมูลที่ไม่ประสงค์ดีกับธนาคารใช้กฎหมายเป็นเครื่องมือในการโจมตีธนาคารเพื่อเรียกร้องค่าตอบแทน

5.1.1.2 ผลกระทบในระดับองค์กรจากการปรับใช้ พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบในระดับองค์กรของภาคธุรกิจธนาคารพาณิชย์ทั้งปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กร โดยมีรายละเอียด ดังนี้

(1) ผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร

ประกอบด้วยปัจจัย ดังนี้

1. ผลกระทบต่อโครงสร้างองค์กร กลยุทธ์และนโยบาย

ด้านโครงสร้างองค์กร (Organization Structure) จากการสัมภาษณ์กลุ่มผู้ปฏิบัติงานธนาคารและผู้เชี่ยวชาญ พบว่า มีการเพิ่มตำแหน่งงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office: DPO) และจัดให้มีทีมงานเพื่อสนับสนุนการทำงานของ DPO ซึ่งมีเพียงบริษัทเดียวเท่านั้นที่มีทีมงานรับผิดชอบงานสนับสนุน DPO โดยเฉพาะและแยกส่วนงานคุ้มครองข้อมูลส่วนบุคคลออกจากส่วนงานอื่น สำหรับบริษัทส่วนใหญ่ที่ทีมงานสนับสนุนงาน DPO จะเป็นงานที่ได้รับผิดชอบเพิ่มเติมจากงานเดิมและไม่มีการแยกส่วนงานคุ้มครองข้อมูลส่วนบุคคลออกจากส่วนงานเดิม ซึ่งบุคลากรที่ถูกแต่งตั้งให้ดำรงตำแหน่ง DPO มาจากส่วนงานกำกับดูแลกิจการ (Compliance) และส่วนงานกฎหมาย (Legal) ที่ต้องดำรงตำแหน่งงานเดิมและเพิ่มเติมตำแหน่ง DPO ด้วย แต่อย่างไรก็ตาม DPO ของบริษัทจะรายงานตรงต่อผู้มีอำนาจตัดสินใจสูงสุดขององค์กร

ด้านกลยุทธ์ (Strategy) กลุ่มผู้ปฏิบัติงานภาคธนาคารมองว่ากลยุทธ์ขององค์กรจะมุ่งเน้นการปฏิบัติตามกฎหมายให้มีความสำคัญกับเรื่องกระบวนการควบคุม การรักษาความปลอดภัยของข้อมูลส่วนบุคคลมากขึ้น บริหารความเสี่ยงในกิจกรรมที่ทำให้เกิดความเสี่ยงทางด้านกฎหมาย โดยการตัดสินใจเชิงกลยุทธ์ทั้งหมดจะอยู่บนพื้นฐานของการหาสมดุลระหว่างการผลประโยชน์ของลูกค้าและการปฏิบัติตามกฎหมายกับการดำเนินธุรกิจที่ไม่ได้รับผลกระทบมากเกินไป ซึ่งในปัจจุบันสามารถแบ่งธนาคารพาณิชย์ออกเป็น 2 กลุ่มกลยุทธ์ ตามมุมมองการตีความทางด้านกฎหมายของแต่ละธนาคาร ได้แก่ 1) กลุ่มที่ตีความกฎหมายอย่างเคร่งครัด (Conservative) โดยจะเน้นการขอความยินยอม (Consent) และการปฏิบัติตามสัญญา (Contract) และ 2) กลุ่มที่ตีความโดยมุ่งเน้นการดำเนินธุรกิจเป็นหลักเน้นใช้หลักประโยชน์อันชอบธรรม (Legitimate Interest)

ด้านนโยบาย (Policy) กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมองไปในทิศทางเดียวกันว่าต้องปรับปรุงนโยบายเดิมที่มีอยู่แล้วในองค์กรโดยให้สอดคล้องกับเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล เพิ่มประสิทธิภาพในการควบคุมมากขึ้น พร้อมทั้งมีการกำหนดบทลงโทษสำหรับบุคลากรในองค์กรที่กระทำผิด นอกจากนี้ยังมีการเพิ่มเติมในส่วนของการคุ้มครองข้อมูลส่วนบุคคลเข้าไปในนโยบายธรรมาภิบาลข้อมูล (Data Governance Policies) และการออกประกาศนโยบายใหม่สำหรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของบริษัทโดยเฉพาะและจัดทำนโยบายความเป็นส่วนตัว (Privacy Policy)

ดังนั้นจึงสรุปได้ว่าจากการเก็บข้อมูลโดยการสัมภาษณ์กลุ่มตัวอย่างพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อการเปลี่ยนแปลงโครงสร้างองค์กร กลยุทธ์และนโยบาย โดยมีการเพิ่มตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และทีมงานสนับสนุนการทำงานของ DPO ซึ่งเป็นไปตามกฎหมายกำหนด รวมถึงปรับปรุงกลยุทธ์มุ่งเน้นผลประโยชน์ของลูกค้าและการปฏิบัติตามกฎหมายที่สามารถดำเนินธุรกิจต่อไปได้อย่างมีประสิทธิภาพ และปรับปรุงนโยบายบริษัทให้ตอบสนองกับการปฏิบัติตามกฎหมาย ซึ่งสอดคล้องกับแนวคิดรูปแบบการเปลี่ยนแปลงองค์กรของ Robbins and Coulter (2008) ที่กล่าวว่าการเปลี่ยนแปลงโครงสร้างเป็นหนึ่งในรูปแบบการเปลี่ยนแปลงองค์กร ซึ่งเป็นการเปลี่ยนแปลงให้สอดคล้องกับการเปลี่ยนแปลงที่อาจเกิดจากปัจจัยภายในหรือภายนอก ซึ่งหมายถึงการเปลี่ยนแปลงองค์ประกอบต่าง ๆ ของโครงสร้างองค์กร

2. ผลกระทบต่อกระบวนการปฏิบัติงาน

ธนาคารมีการเปลี่ยนแปลงในกระบวนการปฏิบัติงานต่าง ๆ ทั้งทั้งองค์กร เพื่อให้การปฏิบัติงานเป็นไปตามกฎหมายกำหนดซึ่งสามารถแบ่งเป็น 2 ส่วน คือ 1) การปรับปรุงกระบวนการปฏิบัติงานเดิม 2) การเพิ่มกระบวนการปฏิบัติงานใหม่

การปรับปรุงกระบวนการปฏิบัติงานเดิม ทั้งกระบวนการภายในและภายนอกองค์กรจะถูกทบทวนทุกกระบวนการของบริษัทที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล (Data Flow) เพื่อให้บริษัทมั่นใจได้ว่าทุกกระบวนการที่เกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดของกฎหมาย ข้อมูลถูกเก็บรวบรวมอย่างถูกต้องตามฐานการประมวลข้อมูล มีการใช้ข้อมูลอย่างถูกต้อง โปร่งใสเป็นไปตามวัตถุประสงค์ และมีการเปิดเผยข้อมูลตามที่กฎหมายกำหนด พร้อมทั้งมีกระบวนการรักษาความปลอดภัยข้อมูลที่เป็นมาตรฐาน มีการออกแบบการควบคุมที่เหมาะสมตามความเสี่ยงของข้อมูลที่จะส่งผลกระทบต่อเสรีภาพของบุคคล ออกแบบการให้บริการและการสื่อสารกับลูกค้าเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร อีกทั้งยังมีการปรับปรุงกระบวนการทางการตลาดที่ต้องใช้ข้อมูลที่ได้รับคามยินยอมจากลูกค้าและใช้ตามวัตถุประสงค์ที่ระบุไว้เท่านั้น รวมถึงออกแบบการกระบวนการขอความยินยอม (Consent) จากลูกค้าที่ทำให้ลูกค้ายินยอมให้ข้อมูลแก่บริษัท กระบวนการจัดจ้างที่ต้องเพิ่มหลักเกณฑ์ในการพิจารณาเกี่ยวกับเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และเพิ่มขอบเขตการตรวจสอบภายในองค์กรเกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการตรวจสอบ

การเพิ่มกระบวนการปฏิบัติงานใหม่ หลังจากการปรับใช้กฎหมายมีกระบวนการปฏิบัติงานใหม่เพิ่มขึ้นหลัก ๆ 3 กระบวนการ ดังนี้

(1) กระบวนการบริหารจัดการการขอความยินยอม (Consent Management) เมื่อบริษัทกำหนดได้ว่าข้อมูลส่วนบุคคลใดที่บริษัทจำเป็นต้องจัดเก็บ ใช้ และเปิดเผยภายใต้ฐานความยินยอม (Consent) ต้องจัดให้มีกระบวนการขอความยินยอมและการแจ้งประกาศความเป็นส่วนตัว (Privacy notice) ที่มีความชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิด พร้อมทั้งจัดให้มีกระบวนการถอนความยินยอมที่สามารถทำได้โดยง่าย

(2) กระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right Management) ต้องมีการออกแบบกระบวนการทำงานให้รองรับการเข้ามาใช้สิทธิของเจ้าของข้อมูลตามที่กฎหมายกำหนด และช่องทางในการเข้ามาใช้สิทธิของเจ้าของข้อมูล รวมถึงกระบวนการจัดการข้อร้องเรียนจากเจ้าของข้อมูล ซึ่งเป็นสิ่งที่ผู้บริหารธนาการมีความกังวลกับสิทธิในการลบ (Right to be Forgotten) ที่ในทางปฏิบัติสามารถทำได้ยากโดยเฉพาะข้อมูลเก่า ๆ เพราะข้อมูลกระจายอยู่ทั่วองค์กรและสิทธิในการโอนย้ายข้อมูล (Right to Data Portability) เนื่องจากยังต้องอาศัยความพร้อมและความชัดเจนในหลาย ๆ ด้านทั้งภาครัฐและเอกชน ซึ่งมีการลงทุนที่ค่อนข้างสูง

(3) กระบวนการแจ้งการรั่วไหลของข้อมูล (Data Breach Notification) จัดให้มีการกระบวนการตรวจสอบสาเหตุการรั่วไหลของข้อมูลที่มีความรวดเร็ว และ

ออกแบบกระบวนการแจ้งเหตุการณ์รั่วไหลข้อมูลต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลที่สามารถแจ้งเหตุการณ์ได้ภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด

ดังนั้นจึงสรุปได้ว่าการเก็บข้อมูลโดยการสัมภาษณ์กลุ่มตัวอย่างพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อกระบวนการปฏิบัติงานของธนาคารโดยมีการเปลี่ยนแปลงในกระบวนการปฏิบัติงานต่าง ๆ ทั้งทั้งองค์กร เพื่อให้การปฏิบัติงานเป็นไปตามกฎหมายซึ่งแบ่ง 2 ส่วน ได้แก่ 1) ปรับปรุงกระบวนการปฏิบัติงานเดิม 2) เพิ่มกระบวนการปฏิบัติการใหม่ ซึ่งสอดคล้องกับแนวคิดการเปลี่ยนแปลงองค์กรโดยการเปลี่ยนแปลงกระบวนการ (Process Change) เป็นหนึ่งในรูปแบบการเปลี่ยนแปลง โดยเป็นการเปลี่ยนแปลงขั้นตอนการทำงาน เพื่อวัตถุประสงค์สำคัญ คือ การลดระยะเวลาของกระบวนการต่าง ๆ การเพิ่มความน่าเชื่อถือ การลดต้นทุน และการเพิ่มประสิทธิภาพการทำงาน (Society for Human Resource Management, 2005) และ Jennifer (2020) ที่กล่าวไว้ในบทความ GDPR มีผลกับธุรกิจอย่างไร ว่า GDPR ได้เปลี่ยนแปลงหลายกระบวนการในบริษัท เช่น วิธีการขายของทีมงานตลาด หรือวิธีการจัดการกิจกรรมทางการตลาด บริษัทต้องตรวจสอบกระบวนการทางธุรกิจ แอปพลิเคชันและแบบฟอร์มต่าง ๆ เพื่อให้สอดคล้องกับกฎหมาย

3. ผลกระทบต่อทรัพยากรบุคคล

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญให้ความเห็นในทิศทางเดียวกันต่อผลกระทบด้านทรัพยากรบุคคล ซึ่งสามารถสรุปได้ 4 ประเด็น ได้แก่ 1) ภาระงานที่เพิ่มขึ้น 2) เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้านข้อมูล (Data Literacy) 3) มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 4) เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

ภาระงานที่เพิ่มขึ้น

พนักงานมีภาระงานที่เพิ่มมากขึ้นทั้งส่วนงานสนับสนุน (Back Office) และส่วนงานปฏิบัติการ (Staff) โดยส่วนงานสนับสนุน (Back Office) ก็จะมีภาระที่เพิ่มขึ้นจากการที่ต้องวางแผนและออกแบบการปฏิบัติงานในการปรับใช้กฎหมายกับกระบวนการทางธุรกิจ ซึ่งจะมีการแต่งตั้ง DPO และคณะทำงาน (Working Team) จากส่วนงานต่าง ๆ ซึ่งยังต้องรับผิดชอบหน้าที่งานในส่วนเดิมที่ต้องดูแลและเพิ่มเติมงานหน้าที่งานใหม่ในการปรับใช้กฎหมาย แต่อย่างไรก็ตามในอนาคตอาจมีการพิจารณาสรรหาคนเพิ่ม ส่วนงานปฏิบัติการพนักงานธนาคารที่ให้บริการลูกค้าก็จะมีขั้นตอนการปฏิบัติงานที่เพิ่มมากขึ้น ต้องมีการสื่อสารสร้างความเข้าใจกับลูกค้าเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะการขอความยินยอม(Consent) จากลูกค้า รวมถึงต้องเรียนรู้กระบวนการทำงานที่เปลี่ยนแปลงไป

เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้าน

ข้อมูล (Data Literacy)

พนักงานทุกคนในองค์กรควรมีการเพิ่มทักษะในการทำความเข้าใจข้อมูล (Data Literacy) ซึ่งสำคัญมากในยุคที่ข้อมูลมีอยู่มากมาย พนักงานจึงต้องมีความเข้าใจกับข้อมูลที่ใช้ทั้งในแง่ของกฎหมายและการใช้ให้เกิดประโยชน์อย่างสูงสุด และที่สำคัญต้องได้รับการอบรมความรู้เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงทัศนคติต่อข้อมูลส่วนบุคคลต้องเปลี่ยนแปลงไปจากเดิมที่มองว่าข้อมูลเป็นสินทรัพย์ของบริษัทแต่ปัจจุบันนี้เป็นสินทรัพย์ของเจ้าของข้อมูล

มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

พนักงานภายในองค์กรต้องได้รับบทลงโทษจากการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทกำหนดเพื่อเป็นการควบคุมการปฏิบัติตามกฎหมายและกฎระเบียบของคนในองค์กร รวมถึงผู้บริหารที่มีโทษทางอาญาตามกฎหมายอีกด้วย

เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

ถือว่าเป็นผลกระทบในเชิงบวกแก่บุคลากรในองค์กรในการเพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path) เพื่อดำรงตำแหน่ง DPO หรือทีมงานสนับสนุน DPO ในหลาย ๆ สายงาน เช่น สายงานบริหารความเสี่ยง สายงานกำกับดูแลกิจการ สายงานกฎหมาย สายงานเทคโนโลยีสารสนเทศ และสายงานตรวจสอบ เป็นต้น

ดังนั้นจึงสรุปได้ว่าจากการเก็บข้อมูลโดยการสัมภาษณ์กลุ่มตัวอย่างพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อทรัพยากรบุคคล ในหลายประเด็นซึ่งสามารถสรุปได้ 4 ประเด็น ได้แก่ 1) ภาระงานที่เพิ่มขึ้น 2) เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้านข้อมูล (Data Literacy) 3) มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 4) เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path) ซึ่งสอดคล้องกับแนวคิดรูปแบบการเปลี่ยนแปลงองค์กรของ Robbins and Coulter (2008) ที่กล่าวว่า การเปลี่ยนแปลงคนเป็นหนึ่งในรูปแบบการเปลี่ยนแปลงองค์กร ซึ่งการเปลี่ยนแปลงคน ผู้บริหารจะต้องพยายามปรับเปลี่ยนพนักงานใน ด้านต่าง ๆ เช่น ทัศนคติ ความคาดหวัง การรับรู้ และพฤติกรรม เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพมากขึ้น และ Deloitte (2018) กล่าวว่า GDPR ได้ส่งผลกระทบเป็นวงกว้างทั้งองค์กร รวมถึงทรัพยากรบุคคล ซึ่งสามารถแบ่งออกเป็น 3 ประเด็น ได้แก่ 1) เพิ่มหน้าที่งานให้คนในองค์กร 2) สรรหาพนักงานเพิ่ม 3) พนักงานทุกคนในองค์กรต้องได้รับการอบรม และมีประเด็นเพิ่มเติมจากองค์ความรู้เดิม คือ มีความ

เสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการเพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

4. ผลกระทบต่อเทคโนโลยี

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญให้ความเห็นในทิศทางเดียวกันเกี่ยวกับผลกระทบต่อเทคโนโลยีซึ่งมีผลกระทบใน 2 ส่วน ได้แก่ 1) การลงทุนในเทคโนโลยีใหม่ 2) การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร โดยมีรายละเอียด ดังนี้

การลงทุนในเทคโนโลยีใหม่

ไม่ได้เป็นการลงทุนในซอฟต์แวร์สำเร็จรูปสำหรับ PDPA เป็นการเฉพาะ เนื่องจากผู้ประกอบการเห็นว่ายังไม่มีซอฟต์แวร์สำเร็จรูปใดที่จะปรับใช้ได้กับกระบวนการปฏิบัติงานของทุกองค์กร แต่จะลงทุนในเทคโนโลยีใหม่ ๆ ในระบบการบริหารจัดการการขอความยินยอม (Consent Management) และระบบการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) นอกจากนี้ก็มีการเปลี่ยนซอฟต์แวร์บางรุ่นที่ไม่สามารถพัฒนาได้หรือต้นทุนในการพัฒนาสูงเพื่อให้รองรับกับกฎหมาย

ส่วนในเรื่องของเทคโนโลยีทางด้านการรักษาความปลอดภัยธนาคารให้ความสำคัญและลงทุนในเรื่องนี้มาระยะหนึ่งแล้วจึงไม่ได้รับผลกระทบมากนักแต่ก็ยังมีการเพิ่มความเข้มข้นในการรักษาความปลอดภัยเพิ่มขึ้นและมองหาเครื่องมือใหม่ ๆ ที่จะเข้ามาช่วยในเรื่องของการป้องกันข้อมูลเพิ่มขึ้น

อย่างไรก็ตามการใช้เทคโนโลยีเข้ามาช่วยในการปฏิบัติตามกฎหมายก็ต้องแลกมาด้วยความเสี่ยงทางด้านความปลอดภัยยิ่งใช้เทคโนโลยีมากขึ้นเท่าไรก็ต้องลงทุนในการรักษาความปลอดภัยเพิ่มมากขึ้นด้วย

การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร

ผลกระทบทางด้านการพัฒนาเทคโนโลยีในภาคอุตสาหกรรมธนาคารถือว่าเป็นโอกาสในการพัฒนาและผลักดันเทคโนโลยีในภาคธุรกิจให้เป็นธนาคารยุคดิจิทัลมากขึ้น (Digital Banking) เนื่องจากกฎหมายเข้ามาเสริมความเชื่อมั่นในการปกป้องข้อมูลส่วนบุคคลในกับลูกค้าเพียงแค่ว่าในช่วงแรกของการปรับใช้กฎหมายอาจจะทำให้การพัฒนาเทคโนโลยีชะลอตัวลงเท่านั้น

ดังนั้นสามารถสรุปได้ว่าการเก็บข้อมูลโดยการสัมภาษณ์กลุ่มตัวอย่างพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อเทคโนโลยีซึ่งมีผลกระทบใน 2 ส่วน ประกอบด้วย 1) การลงทุนในเทคโนโลยีใหม่ 2) การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร สอดคล้องกับงานวิจัยของ Deloitte (2018) ที่ระบุว่าจากผลการสำรวจ พบว่า เกินกว่า 70% ไม่ว่าจะเป็นอุตสาหกรรมในภาคการเงินหรือภาคอุตสาหกรรมอื่น ส่วน

ใหญ่เลือกใช้เทคโนโลยีเข้ามาเป็นตัวช่วยในการคุ้มครองข้อมูลส่วนบุคคล เทคโนโลยีมีส่วนสำคัญในการคุ้มครองข้อมูล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ซึ่งเทคโนโลยีสามารถช่วยในการระบุและลดความเสี่ยงในการคุ้มครองข้อมูลซึ่งเป็นส่วนหนึ่งของแนวปฏิบัติตามกฎหมาย GDPR และงานวิจัยของ PricewaterhouseCoopers (2017) ที่ระบุว่า ผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือ ระบบ IT ที่เกี่ยวข้องกับการทำงาน PwC เห็นโอกาสในการปฏิบัติตาม GDPR ที่สามารถนำไปสู่ประสิทธิภาพในการปฏิบัติงานและการสร้างชื่อเสียงที่ดีเตรียมความพร้อมสู่ยุคดิจิทัล

5. ผลกระทบต่อรายได้และต้นทุนองค์กร

ผลกระทบต่อรายได้ (Revenue)

ทางกลุ่มผู้ปฏิบัติงานภาคธนาคารมองว่าไม่เกิดผลกระทบต่อรายได้ของบริษัทและไม่เป็นการสร้างโอกาสในการแข่งขันเนื่องจากในภาคธุรกิจธนาคารพาณิชย์มักจะมีแนวปฏิบัติที่เป็นมาตรฐานเป็นไปในทิศทางเดียวกันจึงทำให้การสร้างความแตกต่างเพื่อการสร้างความได้เปรียบในการแข่งขันเป็นไปได้ยาก ในขณะที่กลุ่มผู้เชี่ยวชาญมองว่าหากบริษัทสามารถทำได้ดีในเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะเป็นการสร้างเชื่อมั่นให้กับลูกค้าและเป็นการดึงดูดลูกค้ามาเป็นของบริษัท เพิ่มความสัมพันธ์ในระยะยาวกับลูกค้าแต่อย่างไรก็ตามต้องอยู่บนพื้นฐานที่ว่าลูกค้าให้คุณค่ากับการคุ้มครองข้อมูลส่วนบุคคลมาน้อยแค่ไหน

ผลกระทบต่อต้นทุน (Cost)

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมีความเห็นเป็นไปในทิศทางเดียวกันว่าบริษัทจะมีต้นทุนการบริหารข้อมูลที่เพิ่มขึ้นจาก 1) ต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) ซึ่งต้นทุนจะแบ่งออกเป็นสองช่วง คือ ต้นทุนช่วงแรกจะเป็นต้นทุนเริ่มต้นเพื่อปรับใช้กฎหมาย PDPA และ ต้นทุนหลังการปรับใช้กฎหมาย PDPA 2) ต้นทุนจากการจ้างงานคนภายนอกองค์กร (Outsource) ที่เพิ่มสูงขึ้น ในขณะเดียวกันก็มีส่วนป้องกันการเกิดค่าปรับจำนวนมหาศาลจากการทำผิดกฎหมายและช่วยให้บริษัทสามารถลดต้นทุนการจัดเก็บข้อมูลเนื่องจากมีการจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น

(1) ต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost)

- ต้นทุนช่วงแรกจะเป็นต้นทุนเริ่มต้นเพื่อปรับใช้กฎหมาย PDPA หลัก ๆ จะประกอบด้วย ต้นทุนทรัพยากรบุคคล (Manhours) ที่ใช้ในการวางแผนและออกแบบปรับปรุงเปลี่ยนแปลงกระบวนการทำงานทั้งองค์กรเพื่อรองรับกฎหมาย ต้นทุนในการซื้อเทคโนโลยีใหม่ ๆ ตามที่ได้กล่าวไปแล้วข้างต้นรวมถึงต้นทุนในการติดตั้งและปรับแต่งเพื่อให้สามารถใช้งานเชื่อมต่อกับระบบเก่าต่าง ๆ ในองค์กรได้ นอกจากนี้ยังมีต้นทุนในการฝึกอบรมให้ความรู้ สร้างการตระหนักรู้ให้พนักงานภายในองค์กรทุกระดับ และต้นทุนจากการจ้างที่ปรึกษาภายนอกอีกด้วย

- ต้นทุนในช่วงหลังการปรับใช้กฎหมายนั้นจะเป็นต้นทุนจากการปรับปรุงกระบวนการเมื่อปรับใช้จริงแล้วมีปัญหาที่อาจจะไม่สะดวก ไม่เป็นที่พอใจของลูกค้า หรือเสี่ยงต่อการไม่ปฏิบัติตามกฎหมายก็จะมีต้นทุนในการตรวจสอบ ประเมินผลและออกแบบการควบคุมใหม่ รวมถึงค่าบำรุงรักษาระบบต่าง ๆ

(2) ต้นทุนจากการจ้างงานคนภายนอกองค์กร (Outsource) ที่เพิ่มสูงขึ้น

ผู้ให้บริการมีการคิดอัตราค่าบริการที่สูงขึ้นจากต้นทุนการปฏิบัติตามกฎหมาย (Compliance Cost) ที่เพิ่มขึ้น โดยเฉพาะรายที่มีการผูกขาด รวมถึงต้นทุนที่บริษัทต้องปรับตัวเพื่อเป็นมาตรฐานให้บริษัทสามารถใช้บริการ

อย่างไรก็ตามมีผู้ปฏิบัติงานภาคธนาคารและกลุ่มผู้เชี่ยวชาญที่มองว่ากฎหมายมีส่วนช่วยให้บริษัทสามารถลดต้นทุนการจัดเก็บข้อมูลเนื่องจากการจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น และช่วยลดความเสี่ยงจากการทำผิดกฎหมายและเกิดค่าปรับจำนวนมาก

สุดท้ายแล้วแน่นอนว่ามันเกิดเป็น Compliance Cost ที่สามารถวัดเป็นตัวเงินได้ แต่ในขณะเดียวกันถ้าบริษัทปฏิบัติตามกฎหมายก็จะมี Compliance Benefit เกิดขึ้นด้วย เช่น ไม่ต้องเก็บข้อมูลมากมายที่เป็นความเสี่ยง ประหยัดพื้นที่การจัดเก็บ ลดความเสี่ยงจากการถูกปรับและเสียชื่อเสียงองค์กรซึ่งไม่สามารถวัดเป็นตัวเงินได้ ดังนั้นไม่สามารถทราบได้แน่ชัดว่าระหว่าง Compliance Cost และ Compliance Benefit สุดท้ายแล้วผลจะเป็นต้นทุนที่เพิ่มขึ้นหรือประโยชน์ที่มากกว่า

ดังนั้นสามารถสรุปได้ว่าผลกระทบต่อรายได้จากการสัมภาษณ์กลุ่มตัวอย่างพบว่า กลุ่มผู้ปฏิบัติงานภาคธนาคารมองว่ากฎหมายไม่ส่งผลกระทบต่อรายได้และไม่เป็นการสร้างโอกาสในการแข่งขัน ซึ่งแตกต่างจากกลุ่มผู้เชี่ยวชาญที่มองว่าหากบริษัทสามารถทำได้ดีในเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะเป็นการสร้างเชื่อมั่นให้กับลูกค้าและเป็นการดึงดูดลูกค้ามาเป็นของบริษัท แต่อย่างไรก็ตามต้องอยู่บนพื้นฐานที่ว่าลูกค้าให้คุณค่ากับการคุ้มครองข้อมูลส่วนบุคคลมากน้อยแค่ไหน ซึ่งสอดคล้องกับบทความ GDPR มีผลกับธุรกิจอย่างไร ของ Jennifer (2020) ที่กล่าวว่า GDPR สร้างโอกาสกับบริษัทที่สามารถแสดงให้เห็นว่าบริษัทได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล นอกเหนือจากการปฏิบัติตามกฎหมายเท่านั้นจะเป็นการสร้างควมไว้วางใจให้กับลูกค้าและเป็นการรักษาลูกค้าให้มีความภักดีต่อบริษัทมากขึ้นส่งผลต่อรายได้ของธุรกิจ

ส่วนผลกระทบต่อต้นทุนกลุ่มตัวอย่างระบุว่า บริษัทจะมีต้นทุนการบริหารข้อมูลเพิ่มขึ้นจาก 1) ต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) 2) ต้นทุนจากการจ้างงานคนภายนอกองค์กร (Outsource) ที่เพิ่มสูงขึ้น อย่างไรก็ตามมีผู้ปฏิบัติงานภาคธนาคารและกลุ่มผู้เชี่ยวชาญมองว่ากฎหมายมีส่วนช่วยให้บริษัทสามารถลดต้นทุนการจัดเก็บข้อมูลเนื่องจากการ

จัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น และช่วยลดความเสี่ยงจากการทำผิดกฎหมายและเกิดค่าปรับจำนวนมาก ซึ่งสอดคล้องกับบทความ GDPR มีผลกระทบต่อธนาคารอย่างไร ของ Abi (2018) ซึ่งกล่าวว่าธนาคารมีต้นทุนในการดำเนินการตาม GDPR ไม่มีธนาคารใดที่ไม่ได้รับผลกระทบโดยเฉลี่ยแล้วค่าใช้จ่ายในการดำเนินการตาม GDPR สำหรับธนาคารในสหราชอาณาจักรมีค่าใช้จ่ายสูงสุดของทุกภาคอุตสาหกรรม อย่างไรก็ตามแม้ว่าการปฏิบัติตามข้อกำหนดจะมีค่าใช้จ่ายสูงแต่การไม่ปฏิบัติตามกฎหมายอาจมีค่าใช้จ่ายที่สูงกว่า

ตารางที่ 5.2

สรุปผลกระทบต่อปัจจัยสภาพแวดล้อมภายในองค์กร

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
1. ผลกระทบต่อโครงสร้างองค์กร กลยุทธ์และนโยบาย	
แนวคิดรูปแบบการเปลี่ยนแปลงองค์กรของ Robbins and Coulter (2008) ที่กล่าวว่าการเปลี่ยนแปลงโครงสร้างเป็นหนึ่งในรูปแบบการเปลี่ยนแปลงองค์กร ซึ่งเป็นการเปลี่ยนแปลงให้สอดคล้องกับการเปลี่ยนแปลงที่อาจเกิดจากปัจจัยภายในหรือภายนอก ซึ่งหมายถึงการเปลี่ยนแปลงองค์ประกอบต่าง ๆ ของโครงสร้างองค์กร	ผลกระทบต่อโครงสร้างองค์กร รวมถึงกลยุทธ์และนโยบาย ได้แก่ 1) เพิ่มตำแหน่งงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office: DPO) โดยบุคลากรที่ถูกแต่งตั้งให้ดำรงตำแหน่ง DPO มาจากส่วนงานกำกับดูแลกิจการ (Compliance) และส่วนงานกฎหมาย (Legal) ซึ่งต้องดำรงตำแหน่งงานเดิมและเพิ่มเติมตำแหน่ง DPO ด้วยแต่อย่างไรก็ตาม DPO ของบริษัทจะรายงานตรงต่อผู้มีอำนาจตัดสินใจสูงสุดขององค์กร 2) จัดให้มีทีมงานเพื่อสนับสนุนการทำงานของ DPO ซึ่งสามารถรับผิดชอบงานสนับสนุน DPO เป็นการเฉพาะและแยกส่วนงานคุ้มครองข้อมูลส่วนบุคคลออกจากส่วนงานอื่น หรือรับผิดชอบงานสนับสนุน DPO เพิ่มเติมจากงานเดิมและไม่มี การแยกส่วนงานคุ้มครองข้อมูลส่วนบุคคลออกจากส่วนงานเดิม

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตวิทยาลัยสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	3) กลยุทธ์ขององค์กรจะมุ่งเน้นการหาสมดุลระหว่างการผลประโยชน์ของลูกค้าและการปฏิบัติตามกฎหมายกับการดำเนินธุรกิจที่ไม่ได้รับผลกระทบมากเกินไป 4) ปรับปรุงนโยบายเดิมที่มีอยู่แล้วให้สอดคล้องกับเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล และออกประกาศนโยบายใหม่สำหรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของบริษัทโดยเฉพาะและจัดทำนโยบายความเป็นส่วนตัว (Privacy Policy)
2. ผลกระทบต่อกระบวนการปฏิบัติงาน	
แนวคิดการเปลี่ยนแปลงองค์กรของ Society for Human Resource Management, (2005) กล่าวว่า การเปลี่ยนแปลงกระบวนการ (Process Change) เป็นหนึ่งในรูปแบบการเปลี่ยนแปลง โดยเป็นการเปลี่ยนแปลงขั้นตอนการทำงาน เพื่อวัตถุประสงค์สำคัญคือการลดระยะเวลาของกระบวนการต่าง ๆ การเพิ่มความน่าเชื่อถือ การลดต้นทุน และการเพิ่มประสิทธิผลการทำงาน และ Jennifer (2020) กล่าวไว้ในบทความ GDPR มีผลกับธุรกิจอย่างไร ว่า GDPR ได้เปลี่ยนแปลงหลายกระบวนการในบริษัท เช่น วิธีการขายของที่มีการตลาด หรือวิธีการจัดการกิจกรรมทางการตลาด บริษัทต้องตรวจสอบกระบวนการทางธุรกิจ	ผลกระทบต่อกระบวนการปฏิบัติงาน (Process) ธนาคารมีการเปลี่ยนแปลงในกระบวนการปฏิบัติงานต่าง ๆ ทั่วทั้งองค์กร เพื่อให้การปฏิบัติงานเป็นไปตามกฎหมายซึ่งแบ่งเป็น 2 ส่วน ได้แก่ 1) การปรับปรุงกระบวนการปฏิบัติงานเดิม (1.1) ทบทวนทุกกระบวนการของบริษัทที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล (Data Flow) เพื่อให้บริษัทมั่นใจได้ว่าทุกกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดของกฎหมาย (1.2) ปรับปรุงกระบวนการรักษาความปลอดภัยข้อมูลที่เป็นมาตรฐาน (1.3) ออกแบบการควบคุมที่เหมาะสมตามความเสี่ยงของข้อมูลที่จะส่งผลต่อเสรีภาพของบุคคล (1.4) ออกแบบการให้บริการและการสื่อสารกับ

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตวิทยาลัยสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
แอปพลิเคชันและแบบฟอร์มต่าง ๆ เพื่อให้สอดคล้องกับกฎหมาย	ลูกค้าเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (1.5) ปรับปรุงกระบวนการทางการตลาดที่ต้องใช้ข้อมูลที่ได้รับคามยินยอมจากลูกค้าและใช้ตามวัตถุประสงค์ที่ระบุไว้เท่านั้น รวมถึงออกแบบกระบวนการขอความยินยอม (Consent) จากลูกค้าที่ทำให้ลูกค้ายินยอมให้ข้อมูลแก่บริษัท (1.6) กระบวนการจัดจ้างที่ต้องเพิ่มหลักเกณฑ์ในการพิจารณาเกี่ยวกับเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (1.7) เพิ่มขอบเขตการตรวจสอบภายในองค์กรเกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการตรวจสอบ 2) เพิ่มกระบวนการปฏิบัติงานใหม่หลัก ๆ 3 กระบวนการ ดังนี้ (2.1) กระบวนการบริหารจัดการการขอความยินยอม (Consent Management) ต้องจัดให้มีกระบวนการขอความยินยอมและการแจ้งประกาศความเป็นส่วนตัว (Privacy Notice) ที่มีความชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิด พร้อมจัดให้มีกระบวนการถอนความยินยอมที่สามารถทำได้โดยง่าย (2.2) กระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล (Data Subject Right Management) ต้องมีการออกแบบกระบวนการทำงานให้รองรับการเข้ามาใช้สิทธิของเจ้าของข้อมูลตามที่กฎหมายกำหนด และช่องทางในการเข้ามาใช้สิทธิของเจ้าของข้อมูล รวมถึงกระบวนการจัดการข้อ

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	ร้องเรียนจากเจ้าของข้อมูล (2.3) กระบวนการแจ้งการรั่วไหลของข้อมูล (Data Breach Notification) ออกแบบกระบวนการแจ้งเหตุการณ์รั่วไหลของข้อมูลได้ภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด
3. ผลกระทบต่อทรัพยากรบุคคล	
แนวคิดรูปแบบการเปลี่ยนแปลงองค์กร ของ Robbins and Coulter (2008) ที่กล่าวว่าการเปลี่ยนแปลงคนเป็นหนึ่งในรูปแบบการเปลี่ยนแปลงองค์กร ซึ่งการเปลี่ยนแปลงคน ผู้บริหารจะต้องพยายามปรับเปลี่ยนพนักงานใน ด้านต่าง ๆ เช่น ทักษะคน ความคาดหวัง การรับรู้ และ พฤติกรรม เพื่อให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพมากขึ้น และ Deloitte (2018) กล่าวว่า GDPR ได้ส่งผลกระทบเป็นวงกว้างทั้งองค์กร รวมถึงทรัพยากรบุคคล ซึ่งสามารถแบ่งออกเป็น 3 ประเด็น ได้แก่ 1) เพิ่มหน้าที่งานให้คนในองค์กร บริษัทจำเป็นต้องจัดสรรความรับผิดชอบในการคุ้มครองข้อมูลให้กับผู้เชี่ยวชาญด้านกฎหมายหรือผู้เชี่ยวชาญด้านการกำกับดูแลโดยระบุความรับผิดชอบเกี่ยวกับ GDPR เพิ่มเติมเป็นส่วนหนึ่งของหน้าที่งาน 2) สรรหาพนักงานเพิ่ม โดยองค์กรต้องการพนักงานที่มีความเชี่ยวชาญด้านการคุ้มครอง	ผลกระทบต่อทรัพยากรบุคคล สามารถสรุปได้ 4 ประเด็น ดังนี้ 1) ภาระงานที่เพิ่มมากขึ้น พนักงานงานที่เกี่ยวข้องกับการปรับใช้กฎหมายต้องรับภาระงานในส่วนนี้เพิ่มเติมจากงานเดิม รวมถึง DPO ด้วย ที่ต้องรับตำแหน่ง DPO เพิ่มเติมจากงานเดิม ในอนาคตอาจจะมีพิจารณาสรรหาคนเพิ่ม 2) เพิ่มความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและทักษะด้านข้อมูล (Data Literacy) พนักงานทุกคนในองค์กรควรเพิ่มทักษะในการทำ ความเข้าใจข้อมูล (Data Literacy) และต้องได้รับการอบรมความรู้เกี่ยวกับกฎหมาย PDPA และแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงทัศนคติต่อข้อมูลส่วนบุคคลต้องเปลี่ยนแปลงไปจากเดิมที่มองว่าข้อมูลเป็นสินทรัพย์ของบริษัทแต่ปัจจุบันนั้นเป็นสินทรัพย์ของเจ้าของข้อมูล 3) มีความเสี่ยงจากการได้รับโทษในการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พนักงานภายในองค์กรต้องได้รับบทลงโทษจากการกระทำผิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บริษัท

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตวิทยาลัยสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
โดยเฉพาะ ในบริษัทใหญ่ ๆ จะมีการสรรหาเจ้าหน้าที่คุ้มครองข้อมูล (DPO) ผู้จัดการความเป็นส่วนตัวของข้อมูล และเจ้าหน้าที่อาวุโสที่ปฏิบัติงานเกี่ยวกับการปฏิบัติตามข้อกำหนด GDPR 3) พนักงานทุกคนในองค์กรต้องได้รับการอบรม ในพื้นฐานของการปฏิบัติตาม GDPR และย้ำเตือนเป็นประจำเกี่ยวกับขั้นตอนและแนวทางปฏิบัติที่ต้องปฏิบัติตาม	กำหนดเพื่อเป็นการควบคุมการปฏิบัติตามกฎหมาย รวมถึงผู้บริหารที่มีโทษทางอาญาตามกฎหมายอีกด้วย 4) เพิ่มเส้นทางความก้าวหน้าในสายอาชีพ (Career Path) เพื่อดำรงตำแหน่ง DPO หรือทีมงานสนับสนุน DPO ในหลาย ๆ สายงาน เช่น สายงานบริหารความเสี่ยง สายงานกำกับดูแลกิจการ สายงานกฎหมาย สายงานเทคโนโลยีสารสนเทศ และสายงานตรวจสอบ เป็นต้น
4. ผลกระทบต่อเทคโนโลยี	
4.1 งานวิจัยของ Deloitte (2018) ระบุว่า จากการสำรวจ พบว่า เกินกว่า 70% ไม่ว่าจะเป็นอุตสาหกรรมในภาคการเงินหรือภาคอุตสาหกรรมอื่น ส่วนใหญ่เลือกใช้เทคโนโลยีเข้ามาเป็นตัวช่วยในการคุ้มครองข้อมูลส่วนบุคคล เทคโนโลยีมีส่วนสำคัญในการคุ้มครองข้อมูล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ซึ่งเทคโนโลยีสามารถช่วยในการระบุและลดความเสี่ยงในการคุ้มครองข้อมูลซึ่งเป็นส่วนหนึ่งของแนวปฏิบัติตามกฎหมาย GDPR 4.2 งานวิจัยของ Pricewaterhouse Coopers (2017) ระบุว่า ผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือ ระบบ IT ที่	ผลกระทบต่อนโยบาย มีผลกระทบใน 2 ส่วน ได้แก่ 1) การลงทุนในเทคโนโลยีใหม่ พบว่า บริษัทมีการลงทุนในเทคโนโลยีใหม่ ๆ ในระบบบริหารจัดการการขอความยินยอม (Consent Management) และระบบการบริการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล และมองหาเครื่องมือใหม่ ๆ ที่จะเข้ามาช่วยในเรื่องของการป้องกันข้อมูลเพิ่มขึ้น แต่ไม่ได้มีการลงทุนในซอฟต์แวร์สำเร็จรูปสำหรับ PDPA เป็นการเฉพาะ เนื่องจากยังไม่มีซอฟต์แวร์สำเร็จรูปใดที่จะเข้าได้กับกระบวนการปฏิบัติงานของทุกองค์กรได้ 2) การพัฒนาทางด้านเทคโนโลยีในภาคธุรกิจธนาคาร ถือว่าเป็นโอกาสในการพัฒนาและผลักดันเทคโนโลยีในภาคธุรกิจให้เป็นธนาคารยุค

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
เกี่ยวข้องกับการทำงาน PwC เห็นโอกาสในการปฏิบัติตาม GDPR ที่สามารถนำไปสู่ประสิทธิภาพในการปฏิบัติงานและการสร้างชื่อเสียงที่ดี เตรียมความพร้อมสู่ยุคดิจิทัล	ดิจิทัลมากขึ้น (Digital Banking) เนื่องจากกฎหมายเข้ามาเสริมความเชื่อมั่นในการปกป้องข้อมูลส่วนบุคคลในกับลูกค้าเพียงแคในช่วงแรกของการปรับใช้กฎหมายอาจจะทำให้การพัฒนาเทคโนโลยีชะลอตัวลงเท่านั้น
5. ผลกระทบต่อรายได้และต้นทุน	
5.1 Jennifer (2020) กล่าวไว้ในบทความ GDPR มีผลกับธุรกิจอย่างไรว่า GDPR สร้างโอกาสกับบริษัทที่สามารถแสดงให้เห็นว่าบริษัทได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลที่นอกเหนือจากการปฏิบัติตามกฎหมายเท่านั้นจะเป็นการสร้างควมไว้วางใจให้กับลูกค้าและเป็นการรักษาลูกค้าให้มีความภักดีต่อบริษัทมากขึ้นส่งผลต่อรายได้ของธุรกิจ	ผลกระทบต่อยาได้สามารถแยกความเห็นออกเป็น 2 กลุ่ม 1) กลุ่มผู้ปฏิบัติงานภาคธนาคาร มองว่าไม่เป็นการสร้างโอกาสในการแข่งขันเนื่องจากในภาคธุรกิจธนาคารพาณิชย์มักจะมีแนวปฏิบัติที่เป็นมาตรฐานเป็นไปในทิศทางเดียวกันจึงทำให้การสร้างแตกต่างเพื่อการสร้างความได้เปรียบในการแข่งขันเป็นไปได้ยาก 2) กลุ่มผู้เชี่ยวชาญมองว่าหากบริษัทสามารถทำได้ดีในเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะเป็นการสร้างเชื่อมั่นใจกับลูกค้าและเป็นการดึงดูดลูกค้ามาเป็นของบริษัท เพิ่มความสัมพันธ์ในระยะยาวกับลูกค้าแต่อย่างไรก็ตามต้องอยู่บนพื้นฐานที่ว่าลูกค้าให้คุณค่ากับการคุ้มครองข้อมูลส่วนบุคคลไม่น้อยแค่ไหน
5.2 จากบทความ GDPR มีผลต่อธนาคารอย่างไร ของ Abi (2018) กล่าวว่าธนาคารมีต้นทุนในการดำเนินการตาม GDPR ไม่มีธนาคารใดที่ไม่ได้รับผลกระทบโดยเฉลี่ยแล้วค่าใช้จ่ายในการดำเนินการตาม GDPR สำหรับธนาคารในสหราชอาณาจักรมี	ผลกระทบต่อดัชนี พบว่า บริษัทจะมีต้นทุนการบริหารข้อมูลที่เพิ่มขึ้นจาก 1) ต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) ซึ่งต้นทุนจะแบ่งออกเป็นสองช่วง คือ ต้นทุนช่วงแรกจะเป็นต้นทุนเริ่มต้นเพื่อปรับใช้กฎหมาย PDPA และ ต้นทุนหลังการปรับใช้กฎหมาย PDPA 2) ต้นทุน

ตารางที่ 5.2

สรุปผลกระทบต่อบัณฑิตวิทยาลัยสภาพแวดล้อมภายในองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
ค่าใช้จ่ายสูงสุดของทุกภาคอุตสาหกรรม อย่างไรก็ตามแม้ว่าการปฏิบัติตามข้อกำหนดนั้นมีค่าใช้จ่ายสูงแต่ค่าปรับนั้นสูงยิ่งกว่า	จากการจ้างงานคนภายนอกองค์กร (Outsource) ที่เพิ่มสูงขึ้น แต่อย่างไรก็ตามกฎหมายมีส่วนช่วยให้บริษัทสามารถลดต้นทุนการจัดเก็บข้อมูล เนื่องจากมีการจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น และช่วยลดความเสี่ยงจากค่าปรับจำนวนมาก 1) ต้นทุนในการปฏิบัติตามกฎหมาย (Compliance Cost) - ต้นทุนช่วงแรกจะเป็นต้นทุนเริ่มต้นเพื่อปรับใช้กฎหมาย PDPA หลัก ๆ จะประกอบด้วย ต้นทุนทรัพยากรบุคคล (Manhours) ต้นทุนในการลงทุนปรับปรุงและซื้อเทคโนโลยี และต้นทุนในการฝึกอบรมให้ความรู้ สร้างการตระหนักรู้ให้พนักงานภายในองค์กรทุกระดับ และต้นทุนจากการจ้างที่ปรึกษาภายนอกอีกด้วย - ต้นทุนในช่วงหลังการปรับใช้กฎหมายนั้นจะเป็นต้นทุนจากการปรับปรุงกระบวนการเมื่อปรับใช้จริงแล้วมีปัญหาที่อาจจะไม่สะดวก ไม่เป็นที่พอใจของลูกค้า หรือเสี่ยงต่อการไม่ปฏิบัติตามกฎหมายก็จะมีต้นทุนในการตรวจสอบประเมินผล และออกแบบการควบคุมใหม่ รวมถึงค่าบำรุงรักษาระบบต่าง ๆ 2) ต้นทุนที่เพิ่มสูงขึ้นจากการจ้างงานคนภายนอก (Outsource) ที่จะมีการคิดอัตราค่าบริการที่สูงขึ้นจากต้นทุนการปฏิบัติตามกฎหมาย (Compliance Cost) ที่เพิ่มขึ้น

(2) ผลกระทบต่อปัจจัยสภาพแวดล้อมภายนอกองค์กร

1. ผลกระทบต่อลูกค้า

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมีความเห็นตรงกันว่าลูกค้าได้รับผลกระทบจากกฎหมาย ทั้งผลกระทบในเชิงบวกและผลกระทบในเชิงลบ โดยผลกระทบในเชิงบวก คือ ลูกค้าได้สิทธิในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลจากธนาคาร สร้างความมั่นใจให้กับลูกค้าว่าข้อมูลส่วนบุคคลจะไม่ถูกนำไปใช่นอกเหนือวัตถุประสงค์ที่ได้แจ้งไว้และมีความปลอดภัย แต่อย่างไรก็ตามการได้มาซึ่งผลประโยชน์ก็ต้องแลกกับต้นทุนที่เพิ่มขึ้นในกรณีนี้ลูกค้าจะมีต้นทุนค่าบริการเพิ่มขึ้นในรูปแบบของต้นทุนแฝงจากอัตราดอกเบี้ยเงินกู้เพิ่มขึ้นหรือปรับลดอัตราดอกเบี้ยเงินฝากเพื่อที่ธนาคารจะสามารถชดเชยต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามกฎหมาย ซึ่งถือเป็นผลกระทบเชิงลบของลูกค้า นอกจากนี้ยังมีผลกระทบในเชิงลบต่อประสบการณ์การใช้บริการของลูกค้า (Customer Experience) เช่น ขั้นตอนการทำธุรกรรมที่มากขึ้น ลูกค้ารู้สึกเสียเวลา ไม่อยากทำความเข้าใจเรื่องใหม่ๆ มากนัก หรือการใช้บริการเว็บไซต์ ที่จะมีการขออนุญาตเก็บ Cookies ทำให้ไม่สะดวกในการทำงาน เป็นต้น แต่ทั้งนี้ก็ยังขึ้นอยู่กับการตระหนักถึงข้อมูลส่วนบุคคลของลูกค้าแต่ละรายด้วย

ดังนั้นสามารถสรุปได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อลูกค้าในเชิงบวกและเชิงลบ โดยในเชิงบวก คือ ลูกค้าได้รับสิทธิในการคุ้มครองข้อมูลส่วนบุคคลและสามารถมั่นใจในมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลจากธนาคาร แต่มีผลกระทบเชิงลบต่อประสบการณ์การใช้บริการของลูกค้า (Customer Experience) จากขั้นตอนและเวลาการให้บริการที่มากขึ้น สอดคล้องกับ PricewaterhouseCoopers (2017) ที่ได้วิเคราะห์ผลกระทบจาก GDPR ต่อธุรกิจธนาคารในประเทศสวิตเซอร์แลนด์ โดย PwC กล่าวว่าผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือ ประสิทธิภาพของลูกค้า ปฏิสัมพันธ์และการนำเสนอบริการแก่ลูกค้า แต่อย่างไรก็ตามจากการสัมภาษณ์ยังมีประเด็นผลกระทบเชิงลบเพิ่มเติมจากองค์ความรู้เดิม คือ ต้นทุนค่าบริการที่เพิ่มขึ้นในรูปแบบของต้นทุนแฝงจากอัตราดอกเบี้ยเงินกู้เพิ่มขึ้นหรือปรับลดอัตราดอกเบี้ยเงินฝากเพื่อที่ธนาคารจะสามารถชดเชยต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามกฎหมาย

2. ผลกระทบต่อคู่ค้า

กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมีความเห็นเป็นไปในทิศทางเดียวกันว่า คู่ค้าได้รับผลกระทบในเชิงลบใน 3 ประเด็น ได้แก่ 1) โอกาสในการได้รับงานจากธนาคารลดลงและยากขึ้น 2) ต้นทุนในการให้บริการเพิ่มขึ้น 3) เกิดการแย่งชิงข้อมูล

โอกาสในการได้รับงานจากธนาคารลดลงและยากขึ้น เนื่องจากกระบวนการขึ้นเลือกคู่ค้าทั้งการพิจารณาคัดเลือกคู่ค้ารายใหม่และการต่อสัญญาเก่าของธนาคารจะต้องเพิ่มหลักเกณฑ์เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายกำหนด หากคู่ค้า

รายได้ไม่สามารถมาตามปฏิบัติได้ตามหลักเกณฑ์และกระบวนการที่ธนาคารกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลก็จะเสียโอกาสในการรับงาน รวมถึงถูกตรวจสอบกระบวนการทำงานว่าเป็นไปตามเกณฑ์มาตรฐานที่ธนาคารกำหนดหรือไม่ อีกทั้งธนาคารจะใช้บริการ Outsource ที่เกี่ยวกับข้อมูลส่วนบุคคลน้อยลง โดยจะพยายามดึงกลับมาทำเองให้ได้มากที่สุด

ต้นทุนในการให้บริการเพิ่มขึ้น เมื่อมีการปรับตัวปฏิบัติตามกฎหมาย และเกณฑ์การพิจารณาของธนาคารได้ก็ต้องมีต้นทุนที่เพิ่มมากขึ้นแต่หากเป็นผู้ประกอบการรายเล็ก ธนาคารมีอำนาจต่อรองสูงกว่าก็จะไม่สามารถเพิ่มอัตราค่าบริการได้ส่งผลต่อกำไรในการดำเนินงานลดลง

เกิดการแย่งชิงข้อมูล เมื่อมีหลักการเรื่องของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลก็ส่งผลให้เกิดการแย่งชิงข้อมูลกันขึ้น หากตีความว่าผู้ให้บริการ (Outsource) เป็นผู้ประมวลผลข้อมูลซึ่งโดยหน้าที่ตามกฎหมายผู้ประมวลผลข้อมูลจะต้องเก็บ ใช้และเปิดเผยตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้นไม่สามารถกระทำการนอกเหนือคำสั่งได้ ซึ่งบริษัทที่มีอำนาจในการต่อรองมากกว่าก็จะผลักดันให้อีกฝั่งเป็นผู้ประมวลผลข้อมูล โดยที่แท้จริงแล้วตามกฎหมายอาจจะเป็นผู้ควบคุมข้อมูลได้ทั้ง 2 ฝั่ง จึงเกิดเป็นภาพของการแย่งชิงข้อมูลกันแบบปลาใหญ่กินปลาเล็ก

ดังนั้นสามารถสรุปได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ส่งผลกระทบต่อคู่ค้า 3 เรื่อง ได้แก่ 1) โอกาสในการได้รับงานจากธนาคารลดลงและยากขึ้น 2) ต้นทุนในการให้บริการเพิ่มขึ้น 3) เกิดการแย่งชิงข้อมูล ซึ่งสอดคล้องกับ บทความของ วิษณุ วงศ์หาญเชาว์ (2562) ที่กล่าวว่า สำหรับองค์กรที่ทำงานร่วมกับผู้ให้บริการด้านไอที หรืออยู่ระหว่างพิจารณาคัดเลือกผู้ให้บริการ จะต้องแน่ใจว่าผู้ให้บริการจะต้องเข้าใจและให้ความสำคัญกับงานด้านความปลอดภัยในการประมวลผลข้อมูลตามกฎหมายของ GDPR ในประเด็นโอกาสในการได้รับงานจากธนาคารจะยากขึ้นเพราะต้องพิจารณาคุณสมบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย PDPA เพิ่มเติม ส่วนประเด็นที่ได้เพิ่มเติมจากองค์ความรู้เดิม คือ ต้นทุนการให้บริการที่เพิ่มขึ้นและเกิดการแย่งชิงข้อมูลลูกค้า

ตารางที่ 5.3

สรุปผลกระทบต่อบัณฑิตสภาแวดล้อมภายนอกองค์กร

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
1. ผลกระทบต่อลูกค้า	
จากงานวิจัยของ Pricewaterhouse Coopers (2017) ที่ได้วิเคราะห์ผลกระทบจาก GDPR ต่อธุรกิจธนาคารในประเทศ สวิตเซอร์แลนด์ โดย PwC กล่าวว่า ผลกระทบสำคัญจาก GDPR ต่อธนาคาร คือ ประเภทของลูกค้า ปฏิสัมพันธ์และการนำเสนอบริการแก่ลูกค้า	ลูกค้าได้รับผลกระทบจากกฎหมาย ทั้งผลกระทบในเชิงบวกและผลกระทบในเชิงลบ 1) ผลกระทบในเชิงบวก คือ ลูกค้าได้สิทธิในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและสามารถมั่นใจในมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลจากธนาคาร 2) ผลกระทบเชิงลบ คือ ผลกระทบต่อประสบการณ์การใช้บริการของลูกค้า (Customer Experience) เช่น ขั้นตอนการทำธุรกรรมที่มากขึ้น หรือการใช้บริการเว็บไซต์ ที่จะมีการขออนุญาตเก็บ Cookies ทำให้ไม่สะดวกในการใช้งาน เป็นต้น นอกจากนี้ยังมีต้นทุนค่าบริการเพิ่มขึ้นในรูปแบบของต้นทุนแฝงจากอัตราดอกเบี้ยเงินกู้เพิ่มขึ้นหรือปรับลดอัตราดอกเบี้ยเงินฝากเพื่อที่ธนาคารจะสามารถชดเชยต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามกฎหมาย
2. ผลกระทบต่อคู่ค้า	
บทความ GDPR กับการบริหารความเสี่ยงของข้อมูลส่วนบุคคลเพื่อแต้มต่อทางธุรกิจ วิษญ์ วงศ์หาญเชาว์ (2562) กล่าวว่า สำหรับองค์กรที่ทำงานร่วมกับผู้ให้บริการด้านไอที หรืออยู่ระหว่างพิจารณาคัดเลือกผู้ให้บริการระบบความปลอดภัยเพิ่มเติม จะต้องแน่ใจว่า ผู้ให้บริการหรือเวบเดอ์นั้น ๆ จะต้องเข้าใจ และให้ความสำคัญกับงานด้านความปลอดภัยในการประมวลผลข้อมูลตามกฎหมายของ GDPR	คู่ค้าได้รับผลกระทบจากการปรับใช้กฎหมาย 3 ประการ ได้แก่ 1) โอกาสในการได้รับงานจากธนาคารลดลงและยากขึ้น เนื่องจากธนาคารพยายามดึงงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลมาดำเนินการเอง และในกระบวนการคัดเลือกคู่ค้ามีการเพิ่มหลักเกณฑ์เรื่องการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย PDPA 2) ต้นทุนในการให้บริการเพิ่มขึ้น จากการปรับตัวปฏิบัติตามกฎหมายและหลักเกณฑ์ของบริษัทผู้ว่าจ้าง

ตารางที่ 5.3

สรุปผลกระทบต่อบัณฑิตวิทยาลัยสภาพแวดล้อมภายนอกองค์กร (ต่อ)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	3) เกิดการแย่งชิงข้อมูล เนื่องจากเกิดความเข้าใจที่ไม่ตรงกันระหว่างธนาคารและคู่ค้าในการกำหนดผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูล ซึ่งเกิดจากการแย่งชิงข้อมูลกัน เนื่องจากหาข้อดีความว่าผู้ให้บริการเป็นผู้ประมวลผลข้อมูลจะไม่สามารถกระทำการเกี่ยวกับข้อมูลนอกเหนือคำสั่งของธนาคารได้ ซึ่งหากบริษัทที่มีอำนาจในการต่อรองมากกว่าก็จะผลักดันให้อีกฝั่งเป็นผู้ประมวลผลข้อมูล

5.1.2 แนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

แนวทางการบริหารจัดการองค์กรเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควบคู่กับการดำเนินธุรกิจอย่างมีประสิทธิภาพนั้นต้องมีการบริหารจัดการทั้งปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กร

ปัจจัยสภาพแวดล้อมภายในองค์กรมีองค์ประกอบสำคัญ 3 องค์ประกอบ ได้แก่ คน (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) ซึ่งบริษัทจะต้องบริหารทุกองค์ประกอบให้มีความสอดคล้องซึ่งกันและกันจะขาดองค์ประกอบใดองค์ประกอบหนึ่งไม่ได้ โดยเป็นไปตามกลยุทธ์และนโยบายขององค์กร อย่างไรก็ตามก็ต้องคำนึงถึงปัจจัยภายนอกองค์กรร่วมด้วย ได้แก่ ลูกค้า คู่ค้า โดยมีรายละเอียดเพิ่มเติม ดังนี้

5.1.2.1 ปัจจัยสภาพแวดล้อมภายในองค์กร

(1) คน (People)

จากการสัมภาษณ์กลุ่มตัวอย่างมีความเห็นไปในทิศทางเดียวกันว่าแนวทางการบริหารจัดการด้านคนในองค์กรเพื่อให้บรรลุวัตถุประสงค์การปฏิบัติตามกฎหมายสามารถแบ่งออกได้ 4 ประเด็น ดังนี้

1. การสร้าง Tone at the Top จากผู้บริหาร

คนเป็นองค์ประกอบที่มีความเสี่ยงและสามารถควบคุมได้ยากที่สุดในทั้งหมด 3 ปัจจัย ซึ่งเรื่องของคนต้องเริ่มตั้งแต่ Tone at the Top จากผู้บริหารก่อนอันดับแรก

ผู้บริหารต้องให้ความสำคัญ มีความเอาใจจริงเอาใจและทำให้เห็นเป็นแบบอย่างในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล

2. การออกแบบโครงสร้างองค์กรที่เหมาะสมและทักษะความรู้ของคนที่เหมาะสมกับงาน

มีการแต่งตั้งตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จากหัวหน้างานของส่วนงานที่เกี่ยวข้องกับการปรับใช้กฎหมาย เช่น หัวหน้างานกำกับดูแลกิจการ หัวหน้างานบริหารความเสี่ยง หัวหน้างานกฎหมาย เป็นต้น ส่วนทีมงานที่เข้ามาสนับสนุนการทำงานของ DPO ก็จะเป็นบุคลากรที่มีทักษะทางด้านกฎหมาย ไอที หรือกระบวนการธุรกิจ โดยควรแยกออกมาเป็นอีกหนึ่งส่วนงานที่ดูแลด้านข้อมูลส่วนบุคคลและมี DPO เป็นผู้บังคับบัญชาของส่วนงานในระดับ C-Levels หรืออาจจะตั้งแผนกงานที่ดูแลข้อมูลทั้งองค์กรและกำหนดให้ DPO และทีมงานเป็นส่วนงานหนึ่งในแผนกที่ดูแลเรื่องข้อมูลส่วนบุคคลโดยเฉพาะ และกำหนดให้ DPO สามารถรายงานตรงต่อผู้มีอำนาจตัดสินใจสูงสุดขององค์กร

3. การสื่อสาร การให้ความรู้และการสร้างการตระหนักรู้ (Awareness)

สิ่งที่สำคัญที่สุดเรื่องของคน คือ การสื่อสารและการให้ความรู้แก่คนในองค์กรทุกระดับตั้งแต่คณะกรรมการบริษัทไปจนถึงพนักงานปฏิบัติการ โดยให้เข้าใจเกี่ยวกับบทบาทหน้าที่ของแต่ละระดับในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล ควบคู่ไปกับการสร้างความตระหนักรู้ (Awareness) ถึงมุมมองความเสี่ยง หลักการใช้ข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมาย ผ่านช่องทางการสื่อสารต่าง ๆ เช่น การอบรมที่มีการออกแบบอย่างเหมาะสมกับแต่ละระดับทั้งเนื้อหาและรูปแบบรวมถึงการวัดและประเมินผล การทำ Work Shop เพื่อให้เห็นภาพการปฏิบัติงานจริง หรือ ช่องทางสื่อสารอื่น ๆ ขององค์กร เป็นต้น และปัจจัยอีกประการที่สำคัญคือการสร้างวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคลให้กับคนในองค์กร (Protection Culture) ให้คนในองค์กรรู้ว่าอะไรเป็นสิ่งที่ควรทำหรือไม่ควรทำ

4. การกำหนดบทลงโทษและการบังคับใช้

มีการกำหนดบทลงโทษผ่านกฎระเบียบของบริษัทหรือกำหนดเป็นหนึ่งใน KPI โดยหากปฏิบัติไม่เป็นไปตามระเบียบที่บริษัทกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะมีผลลบต่อ KPI และมีการบังคับใช้อย่างจริงจัง แต่อย่างไรก็ตามเพื่อไม่ให้เป็นการบรรยากาศการทำงานที่หนักแล้ว ควรเริ่มต้นจากการชื่นชมพนักงานที่สามารถทำได้ดีซึ่งจะเป็นการสร้างแบบอย่างให้กับคนอื่น ๆ ในองค์กร

(2) กระบวนการ (Process)

กลุ่มตัวอย่างมีความเห็นไปในทิศทางเดียวกันถึงแนวทางการบริหารจัดการกระบวนการทำงานให้ตอบรับกับการกฎหมาย โดยสามารถแบ่งออกเป็น 5 ประเด็น ดังนี้

1. ออกแบบกระบวนการบริการจัดการข้อมูล (เก็บรวบรวม ใช้ เปิดเผย)
ให้เป็นไปตามกฎหมายกำหนด

โดยต้องมีการทบทวนกระบวนการปฏิบัติงานทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและกระบวนการไหลของข้อมูล เพื่อออกแบบกระบวนการทำงานที่เป็นไปตามข้อกำหนดของกฎหมาย โดยจะทำการเก็บข้อมูลส่วนบุคคลให้เท่าที่จำเป็นให้น้อยที่สุดเพื่อลดความเสี่ยงและสามารถออกแบบการประมวลผลข้อมูลโดยใช้ข้อมูลให้น้อยลงแต่ได้ผลลัพธ์ที่มากขึ้น ซึ่งข้อมูลที่บริษัทเก็บ ใช้และเปิดเผยต้องมีฐานกฎหมายรองรับการเก็บนั้น ๆ แต่โดยส่วนมากแล้วจะเน้นไปที่ฐานกฎหมายอื่นก่อนเลือกระบุเป็นฐานความยินยอม (Consent) เนื่องจากบริษัทจะมีภาระที่เพิ่มมากขึ้น

ส่วนเรื่องการขอความยินยอมจากลูกค้า การตลาดจะออกแบบการให้บริการและเนื้อหาของการขอความยินยอม (Consent) ที่มุ่งใจให้ลูกค้ารู้สึกว่าได้ประโยชน์จากการให้ข้อมูลหรือหากจะมีการมุ่งใจด้วยสิ่งของอื่นใดต้องพิจารณาถึงต้นทุนที่ต้องจ่ายว่าคุ้มค่าหรือไม่ เพราะลูกค้าสามารถถอนความยินยอมได้

2. ออกแบบกระบวนการควบคุมข้อมูลตามความเสี่ยงของข้อมูล

มีกระบวนการประเมินความเสี่ยงของข้อมูลเพื่อออกแบบการควบคุมข้อมูลให้เหมาะสมกับความเสี่ยง รวมถึงมีการจำกัดการเข้าถึงข้อมูลส่วนบุคคลให้เฉพาะผู้ที่มีความจำเป็นเท่านั้นสามารถเข้าถึงได้

3. กระบวนการรักษาความปลอดภัย (Data Security)

จัดให้มีมาตรฐานการรักษาความปลอดภัยของข้อมูลแต่เนื่องจากกฎหมายไม่ได้กำหนดมาตรฐานที่ชัดเจน ในปัจจุบันจึงยึดมาตรฐานของทางไอที ตาม ISO 27001 เป็นหลัก

4. ออกแบบกระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล

ออกแบบกระบวนการที่คอยดูแลเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูล และการแจ้งเหตุการณ์ข้อมูลรั่วไหลภายใน 72 ชั่วโมง

5. กระบวนการตรวจสอบ

จัดให้มีกระบวนการตรวจสอบการปฏิบัติตามแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบขององค์กร เช่น หน่วยงานตรวจสอบภายใน หน่วยงานกำกับดูแลกิจการ หรือทีมตรวจสอบการปฏิบัติตามกฎหมายที่บริษัทตั้งขึ้น

(3) เทคโนโลยี (Technology)

กลุ่มตัวอย่างมีความเห็นไปในทิศทางเดียวกันถึงแนวทางบริหารจัดการกระบวนการทำงานให้ตอบรับกับการกฎหมาย โดยสามารถแบ่งออกเป็น 2 ประเด็น ดังนี้

1. ลงทุนในเทคโนโลยี ด้านการรักษาความปลอดภัยและการบริหารจัดการการขอความยินยอม (Consent Management)

เทคโนโลยีเป็นปัจจัยหนึ่งที่เข้ามาช่วยในการปรับใช้พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ในเรื่องต่าง ๆ เช่น ช่องทางการขอความยินยอม ลดความผิดพลาดจากการปฏิบัติงานของคน (Human Error) Tracking ข้อมูลได้ เรียกดูกิจกรรมการไหลของข้อมูล (Data Log Activity) และตรวจสอบการรั่วไหลของข้อมูลได้ง่ายกว่าข้อมูลที่เป็น Hard Copy ปัจจุบันบริษัทมีการลงทุนในเทคโนโลยีด้านการรักษาความปลอดภัยข้อมูล การบริหารจัดการการขอความยินยอม (Consent Management) ส่วนซอฟต์แวร์ PDPA สำเร็จรูปในปัจจุบันธนาคารเห็นว่ายังไม่ที่ครอบคลุมการปฏิบัติงานตาม PDPA ได้อย่างสมบูรณ์จึงยังไม่มีการลงทุนในส่วนนี้ แต่หากเห็นว่าซอฟต์แวร์มีประสิทธิภาพมากพอบริษัทก็พร้อมที่จะลงทุน

2. เตรียมลงทุนในส่วนของการบริหารจัดการเกี่ยวกับสิทธิของเจ้าของข้อมูล

บริษัทเตรียมการลงทุนในส่วนของการบริหารจัดการสิทธิของเจ้าของข้อมูลโดยเฉพาะสิทธิในการโอนข้อมูล Data Portability ซึ่งจะต้องรอความชัดเจนของกฎหมายว่ากฎหมายมีความมุ่งหวังให้บริษัทดำเนินการในลักษณะใดจึงจะมีการลงทุนครั้งใหญ่เกี่ยวกับเรื่องดังกล่าว

แต่อย่างไรก็ตามการใช้เทคโนโลยีเข้ามาช่วยในการปฏิบัติงานก็ต้องพิจารณาถึงการดำเนินงานขององค์กรด้วยว่าเป็นไปในทิศทางมุ่งเน้นในเทคโนโลยีหรือไม่ หากไม่ได้เป็นไปในทิศทางเทคโนโลยีมากนักก็อาจใช้กระบวนการอื่นเข้ามาทดแทนการให้เทคโนโลยีได้ และอีกปัจจัยที่สำคัญ คือ เรื่องงบประมาณของบริษัทที่จะลงทุนในเรื่องเหล่านี้ด้วย เนื่องจากธนาคารมีประเด็นปัญหาและความเสี่ยงที่หลากหลายอาจจะต้องพิจารณาจัดลำดับความสำคัญในการลงทุนด้วย อีกทั้งต้องพิจารณาเพิ่มด้วยว่าการใช้เทคโนโลยีเข้ามาช่วยในการทำงานให้มีความสะดวกมากขึ้นก็จริงแต่ก็แลกมาด้วยความเสี่ยงจากการรั่วไหลของข้อมูลที่มีผลกระทบมหาศาล ดังนั้นเพื่อบริหารความเสี่ยงนี้จึงต้องมีการลงทุนทางด้านการรักษาความปลอดภัยเพิ่มขึ้นตามความเสี่ยงที่เพิ่มมากขึ้นด้วย

ท้ายที่สุดแล้วการทำงานแบบสอดคล้องประสานกันทั้ง 3 องค์ประกอบในองค์ประกอบที่สำคัญที่สุดก็คือเรื่องของคนที่ต้องเน้นย้ำอย่างหนัก แม้ว่าจะมีการวางแผนและออกแบบกระบวนการมาอย่างดีและมีการลงทุนในเทคโนโลยีที่เหมาะสมอย่างเต็มที่แล้วซึ่งเป็นจุดที่บริษัทสามารถควบคุมได้ทั้ง 2 องค์ประกอบแต่องค์ประกอบสุดท้ายอย่างคนซึ่งเป็นองค์ประกอบที่ควบคุมได้ยากที่สุด ดังนั้นจึงต้องอาศัยการให้ความรู้ จนเกิดความตระหนักรู้ และเกิดเป็นวัฒนธรรมแห่งการคุ้มครองข้อมูลส่วนบุคคลควบคู่กับการควบคุมตรวจสอบจากหน่วยงานภายในองค์กรจึงจะทำให้

ให้บริษัทบรรลุวัตถุประสงค์การปฏิบัติตามกฎหมายอย่างแท้จริง แต่อย่างไรก็ตามทั้ง 3 องค์ประกอบนี้ควรอยู่บนหลักของการใช้ต้นทุนน้อยที่สุดแต่สามารถปฏิบัติได้ตามที่กฎหมายกำหนด อย่างน้อยที่สุดหากไม่ได้เป็นการสร้างรายได้เพิ่มก็ถือว่าเป็นการไม่ทำให้เกิดค่าใช้จ่ายที่มากเกินไปจากค่าปรับและที่มากไปกว่านั้นคือชื่อเสียงของบริษัทที่ไม่สามารถประเมินมูลค่าได้ แต่หากจะเหนือไปกว่านั้นคือการนำเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของบริษัทไปสร้างโอกาสในการแข่งขันได้

ดังนั้นสามารถสรุปได้ว่าแนวทางการบริหารจัดการองค์กรเพื่อให้ตอบสนองต่อการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กลุ่มผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมีความเห็นไปในทิศทางเดียวกัน คือ องค์ประกอบของสภาพแวดล้อมภายในองค์กรที่สำคัญประกอบด้วย คน(People) กระบวนการ(People) และเทคโนโลยี (Technology) ซึ่งสอดคล้องกับบทความของ ธนาคารแห่งประเทศไทย (2557) ซึ่งกล่าวว่า Information Governance มีบทบาทนอกเหนือจากการดูแลข้อมูลตั้งแต่ต้นจนจบ แต่ยังครอบคลุมถึงการบริหารจัดการความเสี่ยงการใช้งานให้ถูกต้องตามกฎหมายระเบียบและกระบวนการทำงาน โดยอาศัย 3 ปัจจัยหลักเข้ามาควบคุม คือ คน (People), กระบวนการ (Process) และเทคโนโลยี (Technology) โดย 3 ปัจจัยดังกล่าวจำเป็นต้องสอดคล้องตามนโยบายและกลยุทธ์ขององค์กร ตามแนวคิด คน กระบวนการ และเทคโนโลยี (PPT Framework)

ตารางที่ 5.4

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (ปัจจัยสภาพแวดล้อมภายในองค์กร)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
ธนาคารแห่งประเทศไทย (2557) บทความ Information Governance (IG) กล่าวว่า IG มีบทบาทนอกเหนือจากการดูแลข้อมูลตั้งแต่ต้นจนจบ แต่ยังครอบคลุมถึงการบริหารจัดการความเสี่ยงการใช้งานให้ถูกต้องตามกฎหมายระเบียบและกระบวนการทำงาน โดยอาศัย 3 ปัจจัยหลักเข้ามาควบคุม คือ คน (People), กระบวนการ (Process) และเทคโนโลยี(Technology) โดย 3 ปัจจัยดังกล่าวจำเป็นต้องสอดคล้องตามนโยบายและกลยุทธ์ขององค์กร ตามแนวคิด คน กระบวนการ และเทคโนโลยี (PPT Framework)	แนวทางการบริหารจัดการองค์กรเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาศัยปัจจัยภายในองค์กร 3 องค์ประกอบ ได้แก่ คน (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) ซึ่ง บริษัทจะต้องบริหารทุกองค์ประกอบให้มีความสอดคล้องซึ่งกันและกัน จะขาดองค์ประกอบใดองค์ประกอบหนึ่งไม่ได้ และเป็นไปตามกลยุทธ์และนโยบายขององค์กร

ตารางที่ 5.4

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย
(ปัจจัยสภาพแวดล้อมภายในองค์กร) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
1) People: ส่งเสริมและสร้างความตระหนัก (Awareness) ให้กับพนักงานในการใช้และส่งต่อข้อมูลสำคัญด้วยความระมัดระวัง โดยใช้ช่องทางที่ปลอดภัย หรือเข้ารหัสข้อมูลด้วยโปรแกรมเสริม พร้อมทั้งประชาสัมพันธ์ และจัดงานให้ความรู้ ความเข้าใจในวงกว้าง	แนวทางการบริหารจัดการเรื่องคน (People) สามารถแบ่งได้เป็น 4 ประเด็น ดังนี้ 1) การสร้าง Tone at the Top จากผู้บริหาร ผู้บริหารต้องให้ความสำคัญ มีความเอาใจจริงเอาใจ และทำให้เห็นเป็นแบบอย่างในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล 2) การออกแบบโครงสร้างองค์กรที่เหมาะสมและทักษะความรู้ของคนที่เหมาะสมกับงาน โดยต้องจัดให้มีส่วนงานดูแลด้านข้อมูลส่วนบุคคลแยกออกมาต่างหากโดยมี DPO เป็นผู้บังคับบัญชาของส่วนงานในระดับ C-Levels หรืออาจจะตั้งแผนกงานที่ดูแลข้อมูลทั้งองค์กรและกำหนดให้ DPO และทีมงานเป็นส่วนงานหนึ่งในแผนกที่ดูแลเรื่องข้อมูลส่วนบุคคลโดยเฉพาะ และกำหนดให้ DPO สามารถรายงานตรงต่อผู้มีอำนาจตัดสินใจสูงสุดขององค์กร ซึ่งคนที่จะมาดำรงตำแหน่ง DPO และทีมงานต้องมีทักษะความรู้เรื่องกฎหมาย ไอที หรือกระบวนการธุรกิจ 3) การสื่อสาร การให้ความรู้และการสร้างการตระหนักรู้ (Awareness) สิ่งที่สำคัญที่สุดเรื่องของคนคือ การสื่อสารและการให้ความรู้แก่คนในองค์กรทุกระดับให้เข้าใจกฎหมาย บทบาทหน้าที่ของตน ควบคู่ไปกับการสร้างความตระหนักรู้ (Awareness) เกี่ยวกับข้อมูลส่วนบุคคล และการสร้างวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคล(Protection Culture) ให้กับคนในองค์กร 4) การกำหนดบทลงโทษและการบังคับใช้ มีการ

ตารางที่ 5.4

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย
(ปัจจัยสภาพแวดล้อมภายในองค์กร) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	กำหนดบทลงโทษผ่านกฎระเบียบของบริษัทหรือกำหนดเป็นหนึ่งใน KPI และมีการบังคับใช้อย่างจริงจัง แต่อย่างไรก็ตามเพื่อไม่ให้เป็นบรรยากาศการทำงานที่หนักอึ้ง ควรเริ่มต้นจากการชื่นชมพนักงานที่สามารถทำได้ดีซึ่งจะเป็นการสร้างแบบอย่างให้กับคนอื่น ๆ ในองค์กร
2) Process: มีระเบียบและพิธีปฏิบัติ เพื่อให้พนักงานได้ปฏิบัติตาม รวมถึงมีกระบวนการต่าง ๆ ในการปฏิบัติงานสำหรับพนักงานที่มีหน้าที่ดูแลระบบให้มีความปลอดภัย และพร้อมใช้งาน	แนวทางบริหารจัดการกระบวนการทำงานให้ตอบรับกับการกฎหมาย โดยสามารถแบ่งออกเป็น 5 ประเด็น ดังนี้ 1) ออกแบบกระบวนการบริหารจัดการข้อมูล (เก็บรวบรวม ใช้ เปิดเผย) ให้เป็นไปตามกฎหมายกำหนด โดยจะทำการเก็บข้อมูลส่วนบุคคลให้เท่าที่จำเป็นให้น้อยที่สุดเพื่อลดความเสี่ยงและสามารถออกแบบการประมวลผลข้อมูลที่มีประสิทธิภาพมากขึ้น และเรื่องการขอความยินยอม (Consent) การตลาดจะออกแบบการให้บริการและเนื้อหาของ Consent ที่มุ่งใจให้ลูกค้ารู้สึกว่าได้ประโยชน์จากการให้ข้อมูล 2) ออกแบบกระบวนการควบคุมข้อมูลตามความเสี่ยงของข้อมูล รวมถึงมีการจำกัดการเข้าถึงข้อมูลส่วนบุคคลให้เฉพาะผู้ที่มีความจำเป็นเท่านั้นสามารถเข้าถึงได้และเข้าถึงในข้อมูลที่มีความจำเป็นเท่านั้น 3) กระบวนการรักษาความปลอดภัย (Data Security) จัดให้มีมาตรฐานการรักษาความปลอดภัยของข้อมูล แต่เนื่องจากกฎหมายไม่ได้กำหนดมาตรฐานที่ชัดเจนในปัจจุบันจึงยึดมาตรฐานของทางไอที ตาม ISO 27001 เป็นหลัก

ตารางที่ 5.4

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย
(ปัจจัยสภาพแวดล้อมภายในองค์กร) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
	4) ออกแบบกระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูล และการแจ้งเหตุการณ์ข้อมูลรั่วไหลภายใน 72 ชั่วโมง 5) กระบวนการตรวจสอบ จัดให้มีกระบวนการตรวจสอบการปฏิบัติตามแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบขององค์กร
3) Technology: มีการประยุกต์ใช้เครื่องมือและอุปกรณ์เพื่อป้องกัน ภัยคุกคามในทุกระดับ (Layer) ทั้งความเสี่ยงที่อาจเกิดขึ้นจากภายนอก และภายใน เพื่อปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น	แนวทางบริหารจัดการเทคโนโลยี แบ่งออกเป็น 2 ประเด็น ดังนี้ 1) ลงทุนในเทคโนโลยี ด้านการรักษาความปลอดภัย และการบริหารจัดการการขอความยินยอม (Consent Management) บริษัทต้องลงทุนในเทคโนโลยีด้านการรักษาความปลอดภัยข้อมูล การบริหารจัดการการขอความยินยอม (Consent Management) ส่วนของซอฟต์แวร์ PDPA สำเร็จรูปในปัจจุบันธนาคารเห็นว่ายังไม่ที่ครอบคลุมการปฏิบัติงานตาม PDPA ได้อย่างสมบูรณ์จึงยังไม่มีการลงทุนในส่วนนี้ แต่หากเห็นว่าซอฟต์แวร์ใดมีประสิทธิภาพมากพอบริษัทก็พร้อมที่จะลงทุน 2) เตรียมลงทุนในส่วนของการบริหารจัดการเกี่ยวกับสิทธิของเจ้าของข้อมูล โดยเฉพาะสิทธิในการโอนข้อมูลซึ่งจะต้องรอความชัดเจนของกฎหมายว่ากฎหมายมีความมุ่งหวังให้บริษัทดำเนินการในลักษณะใดจึงจะมีการลงทุนครั้งใหญ่เกี่ยวกับเรื่องดังกล่าว

5.1.2.2 ปัจจัยสภาพแวดล้อมภายนอกองค์กร

มีองค์ประกอบหลัก 2 องค์ประกอบ ดังนี้

(1) ลูกค้า (Customer)

จากการสัมภาษณ์กลุ่มตัวอย่าง พบว่า ณ ปัจจุบันกลุ่มลูกค้าส่วนใหญ่ยังไม่ตื่นตัวกับกฎหมายเท่าไรนักหรืออาจจะมีความเข้าใจที่ไม่ครบถ้วนหรือไม่ตรงกันกับบริษัทในบางส่วน ด้วยการให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยที่ยังไม่มากนัก ไม่ได้มีการปลูกฝังกันมาอย่างยาวนานอย่างในต่างประเทศ จึงเป็นเรื่องที่ใหม่สำหรับคนไทย แต่อย่างไรก็ตามลูกค้า คือ หัวใจสำคัญของการทำธุรกิจให้ประสบความสำเร็จ ดังนั้นจึงมีแนวทางในการปฏิบัติต่อลูกค้าที่สำคัญ คือ การสื่อสาร (Communication)

โดยมีการออกแบบการขอความยินยอม (Consent) ซึ่งมีเนื้อหา (Content) ที่ทำให้ลูกค้ารู้สึกถึงประโยชน์ของการให้ความยินยอมและเข้าใจสิทธิของลูกค้าในฐานะเจ้าของข้อมูลพร้อมกับสิทธิของบริษัทในการเก็บข้อมูลของลูกค้าตามฐานการประมวลอื่น ๆ ที่ได้รับยกเว้นไม่จำเป็นต้องขอความยินยอมเพื่อความเข้าใจที่ตรงกันระหว่างบริษัทและลูกค้าลดการฟ้องร้อง ซึ่งจะทำให้ลูกค้ามีความเต็มใจและยินยอมที่จะให้ข้อมูลแก่บริษัท นอกจากนี้ยังต้องสื่อสารถึงมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความเชื่อมั่นให้กับลูกค้าในการใช้บริการและการยินยอมให้ข้อมูล อีกทั้งยังต้องสื่อสารให้ลูกค้าตระถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูล

ดังนั้นสามารถสรุปได้ว่าแนวทางการบริหารจัดการลูกค้า นั้น ผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญมองว่าสิ่งที่สำคัญ คือ การสื่อสาร โดยต้องสื่อสารให้ลูกค้าตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลและให้ลูกค้ารู้สึกถึงประโยชน์ของการให้ความยินยอม รวมถึงสื่อสารเรื่องมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความเชื่อมั่นและยินยอมให้ข้อมูลแก่บริษัทด้วย ซึ่งสอดคล้องกับบทความของ Emma (2019) กล่าวว่า อุตสาหกรรมดิจิทัลเป็นอุตสาหกรรมที่มีข้อมูลเป็นศูนย์กลาง ดังนั้นจึงขึ้นอยู่กับความไว้วางใจของผู้บริโภค วิธีหนึ่งที่ดีที่สุดในการสร้างความไว้วางใจคือการแสดงให้เห็นว่าแนวทางปฏิบัติในการจัดการข้อมูลขององค์กรนั้นมีประสิทธิภาพและมีจริยธรรม รวมถึงการสื่อสารที่มีประสิทธิภาพกับลูกค้าเพื่อให้มั่นใจว่าข้อมูลของพวกเขาปลอดภัยจึงจะเกิดเป็นความได้เปรียบในการแข่งขัน

(2) คู่ค้า (Supplier/Vendor)

การพิจารณาคัดเลือกผู้ให้บริการรายใหม่และการต่อสัญญาเก่าของธนาคารจะต้องเพิ่มหลักเกณฑ์เกี่ยวกับการให้บริการที่ได้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายกำหนดพร้อมจัดทำสัญญาการประมวลผลข้อมูล รวมถึงมีการตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการรายนั้น ๆ ด้วย สำหรับการจ้างงานในลักษณะที่เกี่ยวข้องกับ

ข้อมูลส่วนบุคคลธนาคารควรดึงกลับมาทำเองให้มากที่สุดเพื่อให้ข้อมูลส่วนบุคคลไหลออกไปนอกธนาคารให้น้อยที่สุดเพื่อเป็นการลดความเสี่ยง

ดังนั้นสามารถสรุปได้ว่าแนวทางการบริหารจัดการคู่ค้าผู้ปฏิบัติงานภาคธนาคารและผู้เชี่ยวชาญเห็นว่า บริษัทควรต้องเพิ่มหลักเกณฑ์เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในการพิจารณาคัดเลือกคู่ค้า ซึ่งสอดคล้องกับบทความของ วิชญ์ วงศ์หาญเชาว์ (2562) กล่าวว่า สำหรับองค์กรที่ทำงานร่วมกับผู้ให้บริการด้านไอที หรืออยู่ระหว่างพิจารณาคัดเลือกผู้ให้บริการระบบความปลอดภัยเพิ่มเติมจะต้องแน่ใจว่าผู้ให้บริการหรือเวนเดอร์นั้น ๆ จะต้องเข้าใจ และให้ความสำคัญกับงานด้านความปลอดภัยในการประมวลผลข้อมูลตามกฎหมายของ GDPR นอกจากนี้ยังมีประเด็นเพิ่มเติมจากองค์ความรู้เดิม คือ บริษัทต้องมีการเข้าไปตรวจสอบมาตรฐานการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัทคู่ค้าและการดำเนินงานในลักษณะที่เกี่ยวข้องกับข้อมูลส่วนบุคคลธนาคารควรดึงกลับมาทำเองให้มากที่สุดเพื่อให้ข้อมูลส่วนบุคคลไหลออกไปนอกธนาคารให้น้อยที่สุดเพื่อเป็นการลดความเสี่ยง

ตารางที่ 5.5

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (ปัจจัยสภาพแวดล้อมภายนอกองค์กร)

องค์ความรู้เดิมและงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
บทความของ Emma (2019) เรื่องผลกระทบของ GDPR ต่อ Digital Banking กล่าวว่า อุตสาหกรรมดิจิทัลเป็นอุตสาหกรรมที่มีข้อมูลเป็นศูนย์กลาง ดังนั้นจึงขึ้นอยู่กับความไว้วางใจของผู้บริโภค วิธีหนึ่งที่ดีที่สุดในการสร้างความไว้วางใจคือการแสดงให้ลูกค้าเห็นว่าแนวทางปฏิบัติในการจัดการข้อมูลขององค์กรนั้นมีประสิทธิภาพและมีจริยธรรม รวมถึงการสื่อสารที่มีประสิทธิภาพกับลูกค้าเพื่อให้มั่นใจว่าข้อมูลของพวกเขาปลอดภัยจึงจะเกิดเป็นความได้เปรียบในการแข่งขัน	แนวทางการบริหารจัดการลูกค้าที่สำคัญ คือ เรื่องของการสื่อสาร (Communication) ต้องมีการออกแบบการขอความยินยอม (Consent) ซึ่งมีเนื้อหา (Content) ที่ทำให้ลูกค้ารู้สึกถึงประโยชน์ของการให้ความยินยอมและเข้าใจสิทธิของเจ้าของข้อมูลและสิทธิของบริษัทในการเก็บข้อมูลของลูกค้าตามฐานการประมวลอื่น ๆ ที่ไม่จำเป็นต้องขอความยินยอม เพื่อความเข้าใจที่ตรงกันระหว่างบริษัทและลูกค้าลดการฟ้องร้อง ซึ่งจะทำให้ลูกค้ามีความเต็มใจและยินยอมที่จะให้ข้อมูลแก่บริษัท นอกจากนี้ยังต้องสื่อสารถึงมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความเชื่อมั่นให้กับลูกค้าในการใช้บริการและการยินยอมให้ข้อมูล อีกทั้งยังต้องสื่อสารให้ลูกค้าตระถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูล

ตารางที่ 5.5

สรุปแนวทางการบริหารจัดการองค์กรเพื่อตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย (ปัจจัยสภาพแวดล้อมภายนอกองค์กร) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
บทความ GDPR กับการบริหารความเสี่ยงของข้อมูลส่วนบุคคลเพื่อแต้มต่อทางธุรกิจ วิชญ์ วงศ์หาญเขาว์ (2562) กล่าวว่า สำหรับองค์กรที่ทำงานร่วมกับผู้ให้บริการด้านไอที หรืออยู่ระหว่างพิจารณาคัดเลือกผู้ให้บริการระบบความปลอดภัยเพิ่มเติม จะต้องแน่ใจว่าผู้ให้บริการหรือเวนเดอร์นั้น ๆ จะต้องเข้าใจ และให้ความสำคัญกับงานด้านความปลอดภัยในการประมวลผลข้อมูลตามกฎหมายของ GDPR	1) บริษัทควรต้องเพิ่มหลักเกณฑ์เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในการพิจารณาคัดเลือกผู้ให้บริการพร้อมจัดทำสัญญาการประมวลผลข้อมูล รวมถึงมีการตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการรายนั้น ๆ ด้วย 2) การจ้างงานในลักษณะที่เกี่ยวข้องกับข้อมูลส่วนบุคคลธนาคารควรดึงกลับมาทำเองให้มากที่สุด เพื่อให้ข้อมูลส่วนบุคคลไหลออกไปนอกธนาคารให้น้อยที่สุดเพื่อเป็นการลดความเสี่ยง

5.1.3 แนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กลุ่มธุรกิจธนาคารพาณิชย์และผู้เชี่ยวชาญมีความเห็นเป็นไปในทิศทางเดียวกันโดยมองว่าแนวทางการพัฒนาองค์กรเพื่อตอบรับกับการปฏิบัติตามข้อบังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นการหาจุดสมดุลในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เป็นภาระของภาคธุรกิจมากเกินไป โดยต้องเป็นความร่วมมือกันทั้งภาครัฐและภาคเอกชนในการช่วยกันผลักดันให้เกิดการบังคับใช้กฎหมายที่เป็นประโยชน์อย่างสูงสุดทั้งฝั่งของผู้บริโภคและตัวองค์กรเอง โดยมีประเด็นแนวทางการพัฒนา 3 ประเด็น ดังนี้

5.1.3.1 มีแนวทางการปฏิบัติงานที่ชัดเจนสำหรับภาคธุรกิจ

เนื่องจากกฎหมายฉบับนี้ออกมาเพื่อปรับใช้กับทุกภาคธุรกิจซึ่งในแต่ละธุรกิจก็มีลักษณะการประกอบธุรกิจที่มีความเฉพาะเจาะจงและเงื่อนไขการปฏิบัติงานที่แตกต่างกัน ดังนั้นจึงควรมีการจัดทำแนวปฏิบัติกลางสำหรับภาคธุรกิจเพื่อให้เป็นมาตรฐานและแนวทางการปฏิบัติงานสำหรับภาคธุรกิจ ที่ได้รับความเห็นชอบจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานกำกับดูแล และกำหนดให้ธนาคารแห่งประเทศไทย เป็นผู้กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลของธนาคารโดยตรง ส่วนสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหน่วยงานกำกับดูแลของกฎหมายฉบับนี้จะเข้ามากำกับดูแลเพิ่มเติมผ่านธนาคารแห่งประเทศไทย

ไทย เพื่อสะดวกต่อการกำกับดูแลในภาคธุรกิจและเป็นการลดภาระของหน่วยงานกำกับดูแลที่ต้องดูแลทุกภาคธุรกิจซึ่งมีหลายภาคธุรกิจที่ไม่มีหน่วยงานกำกับดูแลโดยตรง

ซึ่งสอดคล้องกับบทความงานวิจัยของ กิตติพงศ์ กมลธรรมาวงศ์ (2563) ได้กล่าวถึงภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน โดยพบว่า ในช่วงแรกของการปรับใช้กฎหมายของประเทศมาเลเซียภาคเอกชนมีความตื่นตัวในการแลกเปลี่ยนข้อมูลเพื่อหาแนวทางปฏิบัติ ซึ่งองค์กรภาคการเงินที่มีมาตรฐานการคุ้มครองข้อมูลสูงจากการปฏิบัติตามกฎหมาย GDPR เนื่องจากมีความเชื่อมโยงกับบริษัทใน EU จึงได้แบ่งปันแนวปฏิบัติ (Guideline) ของภาคธุรกิจให้กับภาคธุรกิจอื่น แต่อย่างไรก็ตามจากการวิจัยมีประเด็นเพิ่มเติมจากองค์ความรู้เดิมในส่วนของการกำหนดให้ธนาคารแห่งประเทศไทย เป็นผู้กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลของธนาคารโดยตรง เพื่อสะดวกต่อการกำกับดูแลในภาคธุรกิจและเป็นการลดภาระของหน่วยงานกำกับดูแล

5.1.3.2 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริโภคและพนักงานภายในองค์กร

เรื่องของความรู้ ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จนเกิดความตระหนักรู้ (Awareness) เป็นปัจจัยพื้นฐานสำคัญที่จะทำให้กฎหมายฉบับนี้เกิดประโยชน์อย่างแท้จริงกับผู้บริโภคและภาคธุรกิจ

ในส่วนของผู้บริโภคภาครัฐ หน่วยงานกำกับ และธนาคาร ควรออกมาสื่อสาร ความเข้าใจเกี่ยวกับกฎหมาย สร้างความตระหนักรู้ (Awareness) เกี่ยวกับข้อมูลส่วนบุคคล รวมถึงสิทธิและประโยชน์ของผู้บริโภคในทิศทางเดียวกัน เพื่อให้ผู้บริโภคเข้าใจถึงสิทธิที่แท้จริงของตน และสิทธิของธนาคารซึ่งจะทำให้เกิดความเข้าใจที่ตรงกันกับธนาคารถึงการใช้สิทธิในข้อมูลส่วนบุคคล ในปัจจุบันผู้บริโภคมักถูกสื่อสารกันถึงสิทธิของลูกค้าในมุมเดียวแต่ไม่ได้สื่อสารถึงสิทธิในฝั่งธนาคาร และในภาคธนาคารเองก็ต้องมีการสื่อสารความรู้ ความเข้าใจและสร้างการตระหนักรู้ภายในองค์กรอย่างต่อเนื่องและเพิ่มความเข้มข้นขึ้นให้เกิดเป็นวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคล

ซึ่งสอดคล้องกับบทความงานวิจัยของ กิตติพงศ์ กมลธรรมาวงศ์ (2563) ที่ได้เสนอการเตรียมความพร้อมเพื่อการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ต้องสร้างการรับรู้ร่วมกันของสังคมไทยทุกภาคส่วนทั้งภาคเอกชน ภาครัฐและประชาชนไทยให้เข้าใจถึงข้อกำหนดตามกฎหมายและสร้างความตระหนักรู้ในความสำคัญของข้อมูลส่วนบุคคล ผ่านช่องทางสื่อสารต่าง ๆ และรูปแบบที่เหมาะสมกับกลุ่มเป้าหมายแต่ละกลุ่ม โดยเป็นความร่วมมือกันระหว่างภาครัฐและภาคเอกชนเพื่อเผยแพร่ความรู้ ความเข้าใจเกี่ยวกับเรื่องดังกล่าว

5.1.3.3 การควบคุม ติดตาม และประเมินผลการปฏิบัติงานหลังมีการปรับใช้จริงเพื่อปรับปรุงกระบวนการอย่างต่อเนื่อง

หลังจากมีการปรับใช้กฎหมายและธนาครได้ดำเนินการตามกระบวนการที่ได้ออกแบบไว้แล้วจะต้องมีกระบวนการตรวจสอบ ติดตาม และประเมินผลการปฏิบัติงาน เพื่อให้ทราบว่ากระบวนการที่วางไว้มีปัญหาอุปสรรคในการปฏิบัติงานหรือไม่ ทั้งในมุมของการปฏิบัติตามกฎหมายและความพึงพอใจของลูกค้า นอกจากนี้ยังเป็นการควบคุมการปฏิบัติงานให้เป็นไปตามกระบวนการที่ออกแบบไว้เพื่อให้เกิดการปรับปรุงกระบวนการอย่างต่อเนื่อง โดยปรับปรุงและพัฒนาควบคู่ไปกับธรรมาภิบาลข้อมูล (Data Governance)

ซึ่งสอดคล้องกับบทความ PDCA หัวใจสำคัญของการปรับปรุงอย่างต่อเนื่องของ สุธาสนี (2558) กล่าวว่า เครื่องมือสำหรับการปรับปรุงกระบวนการ Deming Cycle หรือ PDCA โดยมีเป้าหมายให้เกิดการพัฒนาอย่างต่อเนื่องปรับตัวให้สอดคล้องกับสถานการณ์ได้ เพื่อให้สามารถบรรลุวัตถุประสงค์ที่วางไว้ ซึ่งโครงสร้างของ PDCA ประกอบด้วย 1) Plan คือ การวางแผน 2) Do คือ การปฏิบัติตามแผน 3) Check คือ การตรวจสอบ 4) Act คือ การปรับปรุงการดำเนินการอย่างเหมาะสมหรือการจัดทำมาตรฐานใหม่ ซึ่งถือเป็นพื้นฐานของการยกระดับคุณภาพ

ดังนั้นสามารถสรุปได้ว่าการที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะเป็นประโยชน์ต่อทั้งผู้บริโภคและภาคธุรกิจเพียงแค่การออกกฎหมายอย่างเดียวไม่เพียงพอต้องมีแนวทางปฏิบัติที่ชัดเจนเป็นมาตรฐาน และที่สำคัญต้องมีความตระหนักรู้ของทั้งคนในองค์กรและผู้บริโภค ภาครัฐและภาคเอกชนต้องให้ความรู้กลุ่มคนเหล่านี้เป็นอย่างดีเพียงพอ และมีการปรับปรุงกระบวนการทำงานภายในองค์กรอย่างต่อเนื่อง

ตารางที่ 5.6

สรุปแนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
จากบทความงานวิจัยของ กิตติพงศ์ กมลธรรมวงศ์ (2563) ได้กล่าวถึงภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน โดยพบว่า ในช่วงแรกของการปรับใช้กฎหมายของประเทศมาเลเซียภาคเอกชนมีความตื่นตัวในการแลกเปลี่ยนข้อมูลเพื่อหาแนวทาง	ภาคธุรกิจธนาคารควรมีการจัดทำแนวปฏิบัติกลางสำหรับภาคธุรกิจเพื่อให้เป็นมาตรฐานและแนวทางการปฏิบัติงานสำหรับภาคธุรกิจ ที่ได้รับความเห็นชอบจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานกำกับดูแล นอกจากนี้เห็นควรให้หน่วยงานกำกับดูแลภาคธุรกิจโดยตรง

ตารางที่ 5.6

สรุปแนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
ปฏิบัติ ซึ่งองค์กรภาคการเงินที่มีมาตรฐานการคุ้มครองข้อมูลสูงจากการปฏิบัติตามกฎหมาย GDPR เนื่องจากมีความเชื่อมโยงกับบริษัทใน EU จึงได้แบ่งปันแนวปฏิบัติ (Guideline) ของภาคธุรกิจให้กับภาคธุรกิจอื่น	(ธนาคารแห่งประเทศไทย) เป็นผู้กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคลของธนาคารโดยตรง เพื่อสะดวกต่อการกำกับดูแลในภาคธุรกิจและเป็นการลดภาระของหน่วยงานกำกับดูแลที่ต้องดูแลทุกภาคธุรกิจซึ่งมีหลายภาคธุรกิจที่ไม่มีหน่วยงานกำกับดูแลโดยตรง
จากบทความงานวิจัยของ กิตติพงศ์ กมลธรรมวงศ์ (2563) ได้เสนอการเตรียมความพร้อมเพื่อการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยว่าสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องสร้างการรับรู้ร่วมกันของสังคมไทยทุกภาคส่วนทั้งภาคเอกชน ภาครัฐและประชาชนไทยให้เข้าใจถึงข้อกำหนดตามกฎหมายและสร้างความตระหนักรู้ในสำคัญของข้อมูลส่วนบุคคล ผ่านช่องทางสื่อสารต่าง ๆ ด้วยรูปแบบที่เหมาะสมกับกลุ่มเป้าหมายแต่ละกลุ่ม โดยเป็นความร่วมมือกันระหว่างภาครัฐและภาคเอกชน เพื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับเรื่องดังกล่าว	เรื่องของความรู้ ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จนเกิดความตระหนักรู้ (Awareness) เป็นปัจจัยพื้นฐานสำคัญที่จะทำให้กฎหมายฉบับนี้เกิดประโยชน์อย่างแท้จริงกับผู้บริโภคและภาคธุรกิจ โดยในส่วนของผู้บริโภค ภาครัฐ หน่วยงานกำกับ และธนาคาร ควรออกมาสื่อสาร ความเข้าใจเกี่ยวกับกฎหมาย สร้างความตระหนักรู้ (Awareness) เกี่ยวกับข้อมูลส่วนบุคคล รวมถึงสิทธิและประโยชน์ของผู้บริโภคในทิศทางเดียวกัน เพื่อให้ผู้บริโภคเข้าใจถึงสิทธิที่แท้จริงของตนและสิทธิของธนาคาร นอกจากนี้ในภาคธนาคารเองก็ต้องมีการสื่อสารความรู้ความเข้าใจและสร้างการตระหนักรู้ภายในองค์กรอย่างต่อเนื่องและเกิดเป็นวัฒนธรรมของการคุ้มครองข้อมูลส่วนบุคคล
บทความ PDCA หัวใจสำคัญของการปรับปรุงอย่างต่อเนื่องของ สุธาสิณี (2558) กล่าวว่า เครื่องมือสำหรับการปรับปรุงกระบวนการ Deming Cycle หรือ PDCA โดยมีเป้าหมายให้เกิดการพัฒนาอย่างต่อเนื่องปรับตัวให้สอดคล้องกับสถานการณ์ได้ เพื่อให้สามารถบรรลุวัตถุประสงค์ที่วางไว้ ซึ่งโครงสร้างของ PDCA	หลังจากมีการปรับใช้กฎหมายและธนาคารได้ดำเนินการตามกระบวนการที่ได้ออกแบบไว้แล้ว จะต้องมีการตรวจสอบ ติดตาม และประเมินผลการปฏิบัติงาน เพื่อให้ทราบว่ากระบวนการที่วางไว้มีปัญหาอุปสรรคในการปฏิบัติงานหรือไม่ ทั้งในมุมของการปฏิบัติตามกฎหมายและความพึงพอใจของลูกค้า นอกจากนี้ยัง

ตารางที่ 5.6

สรุปแนวทางการพัฒนาการบริหารองค์กรของธุรกิจธนาคารพาณิชย์ภายใต้การปฏิบัติตามข้อบังคับของกฎหมาย) (ต่อ)

องค์ความรู้เดิม และงานวิจัยที่สนับสนุน	สรุปประเด็นที่ได้จากการสัมภาษณ์
ประกอบด้วย 1) Plan คือ การวางแผน 2) Do คือ การปฏิบัติตามแผน 3) Check คือ การตรวจสอบ 4) Act คือ การปรับปรุงการดำเนินการอย่างเหมาะสมหรือการจัดทำมาตรฐานใหม่ ซึ่งถือเป็นพื้นฐานของการยกระดับคุณภาพ	เป็นการควบคุมการปฏิบัติงานให้เป็นไปตามกระบวนการที่ออกแบบไว้เพื่อให้เกิดการปรับปรุงกระบวนการอย่างต่อเนื่อง โดยปรับปรุงและพัฒนาควบคู่ไปกับธรรมาภิบาลข้อมูล (Data Governance)

5.2 ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

ทางนักวิจัยขอเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์เป็น 2 ส่วน ได้แก่ ประโยชน์ในการประยุกต์ใช้กับธุรกิจ (Implications for Business) และประโยชน์เชิงวิชาการ (Implication for Academic) โดยมีรายละเอียด ดังนี้

5.2.1 ประโยชน์ในการประยุกต์ใช้กับธุรกิจ (Implications for Business)

5.2.1.1 การให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลทั้งผู้บริโภคและพนักงานภายในองค์กร

เนื่องจากความรู้ ความเข้าใจในเรื่องเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนในประเทศนั้นยังไม่มีที่แพร่หลายมากนัก แม้ว่าในปัจจุบันจะเริ่มมีคนให้ความสนใจกับเรื่องดังกล่าวมากขึ้นก็ตาม จึงทำให้คนส่วนใหญ่ในประเทศยังไม่เกิดความตระหนักรู้ (Awareness) ถึงเรื่องการคุ้มครองข้อมูลส่วนบุคคลมากนัก รวมถึงการสื่อสารความรู้ความเข้าใจที่ครบถ้วนถูกต้องตรงกันระหว่างผู้ประกอบการและผู้บริโภคเพื่อเกิดความร่วมมือและลดความขัดแย้งระหว่างกัน และทำให้ลูกค้ายอมรับประโยชน์ในการในความยินยอม

ดังนั้นทั้งภาครัฐและภาคเอกชนต้องร่วมมือกันในการทำเรื่องดังกล่าว ซึ่งสามารถแบ่งเป็น 2 ช่วง ช่วงแรกระยะสั้น เนื่องจากกฎหมายที่ใกล้จะมีผลบังคับในเดือนมิถุนายน 2564 ดังนั้นทั้งภาครัฐที่เป็นหน่วยงานกำกับดูแลกฎหมาย หน่วยงานกำกับดูแลภาคธุรกิจและธนาคารพาณิชย์ต้องมีการสื่อสารกับผู้บริโภคให้มีความรู้เกี่ยวกับกฎหมาย ทั้งสิทธิของเจ้าของข้อมูล

ประโยชน์ที่ได้รับ และสิทธิในมูของธนาคาร โดยทั้งหน่วยงานภาครัฐและภาคธนาคารต้องสื่อสารไปในทิศทางเดียวกันเพื่อป้องกันความสับสนและสร้างความน่าเชื่อถือ อีกทั้งธนาคารพาณิชย์เองก็ต้องมีการสื่อสารกับคนภายในองค์กรด้วยเช่นกันเพื่อลดความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย และระยะยาวภาครัฐควรปลูกฝังความรู้ความเข้าใจของประชาชนในประเทศอย่างต่อเนื่องถึงความรู้ ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จนเกิดความตระหนักรู้ (Awareness) ซึ่งอาจต้องใช้เวลาพอสมควรเพราะถือเป็นเรื่องใหม่สำหรับประชาชนไทยจึงต้องทำอย่างต่อเนื่องและทั่วถึงอย่างในต่างประเทศที่ประสบความสำเร็จในเรื่องดังกล่าวใช้เวลาอย่างยาวนานเพราะความรู้ความเข้าใจและการตระหนักรู้ (Awareness) เป็นปัจจัยพื้นฐานสำคัญที่จะทำให้กฎหมายฉบับนี้เกิดประโยชน์อย่างแท้จริงกับผู้บริโภคและภาคธุรกิจอย่างแท้จริง

5.2.1.2 ภาคธุรกิจธนาคารพาณิชย์ควรศึกษามุมมองความคาดหวังของผู้บริโภคต่อการคุ้มครองข้อมูลส่วนบุคคล

ในช่วงที่ธนาคารอยู่ระหว่างการเตรียมการเพื่อปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้ความสำคัญกับการทำความเข้าใจและตีความกฎหมายหมายเพื่อออกแบบการปฏิบัติงานให้สอดคล้องกับกฎหมายและการสื่อสารกับคนในองค์กรเพื่อสร้างความรู้ความเข้าใจเกี่ยวกับตัวกฎหมาย แต่อย่างไรก็ตามลูกค้านั้นเป็นปัจจัยหนึ่งที่มีความสำคัญต่อการปรับใช้กฎหมายเช่นกันในฐานะของเจ้าของข้อมูล (Data Subject) และเป็นปัจจัยสำคัญที่จะทำให้ธุรกิจประสบความสำเร็จ ดังนั้นจึงควรศึกษาถึงมุมมองความคาดหวังของลูกค้าหรือผู้บริโภคว่าต้องการให้ธนาคารตอบสนองต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างไร และมีทิศทางความต้องการในเรื่องดังกล่าวมากน้อยเพียงใด เพื่อใช้ประกอบการพิจารณาออกแบบกระบวนการให้บริการที่เป็นไปตามกฎหมายและตรงกับความต้องการลูกค้ามากขึ้นเพื่อเป็นการสร้างโอกาสทางการแข่งขันในธุรกิจ เพราะไม่เพียงแต่ให้ความสำคัญในการปฏิบัติตามกฎหมายเท่านั้นแต่ยังคำนึงถึงความต้องการและความคาดหวังของลูกค้าอีกด้วย

5.2.1.3 ต้องมีการควบคุม ตรวจสอบ และประเมินผลเพื่อปรับปรุงกระบวนการปฏิบัติงานอย่างต่อเนื่อง

หลังจากที่มีการปรับใช้กฎหมายอย่างเต็มรูปแบบในเดือนมิถุนายน 2564 และการออกกฎหมายลำดับรองเพิ่มเติมรวมถึงแนวทางปฏิบัติต่าง ๆ ที่มีความชัดเจนในการปฏิบัติมากขึ้น ธนาคารต้องมีการควบคุม ตรวจสอบการปฏิบัติงานว่าเป็นไปตามกระบวนการที่ออกแบบไว้หรือไม่และเป็นไปตามที่กฎหมายกำหนดอย่างสม่ำเสมอ รวมถึงประเมินผลการปฏิบัติงานว่าเกิดปัญหาอุปสรรคและความเสี่ยงในกระบวนการใด อีกทั้งยังต้องพิจารณาถึงความพึงพอใจของผู้ใช้บริการอีกด้วย เพื่อปรับปรุงแก้ไขกระบวนการทำงานให้มีประสิทธิภาพมากขึ้น

5.2.2 ประโยชน์เชิงวิชาการ (Implication for Academic)

งานวิจัยนี้สามารถนำไปใช้ประโยชน์ให้ผู้ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ประยุกต์ใช้กับธุรกิจธนาคารและสามารถนำไปต่อยอดการศึกษาจากงานวิจัยนี้เพื่อศึกษาเพิ่มเติมหลังจากกฎหมายมีการบังคับใช้อย่างเต็มรูปแบบ มีการออกกฎหมายลำดับรอง และแนวปฏิบัติอื่น ๆ หรือศึกษาเพิ่มเติมในภาคอุตสาหกรรมอื่นต่อไป รวมถึงศึกษาถึงมุมมองและความคาดหวังของผู้บริโภคต่อการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจ

5.3 ข้อจำกัดของงานวิจัย

งานวิจัยฉบับนี้ได้ดำเนินการเก็บข้อมูลโดยการเข้าสัมภาษณ์ผู้ปฏิบัติงานในภาคธุรกิจธนาคารพาณิชย์และผู้เชี่ยวชาญในช่วงที่เดือนตุลาคม-พฤศจิกายน 2563 ซึ่งเป็นช่วงที่กฎหมายยังไม่บังคับใช้อย่างเต็มรูปแบบ อีกทั้งยังมีความไม่ชัดเจนจากกฎหมายในบางส่วนที่ต้องรอการออกกฎหมายลำดับรองและแนวทางการพิจารณาในเรื่องต่าง ๆ จากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลบางผลกระทบและมุมมองต่าง ๆ ของภาคธุรกิจในงานวิจัยฉบับนี้จึงอ้างอิงจากสถานการณ์ที่กล่าวไปข้างต้น หลังจากที่มีการปรับใช้อย่างเต็มรูปแบบและมีความชัดเจนของกฎหมายมากขึ้น ผลกระทบและมุมมองต่าง ๆ อาจจะเปลี่ยนแปลงไป

นอกจากนี้ยังมีข้อจำกัดในการเก็บข้อมูลกลุ่มตัวอย่าง เนื่องจากกลุ่มตัวอย่างในงานวิจัยฉบับนี้เป็นกลุ่มผู้บริหาร (Executive Management) ในภาคธุรกิจธนาคาร ซึ่งเป็นภาคธุรกิจขนาดใหญ่ จึงมีข้อจำกัดในการติดต่อเพื่อขอเข้าสัมภาษณ์ การวิจัยครั้งนี้จึงได้เข้าไปเก็บข้อมูลในกลุ่มธนาคารขนาดกลางถึงขนาดเล็เท่านั้น อีกทั้งยังไม่มีเก็บข้อมูลในมุมมองของกลุ่มเจ้าหน้าที่ให้บริการลูกค้า รวมไปถึงระยะเวลาการให้สัมภาษณ์ที่จำกัดอาจทำให้ขาดประเด็นหรือปัจจัยอื่น ๆ เพิ่มเติมที่อาจส่งผลต่อผลงานวิจัยฉบับนี้

5.4 ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

สำหรับผู้ที่ต้องการศึกษาต่อยอดในอนาคต ผู้วิจัยมีข้อเสนอแนะเพื่อการศึกษาเกี่ยวกับผลกระทบจากการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในภาคธุรกิจ 3 ประเด็น ดังนี้

5.4.1 ทำการเก็บข้อมูลอีกครั้งรวมถึงเก็บข้อมูลจากกลุ่มเจ้าหน้าที่ให้บริการลูกค้า หลังจากที่มีกฎหมายมีผลบังคับใช้อย่างเต็มรูปแบบ และมีความชัดเจนมากขึ้นจากการออกกฎหมายลำดับรองและแนวทางการพิจารณาในเรื่องต่าง ๆ จากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

บุคคลและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อข้อมูลที่สมบูรณ์มากขึ้น และทราบถึงมุมมองผลกระทบและแนวทางปฏิบัติที่เปลี่ยนแปลงไป

5.4.2 ศึกษาเพิ่มเติมในมุมมองของผู้บริโภคเกี่ยวกับการรับรู้และความคาดหวังเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจเพื่อเป็นแนวทางในการพัฒนาการสื่อสารและการให้บริการแก่ภาคธุรกิจ

5.4.3 ศึกษาเพิ่มเติมในกลุ่มธุรกิจอื่นในภาคธุรกิจการเงิน หรือภาคธุรกิจอื่น ที่มีการใช้ข้อมูลส่วนบุคคลส่วนบุคคลจำนวนมาก เช่น ธุรกิจนาโนไฟแนนซ์ (Nano Finance) พิกโกไฟแนนซ์ (PICO Finance) ธุรกิจโรงพยาบาล ธุรกิจโทรคมนาคม เป็นต้น



รายการอ้างอิง

หนังสือและบทความในหนังสือ

- เชมฤทัย สุมาวงศ์ และคณะ. (2556). *การพัฒนากฎหมายเพื่อการคุ้มครองผู้บริโภคในการใช้บริการทางการเงิน: รายงานฉบับสมบูรณ์*. กรุงเทพฯ: สำนักงานเศรษฐกิจการคลังกระทรวงการคลัง.
- ทิพวรรณ หล่อสุวรรณรัตน์. (2547). *ทฤษฎีองค์การใหม่* (พิมพ์ครั้งที่ 5). กรุงเทพฯ: สถาบันบัณฑิตพัฒนบริหารศาสตร์
- เนตร์พัฒนา ยาวีราข. (2560). *การจัดการสมัยใหม่ Modern Management* (พิมพ์ครั้งที่ 11). กรุงเทพฯ: ทริปเพิ้ล กรุป
- ปิยะบุตร บุญอร่ามเรือง, ปิติ เอี่ยมจารุญลาภ, พีรพัฒน์ โชคสุวัฒนสกุล, ชวิน อุณหัทร, และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล. (2562). *Thailand Data Protection Guidelines 2.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย
- สุพิศ ประณีตพลกรัง. (2563). *การคุ้มครองข้อมูลส่วนบุคคล*. กรุงเทพฯ: สมพรการพิมพ์.
- Robbins, S. P. and Coulter, M. (2008). *การจัดการและพฤติกรรมองค์การ แปลจากเรื่อง Management โดย วิรัช สงวนวงค์วาน* (พิมพ์ครั้งที่ 8). กรุงเทพฯ: เพียร์สัน
- เอ็ด ดูเคชั่น อินโดไชน่า.

สื่ออิเล็กทรอนิกส์

- กิตติพงศ์ กมลธรรมวงศ์. (2563). *ประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย*. วารสารสังคมวิจัยและพัฒนา มหาวิทยาลัยธรรมศาสตร์, 2(2). สืบค้นเมื่อ 10 ตุลาคม 2563, จาก <https://he02.tci-thaijo.org/index.php/JMARD/article/download/242417/165149/>
- ญาดา ทองสันสระ. (2559). *การคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคในพาณิชย์อิเล็กทรอนิกส์* (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ). มหาวิทยาลัยธรรมศาสตร์. สืบค้นเมื่อ 20 กันยายน 2563, จาก http://ethesisarchive.library.tu.ac.th/thesis/2016/TU_2016_5764030077_5952_4901.pdf
- ณัฐพล ม่วงท่า. (2563). *สรุป PDPA พ.ร.บ. ข้อมูลส่วนบุคคล กับ 7 เรื่อง ที่ผู้ประกอบการต้องให้ความสำคัญ*. สืบค้นเมื่อ 31 กรกฎาคม 2563, จาก <https://www.everydaymarketing.co/update-news/7-เรื่อง-pdpa-ที่ผู้ประกอบการ/>

ธนาคารแห่งประเทศไทย. (2557). Information Governance. *BOT พระสยาม Magazine*, 17(1).

สืบค้นเมื่อ 18 ตุลาคม 2563, จาก https://www.bot.or.th/Thai/phrasiam/Documents/Phrasiam_1_2557/No.17.pdf

ธนาคารแห่งประเทศไทย. (2561). *ประกาศธนาคารแห่งประเทศไทยที่ สกส. 1_2561 เรื่อง Market Conduct ลงวันที่ 12 มกราคม 2561*. สืบค้นเมื่อ 30 พฤษภาคม 2563, จาก

https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/Doc_Form/Docs_Manual/ประกาศธนาคารแห่งประเทศไทยที่%20สกส.%201_2561%20เรื่อง%20Market%20Conduct%20%20ลงวันที่%2012%20มกราคม%202561.pdf

ธนาคารแห่งประเทศไทย. (2563). *การกำกับดูแลด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct Supervision)*. สืบค้นเมื่อ 1 ตุลาคม 2563, จาก <https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2563/ThaiPDF/25630223.pdf>

ธนาคารแห่งประเทศไทย. (2563). *ธุรกิจการเงินที่ ธปท. กำกับดูแล*. สืบค้นเมื่อ 28 พฤษภาคม 2563, จาก <https://www.bot.or.th/Thai/FinancialInstitutions/OthFlsSupervision/Pages/default.aspx>

ธนาคารแห่งประเทศไทย. (2563). *รายชื่อที่อยู่ Website สถาบันการเงินและ Non-bank*. สืบค้นเมื่อ 28 พฤษภาคม 2563, จาก <https://www.bot.or.th/Thai/FinancialInstitutions/WebsiteFI/Pages/InstList.aspx>

ประชาชาติธุรกิจ. (2563). *กรมส่งเสริมการค้าระหว่างประเทศ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลออกไปอีก 1 ปี*. สืบค้นเมื่อ 26 พฤษภาคม 2563, จาก <https://www.prachachat.net/ict/news-463146>

พร อารยะการกุล. (2563). *องค์กรไทยตื่นตัว เร่งปรับตัวรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)*. *นิตยสาร Electricity & Industry Magazine*, 27(2). สืบค้นเมื่อ 15 กันยายน 2563, จาก <https://www.electricityandindustry.com/electricity-industry-magazine-issues-2020/นิตยสาร-electricity-industry-magazine-issues-mar-apr-2020/>

พัชรพร ลิพพิพัฒน์ไพบูลย์, และณัฐพล เลิศเมธพัฒน์. (2562). *การใช้ปัญญาประดิษฐ์ในไทย กรณีตัวอย่างในภาคการเงิน*. *วารสารวิชาการธนาคารแห่งประเทศไทย*, 12(8). สืบค้นเมื่อ 11 กันยายน 2563, จาก https://www.bot.or.th/Thai/MonetaryPolicy/EconomicConditions/AAA/AI_Aug27.pdf

มร.รอยซ์ เทียว. (2561). *GDPR กับโอกาสของธุรกิจไทยในเอเชียแปซิฟิก*. *วารสาร Engineering Today*, 16(166). สืบค้นเมื่อ 13 กันยายน 2563, จาก <https://www.engineeringtoday.net/>

engineering-today-magazine-issue-2018/engineering-today-issue-166-jul-aug-2018/

วิชญ์ วงศ์หาญเชาว์. GDPR กับการบริหารความเสี่ยงของข้อมูลส่วนบุคคลเพื่อแต้มต่อทางธุรกิจ.

นิตยสาร *Electricity & Industry Magazine*, 25(3). สืบค้นเมื่อ 13 กันยายน 2563, จาก <https://www.electricityandindustry.com/electricity-industry-magazine-issues-2018/นิตยสาร-electricity-industry-magazine-issues-may-jun-2018/>

ศรัณญา วิริยะศาสตร์. (2561). *การปรับตัวของธนาคารพาณิชย์ไทยในยุคฟินเทค* (การค้นคว้าอิสระปริญญาโท). มหาวิทยาลัยธรรมศาสตร์. สืบค้นเมื่อ 20 กันยายน 2563, จาก http://ethesisarchive.library.tu.ac.th/thesis/2018/TU_2018_6002031323_9306_9583.pdf

ศศิมา สุขสว่าง. (ม.ป.ป.). *PDCA เครื่องมือง่าย ๆ สำหรับพัฒนางาน*. สืบค้นเมื่อ 6 ตุลาคม 2563, จาก <https://www.sasimasuk.com/16050690/pdca-เครื่องมือง่าย ๆ สำหรับพัฒนางานและนวัตกรรม>

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2563). *สรุปสาระสำคัญของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. สืบค้นเมื่อ 30 พฤษภาคม 2563, จาก <https://drive.google.com/file/d/1Ni3TQFTU01eMSHNDrXnCgHhOfFEnvrlzc/view>

สุธาสนี โพรจินทร์. (2558). *PDCA หัวใจสำคัญของการปรับปรุงอย่างต่อเนื่อง*. สืบค้นเมื่อ 6 ตุลาคม 2563, จาก <https://www.ftpi.or.th/2015/2125>

อธิพร สิทธิธีรรัตน์. (2558). *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์* (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยธรรมศาสตร์. สืบค้นเมื่อ 17 กันยายน 2563, จาก http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5701033531_3922_2696.pdf

เอกพันธ์ พัฒนาวิจิตร. (2558). *ปัจจัยที่ส่งผลต่อการเปิดเผยข้อมูลส่วนบุคคลกรณีศึกษาการลงชื่อเข้าใช้ด้วยรหัสผู้ใช้เฟซบุ๊ก* (การค้นคว้าอิสระปริญญาโท). มหาวิทยาลัยธรรมศาสตร์. สืบค้นเมื่อ 25 กันยายน 2563, จาก http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5702037135_3915_2778.pdf

Techtalkthai. (2561). GDPR คืออะไร ส่งผลกระทบอย่างไร. สืบค้นเมื่อ 8 กันยายน 2563, จาก <https://www.techtalkthai.com/what-is-gdpr-basics/>

Titima Thumbumrung. (2563). *การเขียน Privacy notice*. สืบค้นเมื่อ 10 กันยายน 2563, จาก <http://www.thailibrary.in.th/2020/01/13/privacy-notice/>

Book

Society for Human Resource Management. (2005). *The Essentials of Managing Change and Transition*. Boston: Harvard Business School Press.

Other Materials

Deloitte. (2018). *How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on* (Research report). United Kingdom: Deloitte LLP.

Khiar, I. L., Trautwein, K., Huber, A., & Stamm, J. (2017). *The EU General Data Protection Regulation (GDPR) in the banking industry: An impact analysis on banks and wealth managers with the focus on Switzerland* (Research report). Switzerland: PricewaterhouseCoopers International Limited

Krivokapic, D., Komazec, S., Todorovic, I., & Krivokapić, D. (2018). *Impact of GDPR on Business: Focus on Data Controllers and Processors not Established within the EU* (Research report). Slovene: University of Maribor

Willaert, M. (2018). *The impact of the GDPR on the Belgian Financial sector* (Research report). Belgium: Ghent University

Electronic Media

Abi, M. (2018). *GDPR: how is it affecting banks?*. Retrieved September 3, 2020, from <https://www.financialdirector.co.uk/2018/06/21/gdpr-how-is-it-affecting-banks/>

Brian, C. (2019). *Top 5 ways GDPR has impacted digital banking*. Retrieved September 4, 2020, from <https://www.worldfinance.com/banking/top-5-ways-gdpr-has-impacted-digital-banking>

Jennifer, L. (2020). *WHAT IS GDPR AND HOW DOES IT IMPACT YOUR BUSINESS?*. Retrieved September 4, 2020, from <https://www.superoffice.com/blog/gdpr/>

Steven, M. (2020). *GDPR FOR SALES: HOW TO FIND NEW CUSTOMERS WITHOUT BREAKING THE LAW*. Retrieved September 4, 2020, from <https://www.superoffice.com/blog/gdpr-sales/>

ประวัติผู้เขียน

ชื่อ	นางสาวจตุพร บุญเหมย
วันเดือนปีเกิด	2 มกราคม 2532
วุฒิการศึกษา	ปีการศึกษา 2554: บัณฑิต มหาวิทยาลัยเชียงใหม่
ตำแหน่ง	นักวิชาการตรวจเงินแผ่นดิน สำนักงานการตรวจเงินแผ่นดิน
ประสบการณ์ทำงาน	2560-ปัจจุบัน: นักวิชาการตรวจเงินแผ่นดิน สำนักงานการตรวจเงินแผ่นดิน 2559-2560: Internal Audit บริษัท กลุ่มเซ็นทรัล จำกัด 2558-2559: Internal Audit บริษัท วันทิวน์ คอนแทคส์ จำกัด (มหาชน) 2554-2558: Internal Audit บริษัท ดับเบิล เอ (1991) จำกัด (มหาชน)