วารสารรามคำแหง ฉบับบัณฑิตวิทยาลัย ปีที่ 6 ฉบับที่ 1 มกราคม - เมษายน 2566
Ramkhamhaeng University Journal: Graduate School Vol. 6 No. 1 January - April 2023
ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

# รูปแบบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs)

# Format in Preparation for Small and Medium-Sized Entrepreneurs (SMEs) for Compliance with Data Protection Act B.E. 2562

ปรีดา โชติมานนท์[1*] และ สุขสมัย สุทธิบดี[2]
[1]ภาควิชากฎหมายพาณิชย์ คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง ประเทศไทย
[2]คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง ประเทศไทย
*ผู้รับผิดชอบบทความ

Preeda Showtimanon[1*] and Suksamai Suthibodee[2]
[1]Commercial Law, Faculty of Law, Ramkhamhaeng University, Thailand
[2]Faculty of Law, Ramkhamhaeng University, Thailand
[*]Corresponding: preeda.s@rumail.ru.ac.th

Received: Nov 3, 2022 / Revised: Jan 30, 2023/ Accepted: Feb 8, 2023

**บทคัดย่อ**

วิสาหกิจขนาดกลางและขนาดย่อม (Small and Medium Enterprises--SMEs) เป็นองค์กรธุรกิจที่มีความสำคัญต่อการขับเคลื่อนเศรษฐกิจของไทยเป็นอย่างยิ่ง การขับเคลื่อนขององค์กรธุรกิจประเภทนี้จะเป็นไปได้มีประสิทธิภาพยิ่งขึ้นหากผู้ประกอบธุรกิจสามารถนำข้อมูลส่วนบุคคลไปช่วยในการพัฒนาการตลาดของตนได้อย่างมีประสิทธิภาพ อย่างไรก็ตามการนำข้อมูลส่วนบุคคลย่อมมาพร้อมกับความรับผิดชอบขององค์กรธุรกิจในการปฏิบัติให้เป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จากการศึกษาพบว่า ประเด็นปัญหาที่สำคัญที่ผู้ประกอบการขนาดกลางและขนาดเล็กควรทำความเข้าใจเพื่อมิให้เกิดผลกระทบจากการไม่ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลมีดังต่อไปนี้

ประเด็นที่หนึ่ง หลักการในการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ผลการใช้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งในแง่เนื้อหา แง่บุคคล และแง่ดินแดน รวมไปถึงหลักการที่สำคัญที่อยู่เบื้องหลังการร่างพระราชบัญญัติดังกล่าว

ประเด็นที่สอง ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ฐานความยินยอม ฐานความจำเป็นในการปฏิบัติตามสัญญากับเจ้าของข้อมูลฐานความจำเป็นของผู้ควบคุมข้อมูลในการปฏิบัติตัวตามกฎหมาย ฐานความจำเป็นในการป้องกันภัยอันตรายต่อชีวิต ฐานความจำเป็นในการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือการปฏิบัติหน้าที่โดยเจ้าหน้าที่ของรัฐ ฐานประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก และฐานเพื่อประโยชน์ในการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ รวมไปถึงการศึกษาวิจัยในเชิงสถิติ

ประเด็นที่สาม สิทธิของเจ้าของข้อมูลส่วนบุคคล ได้แก่ สิทธิในการถอนความยินยอม สิทธิที่จะได้รับการแจ้งข้อมูล สิทธิในการแก้ไขข้อมูลให้ถูกต้อง สิทธิในขอลบข้อมูล สิทธิในการระงับการประมวลผล สิทธิในการโอนข้อมูล สิทธิในการคัดค้านการประมวลผลและสิทธิที่เกี่ยวข้องกับการประมวลผลข้อมูลอัตโนมัติ

**คำสำคัญ:** ข้อมูลส่วนบุคคล; การเปิดเผยข้อมูลส่วนบุคคล; ผู้ประกอบการขนาดกลางและขนาดเล็ก

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

งานวิจัยฉบับนี้ ได้ดำเนินการวิจัยศึกษาวิจัยเชิงคุณภาพโดยรวบรวมและวิเคราะห์ข้อมูลเชิงเอกสาร (documentary research) จากนั้นจึงนำความรู้ที่ได้มาพัฒนาจัดทำเป็นรูปแบบปฏิบัติสำหรับวิสาหกิจขนาดกลางและขนาดย่อมในการปฏิบัติให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ด้วยภาษาที่ชัดเจนและง่ายต่อการนำไปปฏิบัติพร้อมทั้งแบบตรวจสอบเบื้องต้น (checklist) ที่เหมาะสมกับผู้ที่ปฏิบัติงานใกล้ชิดกับข้อมูลส่วนบุคคลได้ตระหนักถึง ความสำคัญของการคุ้มครองส่วนบุคคลอยู่เสมออีกด้วย โดยแบ่งเนื้อหาเป็นสามส่วนตามประเด็นปัญหาที่สำคัญดังกล่าว

**Abstract**

Small and Medium Enterprises (SMEs) are one of the types of business entity which are indispensable for Thai economy and its economic growth. In order that Small and Medium Enterprises can operate their business effectively, it is crucial that, they can make comprehensively use of personal data of their customer, especially for the purpose of improving their marketing strategy. However, Small and Medium Enterprises are responsible for compliance to rules and regulations concerning data protection. These three issues are required for those who run Small and Medium Enterprises;

Firstly, principles of processing personal data prescribed in Personal Data Protection Act B.E. 2562, including material, personal and territorial scope of Personal Data Protection Act B.E. 2562 and its fundamentals.

Secondly, legal bases for data processing, including consent of data subject, necessity for the performance of contract, necessity for compliance with a legal obligation, necessity in order to protect the vital interests, necessity for the performance of a task carried out in the public interest or in the exercise of official authority, legitimate Interest of data processor or third parties and processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Thirdly, rights of data subject, including right to withdraw consent, right to be informed, right of rectification, right to erasure, right to restriction, right to data portability, right to object, and rights related to automated decision-making.

This research aims to examine the use of a qualitative data analysis technique, the documentary method, in the development of knowledge into the handbook of data protection Small and Medium Enterprises and checklist for data protection practitioners in clear and easy language to make sure that these organizations can comply with rules and regulations concerning data protection.

**Keywords:** Personal Data; Disclosure of Personal Data; Small and Medium Enterprises

## 1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้วางแนวทางในการจัดเก็บข้อมูลส่วนบุคคลสำหรับผู้ประกอบธุรกิจ ดังนั้น ภายหลังจากที่พระราชบัญญัติดังกล่าวมีผลบังคับใช้แล้ว ผู้ประกอบธุรกิจต้องปรับตัวให้สอดคล้องกับข้อบังคับของกฎหมายดังกล่าว ประกอบกับในปัจจุบันมีการใช้อินเทอร์เน็ตและเทคโนโลยีดิจิทัลเข้ามามีส่วนร่วมกับการประกอบกิจการทางการค้ากันอย่างแพร่หลาย ทำให้การจัดเก็บข้อมูลลูกค้าของผู้ให้บริการทำได้โดยง่ายมากขึ้น และข้อมูล

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

ที่จัดเก็บก็มีความหลากหลายมากขึ้นด้วย โดยข้อมูลของลูกค้าที่ผู้ประกอบการจัดเก็บนั้น อาจจำแนกได้เป็น 2 ประเภท กล่าวคือ ข้อมูลส่วนบุคคลที่ระบุตัวตนชัดเจน และข้อมูลพฤติกรรมที่เกิดจากการใช้งานของผู้บริโภคที่ไม่สามารถระบุย้อนกลับไปยังตัวตนของผู้ใช้ได้ แต่เป็นข้อมูลที่สามารถนำไปใช้ในเชิงสถิติและการวิเคราะห์พฤติกรรมการบริโภคได้ เช่น ข้อมูลเรื่องเพศ อายุ อาชีพ สถานะทางสังคม เป็นต้น พบข้อสังเกตได้ว่า ในอดีตที่ผ่านมา แอปพลิเคชัน (application) ต่าง ๆ ที่ให้บริการมีการแจ้งเตือนผู้ใช้บริการถึงการจัดเก็บและการนำข้อมูลต่าง ๆ ไปใช้งาน เพื่อให้ผู้ใช้บริการกดยินยอมก่อนที่จะเข้าสู่การใช้งานแอปพลิเคชัน (application) ซึ่งการให้ความยินยอมของผู้ใช้บริการถือเป็นขั้นตอนสำคัญที่ผู้ประกอบการต้องปฏิบัติตามกฎหมาย หรือในบางเว็บไซต์ (website) ที่มีการแจ้งเตือนก่อนว่าเว็บไซต์ (website) นี้ มีการใช้คุกกี้ (cookies) เป็นเครื่องมือในการติดตามพฤติกรรมในการท่องเว็บไซต์ของลูกค้า เป็นต้น อนึ่ง แนวทางการจัดเก็บและรักษาข้อมูล หรือสิทธิของผู้บริโภคที่เกิดขึ้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น สอดคล้องกับสิ่งที่เกิดขึ้นในสหภาพยุโรปและในประเทศสหรัฐอเมริกา ถือว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายไทยที่จะยกระดับผู้ประกอบการไปสู่การปรับตัวสู่ความเป็นสากลก็ว่าได้ โดยเฉพาะอย่างยิ่ง หากในอนาคตต้องการขยายธุรกิจและทำการค้ากับผู้ประกอบการหรือลูกค้าที่อยู่ในต่างประเทศ ดังนั้น ผู้ประกอบการต่าง ๆ ที่มีการจัดเก็บข้อมูลของผู้ใช้งานควรที่จะปฏิบัติตามหลักเกณฑ์ที่พระราชบัญญัติดังกล่าวกำหนดอย่างเคร่งครัด (จุฬาลงกรณ์มหาวิทยาลัย, คณะนิติศาสตร์, 2563, หน้า 5)

ผลจากการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้ผู้ประกอบการต้อง (1) มีนโยบายทางด้านข้อมูลส่วนบุคคลที่โปร่งใสยิ่งขึ้น โดยเฉพาะเรื่องสัญญาในการนำข้อมูลส่วนบุคคลไปใช้งาน (2) ตรวจสอบการเก็บข้อมูลส่วนบุคคลของลูกค้าภายในองค์กร เพื่อให้ทราบว่าปัจจุบันมีการนำข้อมูลใดมาใช้บ้าง และมีความจำเป็นที่ต้องใช้งานต่อหรือไม่ ถ้ามีก็ต้องแจ้งให้ลูกค้ารับทราบ และยินยอมที่จะให้นำไปใช้งาน (3) จัดทำระบบในการจัดเก็บข้อมูลของลูกค้าที่มีความมั่นคงปลอดภัยและพร้อมที่จะลบข้อมูลทันที เมื่อลูกค้าร้องขอ และ (4) การอบรมและให้ความรู้แก่พนักงานถึงหน้าที่ในการขอความยินยอมจากลูกค้าก่อนนำข้อมูลมาใช้งาน (consent) และข้อมูลที่ผู้ประกอบการจัดเก็บหรือได้มานั้นจะถูกนำมาใช้ตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น อาจกล่าวได้ว่า หากผู้ประกอบการใดไม่มีเทคโนโลยีมารองรับและทำให้ไม่สามารถเก็บรักษาข้อมูลสำคัญของลูกค้าได้ จะเป็นสิ่งสะท้อนว่าการบริหารจัดการยังไม่มีประสิทธิภาพอันจะนำไปสู่ความเสี่ยงที่ละเมิดต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

อนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์เพื่อช่วยให้ผู้บริโภคมีสิทธิในข้อมูลส่วนบุคคลของตนเองที่บริษัทหรือผู้ประกอบการธุรกิจได้จัดเก็บข้อมูลไปจัดการให้บริการต่าง ๆ โดยส่วนใหญ่แล้ว ผู้ประกอบการที่มีขนาดใหญ่ มักจะมีฝ่ายกฎหมายเป็นของตัวเองหรือมีงบประมาณสำหรับการว่าจ้างนักกฎหมายในการจัดการเรื่องนี้โดยเฉพาะ ดังนั้น ผู้ประกอบการที่มีขนาดใหญ่ไม่ค่อยจะมีปัญหาเกี่ยวกับการปรับตัวให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับดังกล่าว หากแต่ที่น่าเป็นห่วงก็คือผู้ประกอบการธุรกิจที่มีขนาดกลาง และขนาดเล็ก หรือที่เรียกกันว่า SMEs ซึ่งผู้ประกอบการธุรกิจเหล่านั้นมีงบประมาณไม่มากนักและมิได้มีฝ่ายกฎหมายเป็นของตัวเอง จึงมีความสุ่มเสี่ยงที่จะไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้ และการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อาจได้รับโทษที่ถือว่ารุนแรงมาก หากเทียบเคียงกับวิถีการปฏิบัติทางธุรกิจของผู้ประการขนาดกลางและขนาดเล็กในประเทศไทย

ด้วยเหตุผลทั้งหมดข้างต้น งานวิจัยฉบับดังกล่าวมุ่งศึกษาความสำคัญและข้อได้เปรียบของการใช้ข้อมูลส่วนบุคคลในหน่วยงานหรือกิจการขนาดกลางและขนาดเล็ก จากนั้น จึงจะได้ศึกษาหลักการที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูล ส่วนบุคคล เพื่อที่จะค้นหาปัญหาและอุปสรรคที่อาจเกิดขึ้นสำหรับหน่วยงานหรือกิจการขนาดกลางและขนาดเล็กในการที่จะปฏิบัติให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้ในการกำหนดนโยบายและวางแผนการในทางปฏิบัติเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไป

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

**2. วัตถุประสงค์การวิจัย**

2.1 เพื่อศึกษาถึงสิทธิและหน้าที่ของผู้ประกอบการและผู้บริโภคตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.2 เพื่อศึกษาแนวทางการปฏิบัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ประกอบการขนาดกลางและขนาดเล็กที่สอดคล้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.3 เพื่อศึกษารูปแบบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs)

**3. สมมติฐานการวิจัย**

ผู้ประกอบการขนาดกลางและขนาดเล็กสามารถใช้รูปแบบการปฏิบัติที่จัดทำตามโครงการวิจัยนี้ ในการเตรียมความพร้อม หรือปฏิบัติตามข้อกำหนดที่ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างถูกต้องและมีประสิทธิภาพ

**4. ขอบเขตการวิจัย**

4.1 ศึกษาและรวบรวมนโยบาย ข้อกฎหมาย และข้อเท็จจริงที่เกิดขึ้น ในเรื่องเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

4.2 ศึกษาข้อกฎหมาย และข้อกำหนดในเรื่องสิทธิและหน้าที่ต่าง ๆ ของผู้บริโภคตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3 ศึกษาข้อกฎหมาย และข้อกำหนดในเรื่องสิทธิและหน้าที่ต่าง ๆ ของผู้ประกอบการที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.4 ศึกษาและรวบรวมแนวคิดการจัดทำรูปแบบการปฏิบัติที่เหมาะสมกับประเทศไทย

**5. นิยามศัพท์เฉพาะ**

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประกอบการ หมายความว่า บุคคลซึ่งขายสินค้าหรือให้บริการในทางธุรกิจหรือวิชาชีพไม่ว่าการกระทำดังกล่าวจะได้รับประโยชน์ หรือได้รับค่าตอบแทนหรือไม่ และไม่ว่าจะได้จดทะเบียนภาษีมูลค่าเพิ่มแล้วหรือไม่

การเก็บรวบรวมข้อมูลส่วนบุคคล หมายถึง การเก็บรวบรวมข้อมูลส่วนบุคคล ตามที่ปรากฏในส่วนที่ 2 ว่าด้วยการเก็บรวบรวมข้อมูลส่วนบุคคล แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การใช้ข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคล หมายถึง การใช้ข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคล ตามที่ปรากฏในส่วนที่ 3 ว่าด้วยการใช้หรือเปิดเผยข้อมูลส่วนบุคคล แห่งพระราชบัญญัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

**6. ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย**

6.1 ทำให้ทราบถึงสิทธิและหน้าที่ของผู้ประกอบการและผู้บริโภคตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6.2 ทำให้ทราบถึงแนวทางการปฏิบัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ประกอบการขนาดกลางและขนาดเล็กที่สอดคล้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6.3 ได้รูปแบบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs)

**7. กรอบแนวความคิดในการทำวิจัย**

เพื่อสร้างความตระหนักรู้ให้ผู้ประกอบธุรกิจขนาดกลางและขนาดเล็ก (SMEs) เห็นความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและปฏิบัติตนให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จึงต้องมีการศึกษาเปรียบเทียบหลักการและรูปแบบการปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลฉบับต่าง ๆ ที่เป็นมาตรฐานสากล เพื่อนำมาปรับใช้ให้เข้ากับการจัดทำรูปแบบปฏิบัติเพื่อใช้ในการตรวจสอบเบื้องต้น ในการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจขนาดกลางและขนาดเล็ก (SMEs) โดยเฉพาะ

**8. วิธีดำเนินการวิจัย**

ศึกษาวิจัยเชิงคุณภาพโดยรวบรวมและวิเคราะห์ข้อมูลเชิงเอกสาร (documentary research) ซึ่งค้นคว้าและรวบรวมเอกสารจากหนังสือ บทความทางวิชาการ รายงานการวิจัย รวมถึงตำรา บทความ กฎหมาย ระเบียบและหลักเกณฑ์ต่างประเทศ เช่น GDPR, Guidelines on Assessing Proportionality, OECD Privacy Guidelines, Guidelines 4/2019 on Article 25: Data Protection by Design and by Default, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Necessity Toolkit เป็นต้น (European Commission, 2021; European Data Protection Board, 2021; European Data Protection Supervisor, 2021A, 2021B; European Union, 2021; Information Commissioner's Office, 2021; Organization for Economic Co-operation and Development, 2021)

**9. สรุปผลการวิจัย**

วิจัยฉบับนี้มุ่งศึกษาเกี่ยวกับความสัมพันธ์ระหว่างวิสาหกิจขนาดกลางและขนาดย่อม (Small and Medium Enterprises--SMEs) กับการคุ้มครองข้อมูลส่วนบุคคล โดยเริ่มจากความจำเป็นที่วิสาหกิจขนาดกลางและขนาดย่อมจะต้องดำเนินธุรกิจ โดยคำนึงถึงการใช้ประโยชน์จากข้อมูลส่วนบุคคลในการขับเคลื่อนธุรกิจ แต่ในขณะเดียวกันก็ต้องคำนึงหน้าที่ในการปฏิบัติให้เป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลด้วยเสมอ ดังนั้น สาระสำคัญของการศึกษาจึงพบว่า ประเด็นปัญหาหลักที่สำคัญเกี่ยวกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ที่วิสาหกิจขนาดกลางและขนาดย่อมที่ต้องทำความเข้าใจมี 3 ประเด็น ได้แก่

9.1 หลักการทั่วไปว่าการประมวลผลข้อมูลส่วนบุคคลทั้ง 7 ประการ ได้แก่ หลักความชอบด้วยกฎหมาย ความเป็นธรรมและความโปร่งใสของการบริหารจัดการข้อมูล (lawfulness, fairness, and transparency) หลักการจำกัดวัตถุประสงค์ของการใช้ข้อมูล (purpose limitation) หลักความจำเป็นในการใช้ข้อมูล (data minimization) หลักความแม่นยำในการนำข้อมูลส่วนบุคคลไปใช้ (accuracy) หลักการจำกัดการจัดเก็บข้อมูลส่วนบุคคล (storage limitation) หลักความบริบูรณ์และการรักษาความลับ (integrity and confidentiality) และหลักความรับผิด (accountability)

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

9.2 ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล 7 ประการ ได้แก่ ฐานความยินยอม (consent) ฐานความจำเป็นในการปฏิบัติตามสัญญากับเจ้าของข้อมูล (necessity for the performance of a contract) ฐานความจำเป็นของผู้ควบคุมข้อมูลในการปฏิบัติตามกฎหมาย (necessity for compliance with a legal obligation) ฐานความจำเป็นในการป้องกันภยันตรายต่อชีวิตของบุคคล (necessity in order to protect the vital interests) ฐานความจำเป็นในการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือการปฏิบัติหน้าที่โดยเจ้าหน้าที่ของรัฐ (public task/ official authority) ฐานประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก (legitimate interest) และฐานเพื่อประโยชน์ในการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ รวมไปถึงการศึกษาวิจัยในเชิงสถิติ (scientific or research)

9.3 สิทธิของเจ้าของข้อมูลส่วนบุคคล 9 ประการ ได้แก่ สิทธิในการถอนความยินยอม (right to withdraw consent) สิทธิที่จะได้รับการแจ้งข้อมูล (right to be informed) สิทธิในการเข้าถึงข้อมูล (right of access) สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (right of rectification) สิทธิในการขอลบข้อมูล (right to erasure) หรือสิทธิที่จะถูกลืม (right to be forgotten) สิทธิในการระงับการประมวลผล (right to restriction) สิทธิในการโอนข้อมูล (right to data portability) สิทธิในการคัดค้านการประมวลผล (right to object) และสิทธิที่เกี่ยวข้องกับการประมวลผลข้อมูลอัตโนมัติ (rights related to automated decision making)

ทั้งนี้ นับแต่เวลาที่กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ ได้มีความพยายามจากองค์กรต่าง ๆ ที่จะจัดทำแนวปฏิบัติ (guideline) ในรูปแบบต่าง ๆ เพื่อให้การปฏิบัติให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเหล่านั้น เป็นไปได้โดยง่ายและเป็นไปในแนวทางเดียวกัน เช่น “TDPG 3.0 Thailand Data Protection Guidelines 3.0 – Business Functions แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 3.0” ซึ่งจัดทำโดย คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือแม้จะทั่งการจัดทำการสร้างรายการตรวจสอบ (checklist) ซึ่งเป็นรูปแบบที่ผู้ประกอบการสามารถทำความเข้าใจสิทธิและหน้าที่ของตนได้โดยง่าย และสามารถใช้งานได้สะดวกกว่าแนวปฏิบัติ (guideline) ซึ่งมีความละเอียดและซับซ้อนของการนำเสนอมากกว่ารายการตรวจสอบ (checklist) การสร้างความเข้าใจต่อการปฏิบัติให้เป็นไปตามกฎหมายสำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs) ซึ่งควรเริ่มต้นจากการจัดทำรายการตรวจสอบ (checklist) เพื่อเผยแพร่ต่อผู้ประกอบการก่อน จึงจะได้จัดทำแนวปฏิบัติ (guideline) ที่มีความละเอียดมากยิ่งขึ้นเป็นลำดับถัดไป (ชวิน อุ่นภัทร, 2563, หน้า 150-151)

**10. อภิปรายผลการวิจัยและข้อเสนอแนะ**

จากข้อสรุปดังกล่าว เพื่อให้การดำเนินการของรัฐวิสากิจขนาดกลางและขนาดย่อมเป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงควรมีการจัดทำคู่มือสำหรับองค์ธุรกิจขนาดกลางและขนาดย่อมในการปฏิบัติ ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ด้วยภาษาที่ชัดเจนและ ง่ายต่อการนำไปปฏิบัติ ที่เหมาะสมกับผู้ที่ปฏิบัติงานใกล้ชิดกับข้อมูลส่วนบุคคลได้ตระหนักถึงความสำคัญของการคุ้มครองส่วนบุคคลอยู่เสมออีกด้วย โดยบรรจุเนื้อหาที่เกี่ยวข้องกับหลักการทั่วไปว่าการประมวลผลข้อมูลส่วนบุคคล ทั้งฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมทั้งทางปฏิบัติที่เกี่ยวข้องกับการวางแผนนโยบาย การบริหารจัดการองค์กร และการบริหารจัดการเชิงเทคนิคเพื่อให้เป็นไปตามกฎระเบียบเช่นว่านั้น นอกจากนี้ ยังควรจัดให้มีรูปแบบปฏิบัติเพื่อใช้ในการตรวจสอบเบื้องต้น เพื่อให้ง่ายต่อผู้บริหารและผู้ปฏิบัติในการสร้างความเข้าใจเบื้องต้นและยังสามารถนำไปใช้ในการตรวจสอบถึงข้อบกพร่องเบื้องต้นในการคุ้มครองข้อมูลส่วนบุคคล โดยแบ่งหัวข้อรูปแบบปฏิบัติออกเป็นสามกลุ่ม ได้แก่ หลักการทั่วไปว่าการประมวลผลข้อมูลส่วนบุคคล ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

ตัวอย่างรูปแบบปฏิบัติเพื่อใช้ในการตรวจสอบเบื้องต้นที่เหมาะสมกับบริบทของประเทศไทยมีดังต่อไปนี้

10.1 ส่วนที่หนึ่ง ฐานความชอบด้วยกฎหมายและความโปร่งใสของการประมวลผลข้อมูลส่วนบุคคล (lawful basis and transparency)

10.1.1 ผู้ประกอบการต้องระบุข้อมูลส่วนบุคคลที่อยู่ในกิจการ และกำหนดมาตรการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ผู้ประกอบการขนาดกลางและขนาดเล็กควรจัดทำมาตรการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยประกอบไปด้วยขั้นตอนดังต่อไปนี้ (1) กำหนดนิยามของข้อมูลส่วนบุคคล และนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในแต่ละประเภท (data policy) (2) กำหนดขั้นตอนในการรวบรวม ตรวจสอบ และประเมินผลข้อมูลส่วนบุคคล (data recovery) (3) จัดทำแผนภูมิเพื่อให้เห็นความสัมพันธ์และเชื่อมโยงกันระหว่างข้อมูลส่วนบุคคลต่าง ๆ ที่ได้มีการใช้ภายในองค์กร (data proliferation) (4) กำหนดความเสี่ยงของข้อมูลประเภทต่าง ๆ ภายในองค์กร (data risk level) และ (5) กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยงของข้อมูลแต่ละประเภท (data protection)

นอกจากนี้ ผู้ประกอบการยังต้องตรวจสอบถึงความสอดคล้องของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลกับกฎ หรือระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยจัดทำการประเมินผลกระทบของการประมวลผลข้อมูลส่วนบุคคล (data protection impact assessment) อย่างสม่ำเสมอ

10.1.2 กิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลดังกล่าวเป็นกิจกรรมได้กระทำโดยอาศัยฐานทางกฎหมายที่ถูกต้อง

การประมวลผลข้อมูลส่วนบุคคลย่อมไม่ชอบด้วยกฎหมาย หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถกล่าวอ้างถึงฐานในการประมวลข้อมูลส่วนบุคคลหนึ่งในเจ็ดฐานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกจากนี้ยังมีข้อกำหนดพิเศษที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของเด็กและผู้ที่ต้องได้รับการคุ้มครองเป็นพิเศษในมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยเหตุนี้ ในการประมวลผลข้อมูลส่วนบุคคลจึงต้องมีการทบทวนบทบัญญัติเหล่านี้และเลือกฐานทางกฎหมายที่จะใช้ในการประมวลผลข้อมูลส่วนบุคคล พร้อมทั้งบันทึกเหตุผลในการตัดสินใจเช่นว่านั้น หากผู้ประกอบการเลือก “ความยินยอม” เป็นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ผู้ประกอบการย่อมมีหน้าที่ตามกฎระเบียบที่เกี่ยวข้องเพิ่มเติมด้วย เช่น หน้าที่ในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงสิทธิในการเพิกถอนความยินยอมที่ได้ให้ไว้ และหากผู้ประกอบการเลือก “ประโยชน์อันชอบธรรม” เป็นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ผู้ประกอบการต้องแสดงให้เห็นได้ว่า ผู้ประกอบการ ได้จัดทำการประเมินผลกระทบของการประมวลผลข้อมูลส่วนบุคคล (data protection impact assessment) เป็นที่เรียบร้อยแล้ว

10.1.3 ผู้ประกอบการได้ให้ข้อมูลที่ชัดเจนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลไว้ในนโยบายในการประมวลผลข้อมูลส่วนบุคคล

ผู้ประกอบการต้องแจ้งให้ลูกค้าทราบว่าได้รวบรวมข้อมูลส่วนบุคคล และแจ้งว่าได้รวบรวมข้อมูลดังกล่าวไปเพื่อวัตถุประสงค์ใด ตามมาตรา 21 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉะนั้น ผู้ประกอบการจะต้องอธิบายว่า ผู้ประกอบการได้นำข้อมูลส่วนบุคคลไปประมวลผลด้วยวิธีการใด ใครบ้างที่มีสิทธิเข้าถึงข้อมูลดังกล่าว และผู้ประกอบการจะรักษาข้อมูลเหล่านี้ให้ปลอดภัยได้เช่นใด

นอกจากนี้ ข้อมูลดังกล่าวยังควรปรากฏในการประมวลผลข้อมูลส่วนบุคคลและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบตั้งแต่เวลาที่ได้รวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคล โดยข้อมูลเหล่านี้ต้องถูกนำเสนอในลักษณะที่ชัดเจนและเข้าใจง่าย โดยเฉพาะอย่างยิ่ง ในกรณีที่ต้องสื่อสารข้อมูลดังกล่าวให้กับเด็ก

10.2 ส่วนที่สอง ความปลอดภัยของข้อมูลส่วนบุคคล (data security)

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

10.2.1 ผู้ประกอบการต้องคำนึงถึงหลักเกณฑ์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ทุกครั้งที่มีการประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องกับ “การคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบและการตั้งค่าเบื้องต้น” (data protection by design and by default) ซึ่งรวมไปถึงการปฏิบัติตาม “มาตรการทางเทคนิคและทางการบริหารจัดการองค์กรที่เหมาะสม” (appropriate technical and organizational measures) เพื่อคุ้มครองข้อมูลส่วนบุคคล กล่าวอีกนัยหนึ่งก็คือ ผู้ประกอบการจำเป็นต้องมีความระมัดระวังในการประมวลผลข้อมูลส่วนบุคคลของบุคคลอื่น โดยตัวอย่างของมาตรการทางเทคนิคที่สำคัญ เช่น การสร้างกลไกในการเข้ารหัสเพื่อเข้าถึงข้อมูลส่วนบุคคล ส่วนมาตรการในเชิงบริหารจัดการองค์กร เช่น การจำกัดผู้ที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล หรือการกำหนดให้มีการลบข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็นที่จะใช้ข้อมูลดังกล่าวแล้ว

10.2.2 ต้องมีการเข้ารหัสและทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุเจ้าของข้อมูลส่วนบุคคลทุกครั้งที่สามารถกระทำได้ผู้ประกอบการจะต้องใช้ระบบการเข้ารหัสและการทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ทุกครั้งที่สามารถกระทำได้

10.2.3 สร้างนโยบายที่เกี่ยวข้องกับความปลอดภัยของข้อมูลเพื่อใช้บังคับภายในองค์กร และสร้างความตระหนักรู้ถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ของลูกค้าถึงแม้ว่าสถานประกอบการจะมีระบบรักษาความปลอดภัยที่แข็งแกร่งเพียงใดก็ตาม แต่ระบบดังกล่าวก็ยังอาจมีจุดอ่อนได้ ด้วยเหตุนี้ การจัดทำนโยบายที่เกี่ยวกับความปลอดภัยทางไซเบอร์จึงเป็นสิ่งที่จำเป็น เพื่อให้พนักงานที่เกี่ยวข้องได้ตระหนักรู้ถึงความสำคัญในประเด็นปัญหาดังกล่าว โดยการจัดทำนโยบายควรอธิบายถึงความปลอดภัยในการใช้อีเมล์ การสร้างและใช้รหัสผ่าน การใช้ระบบ “การตรวจสอบหลายปัจจัย” (Two-Factor Authentication--2FA) การใช้ระบบการเข้ารหัส การใช้ VPN เป็นต้น พนักงานของบริษัทที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของลูกค้าจะต้องได้รับการฝึกอบรมในเรื่องกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นพิเศษ

10.2.4 กำหนดระยะเวลาที่ต้องจัดทำการประเมินความเสี่ยงของผลกระทบที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล และมีกระบวนการที่ชัดเจนในการจัดทำการประเมินดังกล่าวจัดทำการประเมินความเสี่ยงของผลกระทบจากการประมวลผลข้อมูลส่วนบุคคล (data protection impact assessment) นั้น เป็นอีกวิธีที่จะช่วยให้ผู้ประกอบการเข้าใจว่าผลิตภัณฑ์หรือบริการของคุณจะสร้างความเสี่ยงให้แก่ความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้ามากน้อยเพียงใด ทั้งยังช่วยให้เข้าใจวิธีการในการลดความเสี่ยงดังกล่าวได้อีกด้วย

10.2.5 มีกระบวนการที่แน่นอนในการแจ้งให้หน่วยงานที่เกี่ยวข้องและเจ้าของข้อมูลส่วนบุคคลทราบในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ในกรณีที่พบการรั่วไหลของข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลถูกเปิดเผย ผู้ประกอบการจะต้องแจ้งเจ้าหน้าที่ที่เกี่ยวข้องในพื้นที่ของคุณภายใน 72 ชั่วโมง นับตั้งแต่มีการรั่วไหลของข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลถูกเปิดเผย ทั้งนี้ ตามมาตรา 47 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

10.3 ส่วนที่สาม ความรับผิดชอบและธรรมาภิบาลของผู้ควบคุมข้อมูลส่วนบุคคล (accountability and governance)

10.3.1 ผู้ประกอบการได้แต่งตั้งเจ้าหน้าที่เพื่อตรวจสอบการปฏิบัติให้เป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

องค์กรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจะต้องรับผิดชอบต่อการปฏิบัติให้เป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยการประเมินนโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการนำนโยบายเหล่านั้นมาใช้ในทางปฏิบัติ

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

10.3.2 ผู้ประกอบการได้ลงนามในข้อตกลงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่จัดทำขึ้นระหว่างองค์กรและบุคคลภายนอกที่กระทำแทนองค์กรในเรื่องการประมวลผลข้อมูลส่วนบุคคล

การลงนามในข้อตกลงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่จัดทำขึ้นระหว่างองค์กรและบุคคลภายนอกที่กระทำแทนองค์กรในเรื่องการประมวลผลข้อมูลส่วนบุคคลนั้น รวมไปถึงบริการของบุคคลภายนอกที่นำข้อมูลส่วนบุคคลของลูกค้าไปใช้ในการประมวลผล เช่น ซอฟต์แวร์วิเคราะห์ข้อมูล บริการอีเมล์ บริการคลาวด์ เป็นต้น ซึ่งผู้ให้บริการส่วนใหญ่มักจะมีข้อสัญญามาตรฐานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเผยแพร่ไว้ในเว็บไซต์ ผู้ประกอบการจึงสามารถตรวจสอบสิทธิและหน้าที่ของคู่สัญญาแต่ละฝ่ายได้จากข้อตกลงเหล่านี้ ด้วยเหตุนี้ ผู้ประกอบการ จึงควรใช้บริการเฉพาะจากผู้ให้บริการที่เชื่อถือได้ และมีกลไกในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

10.3.3 กรณีสถานประกอบการของผู้ประกอบการมีภูมิลำเนาอยู่นอกประเทศ ที่เป็นสมาชิกของสหภาพยุโรป ผู้ประกอบการจะต้องแต่งตั้งตัวแทนไว้ในประเทศที่เป็นสมาชิกของสหภาพยุโรปประเทศใดประเทศหนึ่ง

หากการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับประเทศที่เป็นสมาชิกของสหภาพยุโรปเพียงประเทศใดประเทศหนึ่ง ผู้ประกอบการจะต้องแต่งตั้งตัวแทนในประเทศเพื่อเป็นตัวแทนในการติดต่อสื่อสารกับหน่วยงานเจ้าหน้าที่ที่เกี่ยวข้อง กับการคุ้มครองข้อมูลส่วนบุคคล

10.3.4 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคลล (ในกรณีที่จำเป็น) มาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลใน 3 กรณีดังต่อไปนี้ (1) ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด และ (3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

อย่างไรก็ตาม ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามที่คณะกรรมการประกาศกำหนดตามมาตรา 29 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าวต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย และถึงแม้จะเป็นกรณีที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมิได้กำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แต่ก็จะเป็นประโยชน์หากสถานประกอบการจะตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ถึงแม้จะไม่มีกรณีที่บังคับว่าจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ตาม โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นผู้มีความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล และมีหน้าที่ในการตรวจสอบ ให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามกฎระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ประเมินความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล ให้คำแนะนำเกี่ยวกับการประเมินความเสี่ยงในการประเมินผลข้อมูลส่วนบุคคล และประสานงานกับหน่วยงานเจ้าหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

10.4 ส่วนที่สี่ การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล (privacy rights)

10.4.1 ลูกค้าจะต้องสามารถร้องขอและรับข้อมูลทั้งหมดที่มีที่เกี่ยวข้องกับตนเองได้โดยง่าย

ลูกค้ามีสิทธิที่จะได้รับทราบว่ามีข้อมูลส่วนบุคคลใดที่เกี่ยวข้องกับตนเองบ้าง และข้อมูลเหล่านี้ถูกนำไปใช้อย่างไร นอกจากนี้ เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิที่จะได้รับทราบว่าข้อมูลส่วนบุคคลดังกล่าวจะถูกเก็บไว้นานเท่าใด พร้อมทั้งเหตุผลที่จะเก็บข้อมูลไว้ในระยะเวลาเช่นว่านั้น จะต้องมีการส่งข้อมูลชุดแรกโดยไม่อาจเรียกเก็บค่าใช้จ่าย แต่หากลูกค้า

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

ขอสำเนาข้อมูลในครั้งต่อไปสามารถเรียกเก็บค่าใช้จ่ายในราคาที่พอสมควรแก่เหตุได้ และก่อนที่จะส่งมอบสำเนาข้อมูลเช่นว่านั้น ก็จำเป็นต้องตรวจสอบข้อมูลของผู้ยื่นคำขอก่อน ทั้งนี้ จะต้องส่งสำเนาข้อมูลให้แก่เจ้าของข้อมูลส่วนบุคคลภายในสามสิบวัน นับแต่วันที่ได้รับคำขอ

10.4.2 ลูกค้าสามารถแก้ไขและเปลี่ยนแปลงข้อมูลที่ไม่ถูกต้องและไม่สมบูรณ์ได้โดยง่าย

ทำให้ข้อมูลทันสมัยอยู่เสมอโดยใช้กระบวนการตรวจสอบคุณภาพของข้อมูล เพื่อให้ลูกค้าสามารถเข้าทำให้ข้อมูลครบถ้วนและเป็นปัจจุบันเสมอ และก่อนที่จะแก้ไขข้อมูลเช่นว่านั้น ก็จำเป็นต้องตรวจสอบข้อมูลของผู้ยื่นคำขอเสียก่อน

10.4.3 ลูกค้าสามารถร้องขอให้มีการลบข้อมูลส่วนบุคคลได้โดยง่าย

มาตรา 33 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้ (1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป (3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2) และ (4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

อย่างไรก็ตาม ในการใช้สิทธิของเจ้าของข้อมูลในการขอลบข้อมูลส่วนบุคคลนั้น จะต้องมีการชั่งน้ำหนักกับประโยชน์ที่ได้รับการคุ้มครองทางกฎหมายประการอื่นด้วย การใช้เสรีภาพในการแสดงออก การปฏิบัติตามกฎหมายกำหนดการปฏิบัติภารกิจของรัฐ งานวิจัย สถิติ ประวัติศาสตร์ จดหมายเหตุการใช้สิทธิตามกฎหมาย จำเป็นเพื่อการสาธารณสุข หรือจำเป็นเพื่อการแพทย์ หากผู้ควบคุมข้อมูลส่วนบุคคลสามารถพิสูจน์ได้ถึงการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เหล่านี้ได้ และเป็นกรณีที่วัตถุประสงค์ดังกล่าวมีความสำคัญเหนือสิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลก็อาจปฏิเสธการขอลบข้อมูลส่วนบุคคลได้

ส่วนในประเด็นปัญหาเรื่องค่าใช้จ่ายนั้น ในการใช้สิทธิครั้งแรก ผู้ควบคุมข้อมูลส่วนบุคคลไม่ควรเก็บค่าใช้จ่ายที่เกิดขึ้นจากการใช้สิทธินั้น เว้นแต่เจ้าของข้อมูลส่วนบุคคลจะมาใช้สิทธิหลายครั้ง ผู้ควบคุมข้อมูลส่วนบุคคลสามารถคิดค่าใช้จ่ายในการดำเนินการจริงได้

10.4.4 ลูกค้าสามารถร้องขอให้หยุดการประมวลผลข้อมูลส่วนบุคคลได้โดยง่าย

เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้มีการจำกัด หรือหยุดการประมวลผลข้อมูลส่วนบุคคลได้ เมื่อมีเหตุจำเป็นบางประการ โดยเฉพาะอย่างยิ่ง เมื่อมีข้อโต้แย้งเกี่ยวกับความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคล หรือความถูกต้องของข้อมูลส่วนบุคคล ทั้งนี้ ผู้ประกอบการจะต้องจำกัด หรือหยุดประมวลผลข้อมูลส่วนบุคคลภายในหนึ่งเดือนนับแต่วันที่ได้รับคำขอ ในกรณีที่มีการจำกัดการประมวลผลข้อมูลส่วนบุคคลจะยังสามารถเก็บข้อมูลนั้นไว้ได้ โดยต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อมีการประมวลส่วนบุคคลดังกล่าวนั้นอีกครั้ง

10.4.5 ลูกค้าสามารถร้องขอให้จัดทำสำเนาข้อมูลส่วนบุคคลในรูปแบบที่ง่ายต่อการโอนข้อมูลดังกล่าวให้ผู้ประกอบการอื่นได้โดยง่าย

ผู้ประกอบการจะต้องส่งข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูล ในรูปแบบที่สามารถอ่านได้โดยเจ้าของข้อมูลหรือบุคคลภายนอกที่ได้รับมอบหมายจากเจ้าของข้อมูล ในแง่มุมของการประกอบธุรกิจอาจมองได้ว่าผู้ประกอบการอาจจะเป็นฝ่ายที่เสียเปรียบเนื่องจากคู่แข่งทางธุรกิจอาจได้รับข้อมูลดังกล่าว แต่ในแง่มุมของการคุ้มครองข้อมูลส่วนบุคคลนั้น ลูกค้าย่อมเป็นเจ้าของข้อมูลส่วนบุคคลที่สามารถตรวจสอบข้อมูลได้เสมอ

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

10.4.6 ลูกค้าจะต้องสามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้โดยง่าย

หากผู้ประกอบการมีวัตุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเพื่อนำไปใช้ทำการตลาดโดยตรงต่อลูกค้าของคุณ (direct marketing) จะต้องมีเหตุผลที่ชอบด้วยกฎหมายในการดำเนินการดังกล่าว เพื่อป้องกันการคัดค้านการประมวลผลดังกล่าว

10.4.7 กรณีที่ผู้ประกอบการมีการตัดสินใจโดยอาศัยการประมวลผลข้อมูลส่วนบุคคลแบบอัตโนมัติ จะต้องมีกระบวนการในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ชัดเจน

สถานประกอบการบางประเภทมีความจำเป็นจะต้องใช้การประมวลผลข้อมูลส่วนบุคคลแบบอัตโนมัติเพื่อช่วยในการตัดสินที่มีผลทางกฎหมาย หรือผลกระทบอื่นใดที่มีความคล้ายคลึงกัน หากจะต้องใช้การประมวลผลข้อมูลส่วนบุคคลด้วยวิธีเช่นว่านั้นเช่นเดียวกัน ผู้ประกอบการต้องมีกระบวนการที่ชัดเจนในการคุ้มครองสิทธิ เสรีภาพ และประโยชน์อันชอบธรรมของเจ้าของข้อมูลส่วนบุคคล (นคร เสรีรักษ์, 2563, หน้า 351-352) เจ้าของส่วนบุคคลจะต้องสามารถร้องขอให้พนักงานเข้าแทรกแซงการตัดสินใจอัตโนมัติ ให้มีการชั่งน้ำหนักของการตัดสินใจใหม่ หรือคัดค้านการตัดสินใจที่ได้กระทำลงไปแล้วได้

## 11. กิตติกรรมประกาศ

บทความนี้เรียบเรียงจากโครงการวิจัยเรื่อง “รูปแบบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ประกอบการขนาดกลางและขนาดเล็ก (SMEs)” โดยงานวิจัยฉบับนี้ สำเร็จลงได้ด้วยดี เนื่องจากได้รับทุนอุดหนุนการวิจัยจากงบประมาณรายจ่ายจากรายได้มหาวิทยาลัยรามคำแหง ประเภทมหาวิทยาลัย ประจำปี พ.ศ. 2564 โดยสถาบันวิจัยและพัฒนา รวมทั้งข้อเสนอแนะของคณะกรรมการพิจารณาทุนที่เป็นประโยชน์ รวมทั้งการแก้ไขข้อบกพร่องเพื่อให้งานวิจัยเล่มนี้ ประสบผลสำเร็จไปได้ด้วยดี ผู้วิจัยขอขอบพระคุณเป็นอย่างสูง ณ โอกาสนี้

## 12. เอกสารอ้างอิง

จุฬาลงกรณ์มหาวิทยาลัย, คณะนิติศาสตร์. (2563). *แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand data protection guidelines 3.0).* ค้นเมื่อ 7 กรกฎาคม 2564, จาก https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf.

ชวิน อุ่นภัทร. (2563). คำถามที่ต้องการคำตอบในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์*, *49*(1), 150-151.

นคร เสรีรักษ์. (2563). *ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองส่วนบุคคลในประเทศไทย* (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร: สำนักพิมพ์ฟ้าฮ่าม.

European Commission. (2021). *Article 29 working party opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of directive 95/46/EC.* Retrieved July 2, 2021, from https://ec.europa.eu/justice/article29/documentation/opinion-Recommendation /files/2014/wp217_en.pdf

European Data Protection Board. (2021). *Guidelines 4/2019 on article 25: Data protection by design and by default*. Retrieved June 20, 2021, from https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-42019-article-25-data-protectiondesign-and_en

European Data Protection Supervisor. (2021A). *Guidelines on assessing proportionality.* Retrieved June 17, 2021, from https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

ISSN 2651-1800 (Print) ISSN 2672-9822 (Online)

European Data Protection Supervisor. (2021B). *Necessity toolkit*. Retrieved June 17, 2021, from https://edps.europa.eu/data-protection/our-work/publications/papers/necessitytoolkit_en

European Union. (2021). *The General Data Protection Regulation (GDPR).* Retrieved June 15, 2021, from https://eur-lex.europa.eu/content/news/general-data-protectionregulation-GDPR-applies-from-25-May-2018.html

Information Commissioner's Office. (2021). *Vital interests*. Retrieved July 5, 2021, from https://ico.org.uk/fororganisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/lawful-basisfor-processing/vital-interests

Organization for Economic Co-operation and Development. (2021). *OECD guidelines on the protection of privacy and transborder flows of personal data.* Retrieved June 25, 2021, from https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionof privacyandtransborderflowsofpersonaldata.htm