ปัญหามาตรการรักษาความปลอดภัยข้อมูลภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

The Problems of Data Security Measures under The Framework of the Personal Data Protection Act*

*ณัฐวัฒน์ ตาแว่น***

กองบัญชาการสอบสวนกลาง สำนักงานตำรวจแห่งชาติ

Nuttawat Tawan

Central Investigation Bureau, Royal Thai Police

วันที่รับบทความ 20 พฤศจิกายน 2567; วันแก้ไขบทความ 19 เมษายน 2568; วันตอบรับบทความ 22 มิถุนายน 2568

บทคัดย่อ

ในยุคดิจิทัลนี้ข้อมูลส่วนบุคคลถือเป็นทรัพย์สินอันทรงคุณค่า ทั้งในระดับปัจเจกบุคคลและองค์กร โดยข้อมูลเหล่านี้ถูกรวบรวม ประมวลผล และใช้งานในหลากหลายลักษณะ เช่น ข้อมูลส่วนตัว ข้อมูลการติดต่อ ข้อมูลการเงิน และข้อมูลด้านสุขภาพ ซึ่งมีบทบาทสำคัญในเชิงธุรกิจและการให้บริการภาครัฐ อย่างไรก็ตาม การละเมิดข้อมูลส่วนบุคคลได้กลายเป็นภัยคุกคามสำคัญในยุคดิจิทัล โดยมิจฉาชีพไซเบอร์อาจใช้วิธีการโจมตี เช่น มัลแวร์ ฟิชชิ่ง และการขโมยข้อมูล เพื่อเข้าถึงข้อมูลอันเป็นความลับ ก่อให้เกิดความเสียหายแก่ทั้งบุคคลและองค์กร ส่งผลให้เกิดความสูญเสียทางการเงิน การทำลายชื่อเสียง และความเสี่ยงด้านความปลอดภัย ขณะที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ของประเทศไทยได้ถูกประกาศใช้เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและส่งเสริมการบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐานสากล อย่างไรก็ตาม เมื่อเทียบกับกฎหมายคุ้มครองข้อมูลของสหภาพยุโรป (GDPR) ยังพบข้อจำกัดด้านการบังคับใช้ PDPA ในประเทศไทย รวมถึงความไม่ชัดเจนในการปฏิบัติและขาดมาตรการความปลอดภัยที่ทันสมัยเพื่อตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว

งานวิจัยนี้มุ่งศึกษาวิเคราะห์และเปรียบเทียบการบังคับใช้ PDPA ของประเทศไทยกับ GDPR ของสหภาพยุโรปและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพผ่านการสัมภาษณ์เชิงลึกและการวิเคราะห์ข้อมูลจากแหล่งข้อมูลทุติยภูมิ ผลการศึกษาชี้ให้เห็นว่าการพัฒนาและบังคับใช้ PDPA ให้สอดคล้องกับมาตรฐานสากล เช่น การเพิ่มความเข้มงวดในการฝึกอบรมบุคลากร

---

* บทความนี้เป็นส่วนหนึ่งของการค้นคว้าอิสระ เรื่อง “ปัญหามาตรการรักษาความปลอดภัยข้อมูลภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” หลักสูตรวิทยาศาสตรมหาบัณฑิต
คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

** รองสารวัตร กองกำกับการ 1 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการสอบสวนกลาง สำนักงานตำรวจแห่งชาติ
ที่อยู่: กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ชั้น 6 อาคารกองบัญชาการตำรวจสอบสวนกลาง (พิทักษ์สันติ) เลขที่ 1106 ถนน พหลโยธิน แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900
E-mail: nuttawat.ta@police.go.th

การจัดทำแนวทางปฏิบัติที่ชัดเจนและเข้าใจง่าย ตลอดจนการเสริมสร้างมาตรการด้านความปลอดภัยที่สอดคล้องกับมาตรฐาน ISO 27001 จะช่วยเพิ่มประสิทธิภาพในการปฏิบัติตามกฎหมาย PDPA ในประเทศไทย งานวิจัยนี้เสนอแนะให้ประเทศไทยปรับปรุงกลไกการบังคับใช้กฎหมายและเพิ่มขีดความสามารถในการคุ้มครองข้อมูลส่วนบุคคล เพื่อรองรับภัยคุกคามทางไซเบอร์ในปัจจุบันและสร้างความเชื่อมั่นในความปลอดภัยของข้อมูลในยุคดิจิทัล

คำสำคัญ: มาตรการรักษาความปลอดภัยข้อมูล, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, ความเป็นส่วนตัว

Abstract

In the digital age, personal data is regarded as a valuable asset at both individual and organizational levels. This data is collected, processed, and utilized in various forms, including personal information, contact information, financial details, and health records, all of which play a critical role in business activities and public service delivery. However, breaches of personal data have emerged as significant threats in the digital era. Cybercriminals may employ tactics such as malware, phishing, and data theft to gain unauthorized access to confidential information, causing substantial harm to individuals and organizations alike. This often results in financial losses, reputational damage, and heightened security risks. While Thailand's Personal Data Protection Act B.E. 2562 (PDPA) was enacted to protect the rights of data owners and promote the management of personal data in alignment with international standards, challenges remain. When compared to the European Union's General Data Protection Regulation (GDPR), limitations in the enforcement of the PDPA in Thailand become evident, particularly regarding the clarity of its application and the absence of modern security measures capable of responding to rapidly evolving threats.

This study aims to analyze and compare the enforcement of Thailand's Personal Data Protection Act (PDPA) with the European Union's General Data Protection Regulation (GDPR) and Singapore's personal data protection laws. Using a qualitative research methodology, including in-depth interviews and secondary data analysis, the findings suggest that aligning PDPA implementation with international standards—such as intensifying personnel training, developing clear and accessible guidelines, and strengthening security measures in accordance with ISO 27001—would enhance PDPA compliance in Thailand. This research recommends that Thailand improve its enforcement mechanisms and augment its capacity to protect personal data, thereby addressing current cyber threats and fostering trust in data security within the digital age.

Keywords: Data Security Measures, Personal Data Protection Act, Privacy

1. บทนำ

ในยุคดิจิทัลที่ข้อมูลมีบทบาทสำคัญ ข้อมูลส่วนบุคคลเปรียบเสมือนทรัพย์สินที่มีค่าสำหรับทั้งปัจเจกบุคคลและองค์กร ซึ่งข้อมูลเหล่านี้ถูกเก็บรวบรวม นำไปประมวลผล และใช้งานในหลากหลายรูปแบบ ไม่ว่าจะเป็นข้อมูลส่วนตัว ข้อมูลการติดต่อ ข้อมูลการเงิน ข้อมูลสุขภาพ ข้อมูลประกัน ซึ่งข้อมูลเหล่านี้ล้วนมีความสำคัญต่อเจ้าของข้อมูล โดยข้อมูลเหล่านี้ถูกนำไปใช้เพื่อประโยชน์ส่วนตัว ธุรกิจ หรือบริการภาครัฐ ตัวอย่างการใช้ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลการสมัครงานเพื่อประเมินคุณสมบัติและติดต่อกลับข้อมูลการขอสินเชื่อสำหรับการประเมินความเสี่ยงทางการเงิน ข้อมูลการซื้อขายออนไลน์สำหรับการจัดส่งสินค้าและบริการ ข้อมูลจากโซเชียลมีเดียเพื่อใช้ในการแสดงโฆษณาให้ตรงกับความสนใจของผู้ใช้งาน เป็นต้น อย่างไรก็ตาม ข้อมูลส่วนบุคคลเหล่านี้มีความเสี่ยงต่อการถูกละเมิดโดยอาชญากรทางไซเบอร์ ซึ่งอาจส่งผลเสียหายร้ายแรงต่อทั้งปัจเจกบุคคลและองค์กร ตัวอย่างของการละเมิดข้อมูลที่พบบ่อย ได้แก่ การโจมตีทางไซเบอร์: แฮ็กเกอร์อาจใช้มัลแวร์ โทรจัน หรือไวรัส เพื่อแทรกซึมเข้าสู่ระบบคอมพิวเตอร์และขโมยข้อมูลส่วนบุคคล, การแฮ็กข้อมูล: แฮ็กเกอร์อาจโจมตีเว็บไซต์ หรือฐานข้อมูลเพื่อขโมยข้อมูลส่วนบุคคลจำนวนมาก, การรั่วไหลของข้อมูล: ข้อมูลส่วนบุคคลอาจถูกเปิดเผยโดยไม่ได้รับความยินยอม, Phishing scams: มิจฉาชีพอาจหลอกลวงผู้ใช้งานคอมพิวเตอร์ให้กระทำการอย่างใดอย่างหนึ่ง เพื่อให้เข้าถึงข้อมูล หรือสั่งให้โปรแกรมที่ผู้หลอกลวงซ่อนไว้เริ่มทำงาน เช่น การหลอกลวงให้เข้าเว็บไซต์ปลอมที่ทำเลียนแบบเว็บไซต์จริง โดยหลอกให้ผู้ใช้กรอกข้อมูลสำคัญส่วนบุคคล, Ransomware attacks: มัลแวร์ประเภทหนึ่งที่เข้ารหัสข้อมูลของผู้ใช้และเรียกร้องเงินค่าไถ่เพื่อปลดล็อกข้อมูล เป็นต้น โดยผลกระทบจากการละเมิดข้อมูลส่วนบุคคลอาจร้ายแรงต่อทั้งปัจเจกบุคคลและองค์กร ในส่วนของปัจเจกบุคคล อาจประสบปัญหาทางการเงิน สูญเสียชื่อเสียง ถูกขโมยเงิน หรือถูกคุกคาม ตัวอย่างเช่น ผู้ที่ถูกขโมยข้อมูลบัตรเครดิตอาจถูกนำไปใช้จ่ายโดยไม่ได้รับอนุญาต ข้อมูลส่วนตัวที่ถูกเปิดเผยอาจนำไปใช้เพื่อสร้างบัญชีปลอม หรือทำกิจกรรมฉ้อโกงอื่น ๆ และส่วนองค์กรอาจสูญเสียลูกค้า เสียหายทางการเงิน ถูกดำเนินคดี หรือสูญเสียชื่อเสียง ตัวอย่างเช่น องค์กรที่ถูกละเมิดข้อมูลอาจสูญเสียลูกค้าที่กังวลเกี่ยวกับความปลอดภัยของข้อมูล องค์กรอาจต้องจ่ายค่าปรับและค่าชดเชยความเสียหาย

กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือที่รู้จักกันในชื่อ PDPA (Personal Data Protection Act) มีบทบาทสำคัญทั้งในระดับสากลและระดับประเทศไทย กฎหมายเหล่านี้มุ่งเน้นไปที่การคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และส่งเสริมให้เกิดความโปร่งใสและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

ในต่างประเทศ หลายประเทศมีกฎหมาย PDPA ของตนเอง ตัวอย่างกฎหมาย PDPA ที่เป็นที่รู้จัก ได้แก่ General Data Protection Regulation (GDPR) ของสหภาพยุโรป, Personal Information Protection and Electronic Documents Act (PIPEDA) ของแคนาดา, Personal Information Protection Act (PIPA) ของเกาหลีใต้, Consumer Dat Right Bill ของประเทศออสเตรเลีย และ Act on Protection of Personal Information (APPI) ของญี่ปุ่น เป็นต้น แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศจะมีรายละเอียดและบริบทการบังคับใช้ที่แตกต่างกัน แต่พบว่ากฎหมายที่ได้รับการยอมรับในระดับสากล เช่น General Data Protection Regulation (GDPR) ของสหภาพยุโรป, Personal Information Protection and Electronic Documents Act (PIPEDA) ของแคนาดา และ Personal Information Protection Act (PIPA) ของสาธารณรัฐเกาหลี มีหลักการพื้นฐานบางประการที่คล้ายคลึงกัน อาทิ การให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึง แก้ไข ลบ หรือจำกัดการใช้ข้อมูลส่วนบุคคลของตนเอง ตลอดจนการกำหนดการเก็บรวบรวมและใช้

ข้อมูลส่วนบุคคลอย่างมีวัตถุประสงค์ที่ชัดเจน โดยดำเนินการเก็บข้อมูลเท่าที่จำเป็นเท่านั้น และไม่ใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ที่แจ้งไว้ นอกจากนี้ กฎหมายเหล่านี้ยังให้ความสำคัญกับความยินยอมใน ฐานะหนึ่งของพื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม ความยินยอมไม่ใช่ฐานเดียวที่อนุญาตให้มีการประมวลผลข้อมูลได้ โดยในบางกรณีอาจใช้ฐานอื่น เช่น สัญญา ผลประโยชน์โดยชอบธรรม หรือภาระหน้าที่ตามกฎหมาย ทั้งนี้ เพื่อให้เกิดความเหมาะสมระหว่างการคุ้มครองสิทธิของเจ้าของข้อมูลและการดำเนินงานขององค์กร

ในประเทศไทย กฎหมาย PDPA หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2565 ซึ่งมุ่งเน้นไปที่การคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และส่งเสริมให้เกิดความโปร่งใสและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล โดยกฎหมาย PDPA ของประเทศไทย มีความสำคัญในด้านการคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง สร้างความมั่นใจแก่บุคคลว่าข้อมูลส่วนบุคคลของตนจะถูกใช้โดยชอบด้วยกฎหมาย รวมไปถึงส่งเสริมให้เกิดความโปร่งใสและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล พัฒนาเศรษฐกิจดิจิทัลของประเทศไทย อย่างไรก็ตาม กฎหมาย PDPA ของประเทศไทยยังอยู่ในช่วงเริ่มต้นของการบังคับใช้ ซึ่งส่งผลต่อระดับความรู้และความเข้าใจทั้งในระดับบุคคลและองค์กร กลไกการบังคับใช้ โอกาสทางเทคนิคที่นำไปสู่การรั่วไหลของข้อมูล รวมไปถึงจุดอ่อน ข้อจำกัด และการตีความกฎหมาย PDPA ซึ่งอาจทำให้เกิดช่องว่างทางข้อกฎหมาย และมิจฉาชีพ หรืออาชญากรทางไซเบอร์ได้ใช้ช่องว่างนี้ในการกระทำความผิด รวมไปถึงการรับโทษจากการกระทำความผิดทางกฎหมายในการเข้าถึง เก็บรวบรวม ประมวลผล เปิดเผย เผยแพร่ และรุกรานข้อมูลส่วนบุคคล ตัวอย่างการก่ออาชญากรรมทางข้อมูลโดยอาศัยข้อบกพร่องในด้านเทคโนโลยี หรือระบบการทำงานที่อาจส่งผลกระทบต่อประสิทธิภาพ หรือความปลอดภัยของข้อมูลส่วนบุคคลในประเทศไทย เช่น ในกรณีบริษัทแอลวาย คอร์ป (LY Corp)[2] ซึ่งเป็นเจ้าของแอปพลิเคชัน LINE ประสบปัญหาการรั่วไหลของข้อมูลส่วนบุคคลถึง 440,000 ราย เนื่องจากมัลแวร์ในคอมพิวเตอร์ของพนักงานรายหนึ่งของบริษัท NAVER Cloud Corporation ซึ่งเป็นบริษัทคู่ค้าที่ให้บริการระบบคลาวด์แก่ไลน์, กรณีนายหน้าขายประกันภัยของบริษัทประกันชีวิตแห่งหนึ่ง[3] มีพฤติกรรมลักลอบนำข้อมูลส่วนบุคคลของลูกค้าไปขายให้กับกลุ่มมิจฉาชีพ และกรณีข้อมูลรั่วไหลจากอดีตพนักงานบริษัท เจไอบี คอมพิวเตอร์ กรุป จำกัด หรือ JIB[4] ซึ่งจัดจำหน่ายคอมพิวเตอร์และอุปกรณ์ไอที โดยข้อมูลที่รั่วไหลเป็นข้อมูลการซื้อสินค้าและข้อมูลส่วนบุคคลของลูกค้า JIB เป็นต้น

โดยปัจจุบันได้มีการละเมิดข้อมูลส่วนบุคคลอย่างเป็นวงกว้าง ส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลมีความสำคัญอย่างยิ่ง โดยหน่วยงานภายในประเทศไทยยังประสบกับข้อจำกัดและอุปสรรคในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตัวอย่างเช่น ในภาคธุรกิจประกันวินาศภัย[5] ซึ่งยังขาดอำนาจในการดำเนินงานที่จำเป็น ส่งผลให้ไม่สามารถเปิดเผย หรือแลกเปลี่ยนข้อมูลในฐานข้อมูล

---

[2] สภาองค์กรผู้บริโภค, 'ประกาศเว็บไซต์ LY Corporation (LINE) ชี้แจงเหตุข้อมูลรั่วไหลกว่า 400,000 บัญชี' (28 พฤศจิกายน 2566) <https://www.tcc.or.th/tcc_media/28112566_lineannouncement/> สืบค้นวันที่ 22 กรกฎาคม 2567

[3] ไทยพีบีเอส, 'คปภ.เพิกถอนใบอนุญาต "ตัวแทนประกัน" ลอบขายข้อมูลลูกค้า' (8 พฤศจิกายน 2566) <https://www.thaipbs.or.th/news/content/333644> สืบค้นวันที่ 22 กรกฎาคม 2567

[4] มติชนออนไลน์, 'JIB รับข้อมูลลูกค้ารั่วจริง ดำเนินคดีอดีตพนักงาน เร่งเยียวยา 4 ผู้เสียหาย' (28 มีนาคม 2567) <https://www.matichon.co.th/economy/news_4498411> สืบค้นวันที่ 22 กรกฎาคม 2567

[5] ชนิดำ เกิดกรรณ์, "ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลต่อระบบฐานข้อมูลการประกันภัยในธุรกิจประกันวินาศภัย", (2564) 6(1) วารสารนิติศาสตร์ รัฐศาสตร์ และสังคมศาสตร์ มหาวิทยาลัยราชภัฏเชียงราย, 287–309.

การประกันภัยกับบริษัทประกันวินาศภัยได้ ทั้งนี้ ยังพบข้อบกพร่องและไม่เหมาะสมในมาตรา 25 และ ในส่วนของสถาบันการเงิน[6] ปรากฏความไม่ชัดเจนในการกำหนดโครงสร้างองค์กรของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตลอดจนยังไม่มีการกำหนดคุณสมบัติมาตรฐานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ ยังมีความคลุมเครือในประเด็นการใช้ฐานความจำเป็นเพื่อประโยชน์โดยชอบธรรม (legitimate interest) เพื่อวัตถุประสงค์เดียวกัน โดยปราศจากมาตรฐานในวิธีการประเมิน และนโยบายการเก็บรักษาข้อมูล หรือหลักการอื่น ๆ ยังคงไม่ชัดเจน เป็นต้น โดยพระราชบัญญัติคุ้มครองข้อมูล พ.ศ. 2562 มีบทบาทและหน้าที่สำคัญในการเสริมสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และป้องกันการละเมิดทางไซเบอร์ โดยการกำหนดหลักการและข้อกำหนดในการจัดการข้อมูลส่วนบุคคลเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูลในยุคดิจิทัล

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อวิเคราะห์และเปรียบเทียบการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย กับกฎหมาย GDPR ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ โดยมุ่งเน้นศึกษามาตรการรักษาความมั่นคงปลอดภัยของข้อมูล รวมไปถึงประเด็นข้อจำกัด ด้านเทคโนโลยีที่ส่งผลต่อประสิทธิภาพในการปฏิบัติตามกฎหมาย ทั้งนี้ เพื่อเสนอแนวทางในการลดความเสี่ยงจากการละเมิดข้อมูลทางไซเบอร์ และเสริมสร้างการคุ้มครองสิทธิของเจ้าของข้อมูลและความมั่นคงขององค์กรภาคเอกชนภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. แนวคิดที่เกี่ยวข้อง

ความหมายของข้อมูลส่วนบุคคลในบริบทของการคุ้มครองข้อมูล

ข้อมูลส่วนบุคคลตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้โดยตรง หรือโดยอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม โดยในกฎหมายไทยนั้น ได้รับการคุ้มครองเป็นสิทธิขั้นพื้นฐานตามรัฐธรรมนูญ มาตรา 4 และมาตรา 35 ซึ่งรับรองศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคล การเผยแพร่ข้อมูลซึ่งอาจละเมิดความเป็นส่วนตัว หรือเกียรติยศของบุคคลโดยไม่ได้รับอนุญาตนั้นถือเป็นการละเมิดสิทธิ และกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีบทบาทในการรักษาความลับและความปลอดภัยของข้อมูลดังกล่าว

นิยามของข้อมูลส่วนบุคคลในมาตรฐานสากลและกฎหมายต่างประเทศ

ในกฎหมายระหว่างประเทศและระดับสากล ข้อมูลส่วนบุคคลนั้นมีการให้นิยามที่คล้ายคลึงกัน แต่ปรับตามบริบทของแต่ละประเทศ เช่น ในฮ่องกงและออสเตรเลีย[7] ข้อมูลส่วนบุคคลหมายถึงข้อมูลใด ๆ

---

[6] อริยะ ตังสวานิช,"ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562", (2564) Chulalongkorn University Theses and Dissertations (Chula ETD). 52-57. https://digital.car.chula.ac.th/chulaetd/5257 และทศพร โคตะมะ, 'ปัญหาการใช้ฐานความจำเป็นเพื่อประโยชน์โดยชอบของธนาคารพาณิชย์ในการประมวลผลข้อมูลส่วนบุคคล' (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย 2564)

[7] สุวคนธ์ ภมรสุวรรณ, 'ปัญหาการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : ศึกษา กรณีธุรกิจ' (เอกัตศึกษานิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย 2562)

ที่เชื่อมโยงกับบุคคลได้ ทั้งทางตรงและทางอ้อม รวมถึงความคิดเห็น หรือข้อมูลที่บันทึกไว้ในสื่อทุกรูปแบบ ในสหภาพยุโรปกฎหมาย GDPR ได้ระบุให้ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ได้รับการระบุตัวตน หรือสามารถระบุตัวตนได้ บุคคลธรรมดาที่ระบุตัวตนได้ หมายถึง บุคคลที่สามารถระบุตัวตนได้โดยตรง หรือโดยอ้อม โดยเฉพาะอย่างยิ่งโดยอ้างอิงถึงตัวระบุ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลที่ตั้งตัวระบุออนไลน์ หรือปัจจัยหนึ่งหรือหลายปัจจัยที่เฉพาะเจาะจงต่อลักษณะทางกายภาพ ทางสรีรวิทยา ทางพันธุกรรม ทางจิตใจ ทางเศรษฐกิจ ทางวัฒนธรรม หรือทางสังคมของบุคคลธรรมดานั้น เป็นต้น โดยมาตรฐาน NIST SP 800-122 ของสหรัฐอเมริกา[8] กำหนดให้แยกข้อมูลส่วนบุคคลออกเป็นสามประเภท[9] คือ ข้อมูลที่สามารถ “แยกแยะ” บุคคลได้โดยตรง (เช่น ชื่อและข้อมูลชีวมิติ) ข้อมูลที่ใช้ “ติดตาม” กิจกรรมของบุคคล และข้อมูลที่ “เชื่อมโยง” กับ ข้อมูลอื่นเพื่อระบุตัวตน

การจำแนกประเภทข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลสามารถแบ่งออกเป็นสองประเภทหลัก ได้แก่ ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล หมายเลขประจำตัวประชาชน ข้อมูลการติดต่อ และข้อมูลที่เกี่ยวกับอุปกรณ์ต่าง ๆ และข้อมูลที่มีความละเอียดอ่อน (Sensitive Data) เช่น เชื้อชาติ ความคิดเห็นทางการเมือง พฤติกรรมทางเพศ และข้อมูลสุขภาพ โดยข้อมูลที่มีความละเอียดอ่อนนี้มีความสำคัญอย่างยิ่งในการคุ้มครองความเป็นส่วนตัว

ข้อยกเว้นและมาตรการในการขอความยินยอม

กฎหมายกำหนดให้การจัดการข้อมูลส่วนบุคคลต้องได้รับความยินยอมจาก เจ้าของข้อมูล โดยกฎหมายคุ้มครองข้อมูลมักให้น้ำหนักกับความยินยอม (Consent) เป็นฐานทางกฎหมายหลัก อย่างไรก็ตามในบริบทของ GDPR ได้มีการพัฒนาให้มีฐานทางกฎหมายอื่นที่สำคัญไม่น้อยกว่า เช่น การปฏิบัติตามสัญญา การปฏิบัติตามกฎหมายการปกป้องผลประโยชน์ที่จำเป็น การดำเนินงานเพื่อภารกิจสาธารณะ และผลประโยชน์โดยชอบธรรม ซึ่งฐานเหล่านี้มักถูกใช้อย่างแพร่หลายในองค์กรเพื่อหลีกเลี่ยงปัญหาความไม่เข้าใจหรือการถอนความยินยอมของเจ้าของข้อมูล ซึ่งการให้น้ำหนักกับความยินยอมมากเกินไปอาจส่งผลให้เกิดความซับซ้อนในการดำเนินงาน และไม่สามารถตอบสนองต่อการคุ้มครองข้อมูลในบริบทที่ซับซ้อน เช่น การวิจัย วิทยาศาสตร์ หรือการบริหารงานรัฐ เมื่อไม่สามารถใช้ฐานทางกฎหมายอื่นได้ นอกจากนี้ยังมีแนวคิดเชิงทฤษฎีที่วิพากษ์ความสามารถของความยินยอม ในยุคที่ข้อมูลไหลเวียนอย่างรวดเร็ว โดยเสนอให้เน้นความโปร่งใสในการประมวลผล และการควบคุมโดยระบบ (Systemic safeguards) แทนการพึ่งพาความยินยอมของผู้ใช้แต่เพียงอย่างเดียว

2.1 แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิพื้นฐานที่มีรากฐานจากแนวคิดเรื่อง “สิทธิส่วนบุคคล” ซึ่งถือเป็นสิทธิธรรมชาติที่มนุษย์มีตั้งแต่กำเนิด โดยธรรมชาติแล้ว บุคคลย่อมมีความต้องการที่จะรักษาความเป็นส่วนตัวและปกปิดข้อมูลที่บ่งบอกถึงตัวตน เพื่อให้สามารถควบคุมการเข้าถึงและใช้ข้อมูลของตนได้อย่างอิสระ ความเป็นส่วนตัวในแง่นี้ได้รับการยอมรับว่าเป็นสิทธิมนุษยชนพื้นฐานที่ปรากฏอยู่ในปฏิญญาสากลว่าด้วย

---

[8] ปิยะบุตร บุญอร่ามเรือง, พัฒนาพร โกวพัฒนกิจ, ชวิน อุ่นภัทร, โมกข์พิศุทธิ์ รตารุณ และคณะ, Thailand data protection guidelines 3.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (พิมพ์ครั้งที่ 1, โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2563)

[9] วันพิชิต ชินตระกูลชัย, ‘ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว คืออะไร มีกี่ประเภท มีอะไรบ้าง ?’ (Openpdpa, 20 กันยายน 2564) <https://openpdpa.org/personal-data-type/> สืบค้นวันที่ 22 กรกฎาคม 2567

สิทธิมนุษยชน ซึ่งระบุว่า “บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการคุ้มครองจากการแทรกแซงโดยไม่ชอบด้วยกฎหมายในด้านความเป็นส่วนตัว ชีวิตครอบครัว หรือการสื่อสาร” หลักการนี้เป็นการยืนยันถึงสิทธิที่บุคคลสามารถปกป้องตนจากการเปิดเผย หรือใช้งานข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอม โดยถือเป็นการเคารพศักดิ์ศรีและเสรีภาพของบุคคล

แนวคิดการคุ้มครองสิทธิความเป็นส่วนตัวในปัจจุบันได้ขยายความหมายให้ครอบคลุมถึงข้อมูลส่วนบุคคล ซึ่งถูกนำไปใช้ประโยชน์ในเชิงธุรกิจ หรือการให้บริการต่าง ๆ การคุ้มครองสิทธิดังกล่าวจึงได้รวมถึงการรักษาความลับของข้อมูลในหลายระดับ โดยเฉพาะเมื่อเทคโนโลยีสมัยใหม่มีการเก็บ รวบรวม และวิเคราะห์ข้อมูลที่สามารถระบุตัวบุคคลได้อย่างแพร่หลาย ส่งผลให้บุคคลไม่มีอิสระในการควบคุมการใช้ข้อมูลของตน นำไปสู่ความเสี่ยงในการละเมิดสิทธิในหลายด้าน เช่น ความรู้สึกไม่ปลอดภัย การถูกรบกวน หรือความกังวลเกี่ยวกับความมั่นคงของชีวิต

ในแง่นี้ “สิทธิความเป็นส่วนตัว” จึงถูกกำหนดให้รวมถึงสิทธิในการกำหนดความยินยอม หรือ “หลักการยินยอม” ในการเปิดเผยและใช้ข้อมูลส่วนบุคคลโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงได้กำหนดเงื่อนไขในการให้ความยินยอมจากเจ้าของข้อมูล เพื่อรักษาความเป็นส่วนตัวของบุคคลตามหลักสิทธิขั้นพื้นฐาน อย่างไรก็ตาม สิทธินี้ไม่ใช่สิทธิที่ไม่มีขอบเขต ในบางกรณีการเข้าถึงข้อมูลอาจจำเป็นต่อสาธารณประโยชน์หรือนโยบายของรัฐ เมื่อมีความจำเป็นเพื่อประโยชน์ของชาติ หรือสาธารณะ เช่น ด้านความมั่นคง เศรษฐกิจ การป้องกันอาชญากรรม หรือการรักษาสุขอนามัย นอกจากนี้การกำหนดขอบเขตความเป็นส่วนตัวในข้อมูลส่วนบุคคลยังเป็นความท้าทายในการสร้างความสมดุลระหว่าง “สิทธิส่วนบุคคล” และ “สาธารณะ” ที่อาจมีความแตกต่างไปตามบริบทของวัฒนธรรมและระบบสังคม

ความหมายของ ‘พฤติกรรมการละเมิดข้อมูลส่วนบุคคล’

การละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) หมายถึง การกระทำที่จงใจ หรือกระทำโดยประมาท ซึ่งส่งผลกระทบต่อบุคคลอื่นในประเด็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างผิดกฎหมาย การละเมิดนี้อาจทำให้ผู้เสียหายได้รับความเดือดร้อนและต้องการการชดใช้ตามกฎหมาย โดยสามารถจำแนกพฤติกรรมการละเมิดได้ 4 ประเภทหลัก[10] ดังนี้

1) การเก็บรวบรวมข้อมูล (Information Collection) ซึ่งรวมถึงการสอดแนมและการสอบถามจากเจ้าของข้อมูลโดยที่อาจไม่ได้รับการตอบสนอง การสังเกตข้อมูลพฤติกรรมผ่านอุปกรณ์เทคโนโลยี เช่น การติดตามประวัติการใช้งานเว็บไซต์ ข้อมูลสุขภาพจากอุปกรณ์สวมใส่ ข้อมูลตำแหน่งจากสมาร์ทโฟน หรือการเก็บข้อมูลการซื้อสินค้าผ่านระบบชำระเงินออนไลน์

2) การประมวลผลข้อมูล (Data Processing) ซึ่งครอบคลุมการรวบรวมข้อมูลและการระบุตัวบุคคลอย่างไม่ปลอดภัย รวมถึงการใช้ข้อมูลในวัตถุประสงค์อื่นโดยไม่ได้รับ ความยินยอม เช่น การใช้ข้อมูลธุรกรรมการเงินของลูกค้าสำหรับการโฆษณาผลิตภัณฑ์เพิ่มเติม

3) การเปิดเผยข้อมูล (Information Dissemination) การกระทำนี้รวมถึงการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต เช่น การเปิดเผยข้อมูลทางการเงินให้กับหน่วยงานที่สามเพื่อการตลาด โดยไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอ

---

[10] คณาธิป ทองรวีวงศ์, คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล (พิมพ์ครั้งที่ 3, สำนักพิมพ์นิติธรรม 2565)

4) การรุกราน (Invasion) การแทรกแซงการควบคุมข้อมูลส่วนบุคคล เช่น การโจรกรรมข้อมูลจากฐานข้อมูลที่มีการรักษาความปลอดภัยไม่เพียงพอ รวมถึงการขโมยข้อมูลโดยไม่ได้รับความยินยอม

พฤติกรรมเหล่านี้รวมถึงการเข้าถึง เปิดเผย แก้ไข หรือทำลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งอาจเกิดจากความประมาท ความตั้งใจของบุคคล หรือองค์กรตลอดจนความผิดพลาดของระบบ ซึ่งล้วนส่งผลให้เกิดความเสียหายแก่เจ้าของข้อมูลอย่างมีนัยสำคัญ

ภาพรวมกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน

กลุ่มประเทศอาเซียนได้มีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยมีลักษณะและขอบเขตการบังคับใช้ที่แตกต่างกัน[11] ดังนี้

1) อินโดนีเซีย

ดำเนินการการออกกฎหมาย Law No.11 of 2008 ที่ว่าด้วยธุรกรรมและข้อมูลอิเล็กทรอนิกส์ซึ่งครอบคลุมเฉพาะบางประเภทข้อมูลเท่านั้น อาทิ Banking Law No.7 of 1992 และ The Capital Market Law No.8 of 1995 จนกระทั่งเมื่อวันที่ 17 ตุลาคม พ.ศ. 2565 ได้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDP Law) ซึ่งมีผลบังคับใช้ทั้งกับบุคคลในประเทศและนอกประเทศอินโดนีเซีย หากการดำเนินการมีผลในทางกฎหมาย หรือเกี่ยวข้องกับเจ้าของข้อมูลชาวอินโดนีเซีย

2) มาเลเซีย

เป็นประเทศแรกในอาเซียนที่ออกกฎหมาย Personal Data Protection Act 2010 (PDPA) ซึ่งบังคับใช้ตั้งแต่ปี พ.ศ. 2553 กฎหมายนี้กำหนดให้ผู้ควบคุมการประมวลผลข้อมูลต้องแจ้งรายละเอียดการนำข้อมูลไปใช้และขอความยินยอมจากเจ้าของข้อมูล ทั้งนี้ ข้อมูลต้องได้รับการเก็บรักษาอย่างปลอดภัย และกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

3) ฟิลิปปินส์

ดำเนินการบังคับใช้กฎหมาย Data Privacy Act of 2012 (REPUBLIC ACT NO. 10173) ซึ่งบังคับใช้ตั้งแต่ปี พ.ศ. 2555 มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลในทั้งภาครัฐและเอกชน รวมถึงการประมวลผลข้อมูลของพลเมืองฟิลิปปินส์ที่อยู่นอกประเทศ ฟิลิปปินส์กำหนดให้ผู้เก็บข้อมูลต้องแจ้งวัตถุประสงค์และขอความยินยอมจากเจ้าของข้อมูลก่อน การประมวลผลข้อมูล โดยเฉพาะในกรณีที่ข้อมูลนั้นมีความละเอียดอ่อน

4) สิงคโปร์

ประเทศสิงคโปร์บังคับใช้กฎหมาย Personal Data Protection Act 2012 (PDPA) อย่างเป็นทางการตั้งแต่ปี พ.ศ. 2557 โดยครอบคลุมการประมวลผลข้อมูลส่วนบุคคลของทุกองค์กร ไม่ว่าจะตั้งอยู่ในประเทศหรือไม่ กฎหมายกำหนดให้ต้องขอความยินยอมจากเจ้าของข้อมูลก่อนการใช้ และให้สิทธิในการถอนความยินยอม ทั้งนี้ สิงคโปร์มีแนวทางข้อยกเว้นจากการขอความยินยอมที่ชัดเจน เช่น การอนุมาน

[11] กิตติพงศ์ กมลธรรมวงศ์, 'ประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสาธารณรัฐสิงคโปร์ : บทเรียนสำหรับประเทศไทย' (2563) 2 วารสารสังคมวิจัยและพัฒนา, 7-29.

ความยินยอม และข้อยกเว้นเพื่อประโยชน์สาธารณะ ซึ่งช่วยให้การดำเนินธุรกิจมีความยืดหยุ่น ในขณะเดียวกันยังรักษาสมดุลกับการคุ้มครองสิทธิของเจ้าของข้อมูลได้อย่างมีประสิทธิภาพ

กฎหมาย PDPA ของประเทศสิงคโปร์ได้รับการปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับบริบทของเศรษฐกิจดิจิทัล ทั้งยังสามารถรักษามาตรฐานการคุ้มครอง ข้อมูลส่วนบุคคลในระดับสากลได้อย่างมีประสิทธิภาพ การศึกษากฎหมายของสิงคโปร์จึงมีความสำคัญต่อการพัฒนากฎหมายของประเทศไทย โดยเฉพาะในด้านการออกกฎหมายลำดับรอง กลไกการบังคับใช้ และมาตรการกำกับดูแล ทั้งนี้ เนื่องจากสิงคโปร์ถือเป็นประเทศผู้นำด้านเศรษฐกิจดิจิทัลในภูมิภาคอาเซียนกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์จึงได้รับการยอมรับในฐานะต้นแบบด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับภูมิภาค และถูกนำไปใช้อ้างอิงในประเทศอื่น ๆ รวมถึงประเทศไทย

มาตรฐานการรักษาความปลอดภัยข้อมูล (ระบบมาตรฐาน ISO/IEC 27001:2022)

มาตรฐานการรักษาความปลอดภัยข้อมูล (ระบบมาตรฐาน ISO/IEC 27001:2022)[12] มุ่งเน้นการจัดการความปลอดภัยของข้อมูลและความลับภายในองค์กร โดยให้กรอบการทำงานและแนวทางเพื่อเพิ่มความมั่นคงในการปกป้องข้อมูลขององค์กร ด้วยการประเมินและจัดการความเสี่ยง เพื่อลดความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูลสารสนเทศ ระบบนี้เหมาะสำหรับองค์กรที่ต้องการคุ้มครองข้อมูลส่วนบุคคล หรือข้อมูลธุรกิจที่มีความละเอียดอ่อน เพื่อให้การคุ้มครองข้อมูลส่วนบุคคล (PII) มีประสิทธิภาพ องค์กรต้องมีนโยบายและมาตรการที่ชัดเจนเกี่ยวกับการปกป้องและป้องกันข้อมูล โดยมีขั้นตอนสำคัญหลายประการ ดังต่อไปนี้

1) การประเมินความเสี่ยง

การประเมินและจัดการความเสี่ยงต่อข้อมูลส่วนบุคคลเป็นขั้นตอนสำคัญ ISO 27001 ระบุให้มีการประเมินความเสี่ยงที่อาจเกิดจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Clause 6.1.2) ซึ่งช่วยป้องกันผลกระทบที่อาจเกิดขึ้นและเพิ่มประสิทธิภาพในการปกป้องข้อมูล

2) นโยบายด้านความปลอดภัยข้อมูล

นโยบายความปลอดภัยควรชัดเจนและครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคล ISO 27001 (Clause 5.2) กำหนดให้มีการเผยแพร่นโยบายและสร้างความตระหนักแก่บุคลากร ซึ่งช่วยเสริมความเข้าใจและสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้ส่วนเสีย

3) การควบคุมการเข้าถึง

จำกัดสิทธิในการเข้าถึงข้อมูลเพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต ตามที่กำหนดใน Annex A.9 ของ ISO 27001 โดยต้องมีระบบควบคุมสิทธิตามบทบาทหน้าที่ของแต่ละบุคคล

4) การเข้ารหัสข้อมูล

ใช้เทคโนโลยีการเข้ารหัสเพื่อลดความเสี่ยงจากการถูกเปิดเผย Annex A.10 กำหนดให้มีการใช้การเข้ารหัสเพื่อปกป้องข้อมูลในขณะจัดเก็บและส่งข้อมูล

---

[12] International Organization for Standardization, 'ISO/IEC 27001:2022 – Information security management systems – Requirements' (October,2022) <https://www.iso.org/standard/27001> accessed 22 July 2024

5) การจัดการเหตุการณ์ข้อมูลรั่วไหล

มีขั้นตอนจัดการเหตุการณ์ที่ชัดเจนเพื่อรับมือกับข้อมูลรั่วไหล ตามข้อกำหนดใน Annex A.16 รวมถึงการแจ้งเตือนและการตรวจสอบสาเหตุ เพื่อฟื้นฟูระบบและลดผลกระทบจากการละเมิด

6) การฝึกอบรมและสร้างความตระหนัก

องค์กรควรฝึกอบรมบุคลากรเพื่อเสริมสร้างความเข้าใจเกี่ยวกับการปกป้อง ข้อมูลส่วนบุคคล และปฏิบัติตามนโยบายอย่างเคร่งครัด โดยข้อกำหนดใน Clause 7.2 ให้เน้นการสร้างความตระหนักและให้ความรู้ที่เกี่ยวข้อง

7) การตรวจสอบและปรับปรุงระบบ

การตรวจสอบและปรับปรุงระบบอย่างต่อเนื่องเป็นสิ่งสำคัญ ISO 27001 (Clause 10) เน้นให้ตรวจสอบการเปลี่ยนแปลงสภาพแวดล้อมและเทคโนโลยี เพื่อรักษาความมั่นคงของข้อมูล

8) การปฏิบัติตามกฎหมาย

องค์กรต้องปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูล เช่น PDPA หรือ GDPR เพื่อป้องกันความเสี่ยงจากการละเมิดกฎหมาย ข้อกำหนดใน Annex A.18 ครอบคลุมถึงการปฏิบัติตามกฎหมายและข้อสัญญาที่เกี่ยวข้อง

Annex A 5.34 ใน ISO 27001:2022

Annex A 5.34 มุ่งเน้นให้สร้างแนวทางปกป้อง PII เพื่อลดความเสี่ยงในการจัดการข้อมูลส่วนบุคคล ควรจัดทำนโยบายการจัดการ PII และมอบหมายหน้าที่ให้ Privacy Officer เพื่อดูแลการจัดการและประเมินผลกระทบด้านความปลอดภัย รวมถึงต้องตรวจสอบมาตรฐานเป็นระยะและปรับให้สอดคล้องตามกฎหมาย

ความแตกต่างจาก ISO 27001:2013

Annex A 5.34 ของ ISO 27001:2022 เป็นการปรับปรุงจาก Annex A 18.1.4 ในเวอร์ชั่น 2013 โดยเน้นการสร้างนโยบายเฉพาะด้านข้อมูลส่วนบุคคลและการจัดการข้อมูลในทุกขั้นตอนอย่างมีประสิทธิภาพ โดยมาตรฐาน ISO 27001:2022 ช่วยให้องค์กรสามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างปลอดภัย มั่นคง และสอดคล้องตามข้อกำหนดทางกฎหมาย

2.2 กรณีศึกษาที่เกี่ยวข้องกับมาตรการรักษาความปลอดภัยข้อมูล

1) กรณีศึกษาการใช้ข้อมูลส่วนบุคคลในการประมวลผลข้อมูล

ในยุคที่ข้อมูลเป็นปัจจัยสำคัญในการดำเนินธุรกิจ โดยเฉพาะการใช้ปัญญาประดิษฐ์ (AI) ในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน AI ถูกนำมาใช้ในหลายอุตสาหกรรม เช่น การธนาคาร การประกันภัย และ การให้บริการเกี่ยวกับธุรกิจออนไลน์ โดยหากมีการใช้ข้อมูลในปริมาณมาก ก็ยิ่งทำให้เกิดความเสี่ยงด้านความเป็นส่วนตัวของผู้ใช้สูงมากขึ้น

การให้ความสำคัญกับการปกป้อง รักษาข้อมูลส่วนบุคคลก็เป็นเรื่องที่สำคัญเช่นเดียวกัน ซึ่งหากไม่มีมาตราการการป้องกัน รักษา หรือจัดเก็บข้อมูลส่วนบุคคลอย่างเหมาะสม อาจทำให้ข้อมูลผู้ใช้เสี่ยงต่อการเข้าถึงโดยอาชญากรก็เป็นได้ ดังเช่นกรณีตัวอย่างดังต่อไปนี้

2) กรณีศึกษาตัวอย่างคดีที่เกิดขึ้น

คดี British Airways (ปี พ.ศ. 2561)[13]

สำนักงานคณะกรรมาธิการข้อมูลของสหราชอาณาจักร (Information Commissioner's Office หรือ ICO) ได้ทำการสั่งปรับเงินจำนวนมหาศาลถึง 183.39 ล้านปอนด์ กับสายการบินบริติช แอร์เวย์ส (British Airways) เนื่องจากเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลและข้อมูลทางการเงินของลูกค้าจำนวนมาก โดยเหตุการณ์นี้เกิดขึ้นระหว่างวันที่ 21 สิงหาคม ถึง 5 กันยายน พ.ศ. 2561 ซึ่งแฮกเกอร์สามารถเจาะระบบของสายการบินผ่านเว็บไซต์และแอปพลิเคชั่นของบริติช แอร์เวย์สได้สำเร็จ จากนั้นได้โจรกรรมข้อมูลสำคัญของลูกค้า เช่น ข้อมูลบัตรเครดิตและข้อมูลส่วนบุคคลต่าง ๆ ส่งผลให้ลูกค้าจำนวนมากเสี่ยงต่อการถูกนำข้อมูลไปใช้ในทางที่ผิด

ICO ให้เหตุผลในการปรับว่า สายการบินบริติช แอร์เวย์สมีการรักษาความปลอดภัยที่ไม่เพียงพอ ไม่สามารถปกป้องข้อมูลสำคัญของลูกค้าได้อย่างเหมาะสม เป็นเหตุให้ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และต้องเสียค่าปรับจำนวนมากเพื่อเป็นการกระตุ้นให้บริษัทที่จัดเก็บข้อมูลส่วนบุคคลตระหนักถึงความสำคัญของการป้องกัน ข้อมูลลูกค้าอย่างมีประสิทธิภาพ

คดีเกี่ยวกับบริษัท Facebook (ปี พ.ศ. 2566)[14]

ในปี พ.ศ. 2566 คณะกรรมการคุ้มครองข้อมูลแห่งสหภาพยุโรป (European Data Protection Board หรือ EDPB) ได้มีคำสั่งให้ Meta ซึ่งเป็นบริษัทแม่ของ Facebook จ่ายค่าปรับเป็นจำนวนสูงถึง 1.2 พันล้านยูโร ซึ่งถือเป็นค่าปรับที่สูงที่สุดเท่าที่เคยมีมาภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR (General Data Protection Regulation)

กรณีนี้เกิดขึ้นเนื่องจาก Meta มีการโอนข้อมูลส่วนบุคคลของผู้ใช้ Facebook ในสหภาพยุโรปไปยังเซิร์ฟเวอร์ในสหรัฐอเมริกา โดยการโอนข้อมูลนี้เกิดขึ้นในลักษณะที่ ไม่เป็นไปตามข้อกำหนดของ GDPR ซึ่งกฎหมายดังกล่าวมีข้อกำหนดที่เข้มงวดเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะการถ่ายโอนข้อมูลออกไปยังประเทศนอกเขตสหภาพยุโรป การโอนข้อมูลในลักษณะนี้ทำให้ข้อมูลของผู้ใช้ในสหภาพยุโรปเสี่ยงต่อการถูกเปิดเผย หรือนำไปใช้โดยไม่ได้รับการคุ้มครองตามมาตรฐานของ GDPR

การสืบสวนและดำเนินการในกรณีนี้เริ่มต้นโดยคณะกรรมการคุ้มครองข้อมูลแห่งไอร์แลนด์ (Irish Data Protection Commission หรือ DPC) ซึ่งเป็นหน่วยงานที่รับผิดชอบการกำกับดูแลกิจการของ Meta ในยุโรป เนื่องจากสำนักงานใหญ่ของ Meta ในยุโรปตั้งอยู่ในไอร์แลนด์ DPC พบว่า Meta ไม่สามารถให้การรับรองได้ว่าการโอนข้อมูลส่วนบุคคลไปยังสหรัฐอเมริกาจะเป็นไปตามมาตรการปกป้องข้อมูลของ

---

[13] คมปทิต คงศักดิ์ศรีสกุลม, 'British Airways ถูกสั่งปรับเงินเป็นสถิติกว่า 7 พันล้านบาท จากกรณีข้อมูลลูกค้ารั่วไหลในปี 2018 ?' (THE STANDARD, 8 กรกฎาคม 2562) <https://thestandard.co/british-airways-fine-over-passenger-data-breach/> สืบค้นวันที่ 22 กรกฎาคม 2567

[14] ไทยรัฐออนไลน์, 'META ยื่นฟ้อง Meta บริษัทแม่ Facebook ฐานละเมิดเครื่องหมายการค้า' (27 กรกฎาคม 2565) <https://www.thairath.co.th/news/tech/2456934> สืบค้นวันที่ 22 กรกฎาคม 2567

สหภาพยุโรปอย่างเคร่งครัด และอาจทำให้ข้อมูลผู้ใช้เสี่ยงต่อการเข้าถึงโดยหน่วยงานรัฐบาล หรือ องค์กรในสหรัฐฯ อย่างไม่เหมาะสม

คำสั่งปรับเงินนี้ไม่เพียงสะท้อนถึงการละเมิดข้อกำหนดของ GDPR แต่ยังเป็น การเตือนบริษัทเทคโนโลยีที่ให้บริการในยุโรปให้ปฏิบัติตามมาตรฐานสูงสุดในการคุ้มครองข้อมูลส่วนบุคคล การลงโทษนี้ยังเป็นการส่งสัญญาณให้เห็นถึงความมุ่งมั่นของสหภาพยุโรปในการปกป้องสิทธิและความเป็นส่วนตัวของผู้ใช้ในยุโรป

3) กรณีศึกษาการละเมิดข้อมูลทางด้านธุรกิจประกันภัย[15]

การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ได้ส่งผลกระทบต่อธุรกิจประกันภัยในประเทศไทย ซึ่งต้องมีการเก็บรวบรวมและประมวลผลข้อมูลของผู้เอาประกัน เพื่อใช้ในการพิจารณาการรับประกัน การเสนอขายกรมธรรม์ การพิจารณาสินไหม การบริการหลังการขาย และการประกันภัยต่อโดยบริษัทประกันภัยอาจได้รับข้อมูลจากโรงพยาบาล หรือบุคคลภายนอก แต่เมื่อ PDPA มีผลบังคับใช้ ผู้เอาประกันสามารถใช้สิทธิตามมาตรา 19 ในการถอนความยินยอมที่เคยให้ไว้ ซึ่งอาจทำให้เกิดปัญหาทางธุรกิจ เช่น หากลูกค้าถอนความยินยอมและกลับมาสมัครประกันใหม่โดยไม่เปิดเผยข้อมูลสำคัญ อาจส่งผลให้บริษัทไม่สามารถประเมินความเสี่ยงได้อย่างแม่นยำ

อย่างไรก็ตาม มาตรา 19 วรรคสี่ ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังได้วางหลักการที่สำคัญไว้ว่า *“ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็น หรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ”* จึงหมายความว่า เพื่อให้การดำเนินธุรกิจเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับกฎหมาย บริษัทประกันภัยควรกำหนดนโยบายที่ชัดเจนเกี่ยวกับการให้ความยินยอม โดยเฉพาะในกรณีที่เกี่ยวข้องกับข้อมูลสุขภาพ หรือข้อมูลอ่อนไหว ควรระบุว่า “การยินยอมจะมีผลตลอดอายุของสัญญา” ซึ่งถือว่ามีความจำเป็นตามวัตถุประสงค์ของสัญญาและอยู่ในขอบเขตของกฎหมาย

นอกจากนี้ ประเทศในสหภาพยุโรป เช่น สาธารณรัฐมอลตา ได้ออกกฎหมาย ฉบับใหม่ในปี 2020 ที่ชื่อว่า *Legal Notices 107 of 2020 Processing of Data concerning Health for Insurance Purposes (Amendment) Regulations* เพื่อเสริมข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลสุขภาพสำหรับธุรกิจประกันภัย โดยอนุญาตให้การประมวลผลข้อมูลสุขภาพเป็นไปตามวัตถุประสงค์ของการประกันภัยได้ในกรณีที่จำเป็น หรือในกรณีที่ไม่สามารถขอความยินยอมจากเจ้าของข้อมูลได้

ดังนั้น ในบริบทของธุรกิจประกันภัย ซึ่งต้องอาศัยการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะ ข้อมูลสุขภาพซึ่งถือเป็นข้อมูลอ่อนไหว บริษัทประกันภัยมักจะขอความยินยอมจากผู้เอาประกันภัยล่วงหน้าในขั้นตอนการทำสัญญา ทั้งนี้เพื่อให้สามารถนำข้อมูลดังกล่าวมาใช้ในการพิจารณารับประกัน การประเมินเบี้ย หรือบริการหลังการขาย

[15] สุวคนธ์ ภมรสุวรรณ (n 4) 8.

แม้การกำหนดให้ข้อมูลบางประเภทมีผลตลอดอายุสัญญาจะเป็นแนวทางที่มีเหตุผลในเชิงธุรกิจ แต่เพื่อให้เป็นไปตามมาตรา 19 วรรคสี่ บริษัทควรมีการแยกแยะระหว่าง “ข้อมูลที่จำเป็น” กับ “ข้อมูลเสริม” อย่างชัดเจน เช่น ข้อมูลที่ใช้เพื่อการตลาดหรือวิเคราะห์แนวโน้มลูกค้า ควรอยู่ภายใต้ “ทางเลือกให้ยินยอม” โดยไม่ผูกกับเงื่อนไขของสัญญาหลัก

การขอความยินยอมจึงควรมีลักษณะ “แยกเป็นรายการ (granular)” เปิดให้เจ้าของข้อมูลสามารถเลือกให้ความยินยอมเฉพาะส่วน และควรมีสิทธิถอนยินยอมได้ในส่วนที่ไม่กระทบต่อภาระผูกพันในสัญญาหลัก ทั้งนี้ เพื่อให้เกิดความสมดุลระหว่างประสิทธิภาพทางธุรกิจและการคุ้มครองสิทธิของเจ้าของข้อมูลตามหลักกฎหมาย

4) กรณีศึกษาการละเมิดข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา[16]

ในกระบวนการสืบสวนและสอบสวนคดีอาญาในประเทศไทย การคุ้มครอง ข้อมูลส่วนบุคคลได้รับการยกเว้นไม่ให้อยู่ภายใต้การบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ตามมาตรา 4 (2) ที่ให้ข้อยกเว้นแก่หน่วยงานของรัฐที่ดำเนินการเพื่อความมั่นคงของรัฐและความปลอดภัยสาธารณะ อย่างไรก็ตาม การยกเว้นดังกล่าวครอบคลุมกว้างและอาจเกินความจำเป็น เมื่อพิจารณาจากหลักการในระดับสากลที่มุ่งเน้นความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลกับภารกิจสาธารณะ (public task) ด้านการบังคับใช้กฎหมาย

ในสหภาพยุโรป มีการแยกบทบัญญัติเฉพาะสำหรับการบังคับใช้กฎหมายออกจาก GDPR โดยตราเป็น Law Enforcement Directive (LED) ซึ่งกำหนดมาตรฐานเฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลโดยเจ้าหน้าที่ตำรวจและหน่วยงานบังคับใช้กฎหมาย LED มีหลักการพื้นฐานคือการประมวลผลต้องอยู่ภายใต้กรอบกฎหมายที่ชัดเจน มีวัตถุประสงค์จำเพาะ และดำเนินการภายใต้หลักความจำเป็นและความได้สัดส่วน (necessity and proportionality)

แม้จะมีข้อยกเว้นสำหรับการบังคับใช้กฎหมาย แต่ภายใต้ LED ยังยืนยันสิทธิของเจ้าของข้อมูลในบางบริบท เช่น สิทธิในการเข้าถึง (subject access right) เว้นแต่จะกระทบต่อการสืบสวน และมีหลักการเรื่อง oversight โดยหน่วยงานกำกับอิสระเพื่อป้องกันการใช้ข้อมูลในทางที่ไม่เหมาะสม

ดังนั้น ในบริบทของประเทศไทย ควรมีการทบทวนข้อยกเว้นของ PDPA ที่ครอบคลุมการสืบสวนสอบสวนโดยสิ้นเชิง และปรับใช้แนวคิด “ภารกิจสาธารณะ” แทนการยกเว้นทั้งหมด เพื่อให้หน่วยงานรัฐสามารถปฏิบัติหน้าที่ได้โดยไม่ละเมิดสิทธิขั้นพื้นฐานของประชาชนอย่างไม่จำเป็น การนำกรอบแนวคิดจาก Law Enforcement Directive มาใช้ปรับปรุงกฎหมายวิธีพิจารณาความอาญาและกฎหมายที่เกี่ยวข้องจะช่วยยกระดับการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับมาตรฐานสิทธิมนุษยชนสากลมากยิ่งขึ้น

5) กรณีศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในบริษัทเฮเฟเล่ (ประเทศไทย) จำกัด[17]

การศึกษานี้เน้นแนวทางการคุ้มครองข้อมูลส่วนบุคคลในบริษัทเฮเฟเล่ (ประเทศไทย) จำกัด ซึ่งให้ความสำคัญกับการคุ้มครองข้อมูลของพนักงานทั้งในปัจจุบันและที่พ้นสภาพไปแล้ว โดยการศึกษาได้

---

[16] รติมา สุระรัตน์ชัย, ‘แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย 2565).

[17] ปิยธิดา ดวดขุนทด, อดิศักดิ์ วรพิวุฒิ และ ธัญญาทิพ พิชิตการค้า, ‘แนวทางการคุ้มครองข้อมูลส่วนบุคคลของพนักงานบริษัท กรณีศึกษา : บริษัท เฮเฟเล่ (ประเทศไทย) จำกัด’ (2566) 2 วารสารพัฒนาธุรกิจและอุตสาหกรรม, 29 - 42.

ดำเนินการในลักษณะเชิงคุณภาพ และใช้กลุ่มตัวอย่างที่เป็นพนักงานแผนกทรัพยากรมนุษย์และฝ่ายกฎหมาย รวมทั้งหมด 8 คน

ผลการศึกษาพบว่าแนวทางในการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทนำมาใช้นั้น ประกอบด้วย

1) การจัดทำนโยบายที่ชัดเจน เพื่อควบคุมการจัดการและการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน โดยมีการกำหนดขอบเขตที่ชัดเจนในการเข้าถึงและใช้ข้อมูลของพนักงาน

2) การกำหนดบทบาทและหน้าที่ของผู้รับผิดชอบ ซึ่งรวมถึงการมอบหมายบุคคล หรือแผนกที่รับผิดชอบในการจัดการและปกป้องข้อมูลส่วนบุคคลของพนักงาน และการกำหนดวิธีปฏิบัติงานที่ชัดเจนในการจัดเก็บ ใช้ และเผยแพร่ข้อมูล

3) การสื่อสารเพื่อความเข้าใจในองค์กร โดยการให้ความรู้และสร้างความเข้าใจให้กับพนักงานทุกฝ่ายเกี่ยวกับนโยบายและแนวทางการคุ้มครองข้อมูล เพื่อให้เกิดความตระหนักและสามารถปฏิบัติได้อย่างถูกต้อง

ทั้งนี้ แนวทางดังกล่าว บริษัทเฮเฟเล่ (ประเทศไทย) จำกัด สามารถป้องกันการรั่วไหลและการละเมิดข้อมูลส่วนบุคคลของพนักงานได้อย่างมีประสิทธิภาพ เนื่องจากยังไม่พบการรั่วไหลของข้อมูล หรือการละเมิดข้อมูลส่วนบุคคลของพนักงาน ทำให้เป็นตัวอย่างที่ดีในการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชน

การคุ้มครองข้อมูลส่วนบุคคลได้กลายเป็นประเด็นสำคัญในยุคดิจิทัลที่ข้อมูลส่วนบุคคลสามารถถูกเข้าถึงและเผยแพร่ได้ง่ายผ่านเทคโนโลยีใหม่ ๆ ทั้งนี้ เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวและรักษาความปลอดภัยของข้อมูลส่วนบุคคล ประเทศต่าง ๆ ได้กำหนดกฎหมายและมาตรการควบคุมอย่างเข้มงวด เช่น กฎระเบียบการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation - GDPR) ของสหภาพยุโรป ซึ่งเป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล ด้วยมาตรฐานการปกป้องข้อมูลที่มีความครอบคลุมและรัดกุม

ในประเทศไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act - PDPA) ถูกนำมาใช้เพื่อสร้างกลไกการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพและสอดคล้องกับแนวทางสากล โดย PDPA กำหนดหลักการและข้อกำหนดที่คล้ายคลึงกับ GDPR ในหลายประการ เช่น หลักการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล การปกป้องข้อมูลโดยให้สิทธิแก่เจ้าของข้อมูล รวมถึงการมีระบบควบคุมและตรวจสอบการจัดการข้อมูลของหน่วยงานที่เกี่ยวข้อง อย่างไรก็ตาม ความท้าทายสำคัญของ PDPA คือการประยุกต์ใช้ให้เกิดผลอย่างมีประสิทธิภาพ เนื่องจากข้อจำกัดด้านทรัพยากรและความเข้าใจของบุคคลทั่วไปและองค์กรต่าง ๆ เกี่ยวกับการปฏิบัติตามกฎหมายดังกล่าว

ในการศึกษานี้ได้วิเคราะห์ปัญหาที่เกิดขึ้นในการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทย โดยเปรียบเทียบกับมาตรฐานสากล ได้แก่ General Data Protection Regulation (GDPR) ของสหภาพยุโรป และ PDPA ของประเทศสิงคโปร์ ซึ่งทั้งสองฉบับถือเป็นต้นแบบที่ได้รับการยอมรับอย่างแพร่หลาย และถูกนำมาใช้เป็นแนวทางสำคัญในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงประเทศไทยด้วย การเปรียบเทียบดังกล่าวมีจุดมุ่งหมายเพื่อตรวจสอบว่าประเทศไทยยังมีข้อบกพร่อง หรือข้อจำกัดใดบ้างที่ควรได้รับการปรับปรุง ตัวอย่างเช่น การสร้างระบบสนับสนุนการตรวจสอบ การให้ความรู้แก่ผู้ประกอบการเกี่ยวกับการจัดการข้อมูลที่ถูกต้อง การเสนอแนวทางการพัฒนาการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย เช่น การสนับสนุนการอบรมและพัฒนาทรัพยากร

บุคคลในการตรวจสอบข้อมูลส่วนบุคคล การส่งเสริมการใช้เทคโนโลยีในการติดตามและควบคุมข้อมูล และการสร้างระบบการทำงานที่มีความโปร่งใสและสามารถตรวจสอบได้

3. บทวิเคราะห์

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ถูกประกาศใช้ในประเทศไทยเพื่อตอบสนองความต้องการในการปกป้องข้อมูลส่วนบุคคลที่เพิ่มขึ้นอย่างมากในยุคดิจิทัล แม้ว่ากฎหมายดังกล่าวจะเป็นก้าวสำคัญ แต่การบังคับใช้ยังประสบปัญหาหลายประการ เช่น การรั่วไหลของข้อมูล การละเมิดความปลอดภัยไซเบอร์ การใช้ข้อมูลในทางที่มิชอบ และความเข้าใจที่ไม่ชัดเจนเกี่ยวกับสิทธิเกี่ยวกับข้อมูลส่วนบุคคล ปัญหาเหล่านี้สะท้อนให้เห็นถึงการขาดความพร้อมของหลายหน่วยงานในด้านมาตรการรักษาความปลอดภัยข้อมูล ตัวอย่างการละเมิดข้อมูลที่เกิดขึ้นในประเทศไทย ได้แก่ ข้อมูลลูกค้ารั่วไหลจากองค์กรต่าง ๆ และการโจมตีทางไซเบอร์ที่โรงพยาบาลสระบุรี[18]และสถาบันโรคไตภูมิราชนครินทร์[19] ทำให้ข้อมูลผู้ป่วยและข้อมูลส่วนบุคคลถูกเปิดเผยสู่สาธารณะ

แม้ประเทศไทยจะมีการออกกฎหมาย PDPA เพื่อเสริมสร้างความปลอดภัยของข้อมูลส่วนบุคคล แต่ยังมีความท้าทายในการบังคับใช้ เช่น ข้อจำกัดในทรัพยากรและ ความเข้าใจของหน่วยงานต่าง ๆ ที่เกี่ยวข้องโดยเฉพาะด้านเทคนิคและการบริหารจัดการความเสี่ยง ทั้งนี้ ประเทศต่าง ๆ อย่างสหภาพยุโรปและสิงคโปร์ได้ใช้มาตรการที่เข้มงวดผ่านกฎหมาย GDPR และ PDPA ที่เน้นการรักษาความปลอดภัยและการป้องกันข้อมูลรั่วไหล ซึ่งเป็นแบบอย่างที่ประเทศไทยสามารถนำมาปรับใช้เพื่อเพิ่มความเข้มงวดและความชัดเจนในระบบการคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาด้วยระเบียบวิธีวิจัยเชิงคุณภาพ โดยการสัมภาษณ์ผู้ที่มีประสบการณ์ หรือเกี่ยวข้องกับพราะราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ เจ้าหน้าที่ตำรวจสังกัดกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้บริหารของบริษัทเอกชนด้านความปลอดภัย ผลการศึกษาพบว่า เจ้าหน้าที่ตำรวจและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กำลังเผชิญกับปัญหาที่สำคัญในการดำเนินงาน ได้แก่ การขาดแนวทางการตีความกฎหมายที่เป็นระบบและชัดเจน รวมถึงความท้าทายในการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ ประชาชนและองค์กรยังขาดความรู้เกี่ยวกับสิทธิเกี่ยวกับข้อมูลส่วนบุคคล การปรับปรุงกฎหมายในระดับรอง การจัดทำแนวปฏิบัติที่ชัดเจน การให้ความรู้เกี่ยวกับการรักษาความปลอดภัยข้อมูลตามระดับความเสี่ยง และการพัฒนาระบบตรวจสอบทางเทคนิค เช่น การจัดเก็บและการวิเคราะห์บันทึกการใช้งานในระบบที่เข้าถึงข้อมูลส่วนบุคคล เป็นมาตรการที่ควรปรับปรุงและเสริมสร้างให้สอดคล้องกับระดับความเสี่ยงของข้อมูลที่จัดเก็บและระดับความรุนแรงของการละเมิดข้อมูล ได้มีการเสนอแนะสำหรับการคุ้มครองข้อมูลโดยเน้นที่การประเมินความเสี่ยงและการนำมาตรการรักษาความปลอดภัยแบบ Resilience มาปรับใช้กับประเทศไทย เพื่อเสริมสร้างกลไกการฟื้นฟูและการตอบสนองต่อเหตุการณ์ละเมิด ข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานสากลด้านการคุ้มครองข้อมูล เช่น การกำหนดมาตรการรับมือกับเหตุการณ์ Data

---

[18] ไทยรัฐออนไลน์, ‘รพ.สระบุรี แจงโดนมัลแวร์โจมตี แต่ยังให้บริการได้ กู้คืนข้อมูลได้บางส่วน’ (9 กันยายน 2563) <https://www.thairath.co.th/news/local/central/1926969> สืบค้นวันที่ 17 เมษายน 2568

[19] ไทยพีบีเอส (Thai PBS), ‘รพ.แจ้งความถูกเจาะระบบ ข้อมูลคนไข้เสียหาย 40,000 คน’ (8 กันยายน 2564) <https://www.thaipbs.or.th/news/content/307720> สืบค้นวันที่ 17 เมษายน 2568

Breach รวมถึงการฟื้นฟูข้อมูลข้อตกลงระดับการให้บริการ (SLA) และระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (RTO) การประสานงานระหว่างหน่วยงานรัฐและภาคเอกชนเพื่อสร้างความเข้มแข็งในระบบการคุ้มครองข้อมูลส่วนบุคคลจะช่วยสร้างความมั่นใจในระบบรักษาความปลอดภัยข้อมูลส่วนบุคคล และเป็นการตอบสนองต่อภัยคุกคามในยุคดิจิทัลอย่างมีประสิทธิภาพ ในส่วนขององค์กรภาคเอกชน ได้ให้ความสำคัญกับกระบวนการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยเสนอแนวทางการดำเนินมาตรการด้านความมั่นคงปลอดภัยของข้อมูลเบื้องต้นที่ควรนำไปใช้ภายในองค์กร ได้แก่ การประยุกต์ใช้มาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล เช่น ISO/IEC 27001 และกรอบแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST (NIST Cybersecurity Framework) ตลอดจนการกำหนดนโยบายการกำกับดูแลภายในองค์กร (Policy Governance) การควบคุมสิทธิการเข้าถึงข้อมูล (Access Control) การยืนยันตัวตนของผู้ใช้งาน (Authentication) และการตรวจสอบการใช้งานระบบผ่านการบันทึกและติดตามข้อมูลการเข้าใช้งาน (Log Monitoring) นอกจากนี้ ควรให้ความสำคัญกับการจัดทำเอกสารก่อนการเข้าทำงาน และการจัดให้มีการอบรมพนักงานของบริษัท เพื่อให้ตระหนักเรื่องความปลอดภัยและเข้าใจในหลักปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับองค์กร

จากข้อมูลที่ได้จากการสัมภาษณ์ ผู้ให้ข้อมูลให้ความเห็นถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติที่ครอบคลุมและเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลในระดับหนึ่ง แต่ในทางปฏิบัติกลับยังขาดแนวทาง หรือระบบที่ชัดเจนและเป็นรูปธรรมสำหรับการนำกฎหมายไปใช้ในบริบทของประเทศไทย ส่งผลให้ผู้ที่เกี่ยวข้องในภาคส่วนต่าง ๆ ไม่สามารถปฏิบัติตามกฎหมายได้อย่างมีประสิทธิภาพ อันเนื่องมาจากความเข้าใจในตัวบทกฎหมายที่ยังอยู่ในวงจำกัด ผู้ให้สัมภาษณ์ยังเสนอว่าควรมีการประยุกต์ใช้แนวทางด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลจากต่างประเทศ เช่น GDPR ของสหภาพยุโรป และ PDPA ของประเทศสิงคโปร์ เป็นแนวทางที่ได้รับการยอมรับในระดับสากล โดยเฉพาะในด้านการกำหนดมาตรการทางเทคนิคและการบริหารที่ชัดเจน เช่น การควบคุมสิทธิการเข้าถึง การตรวจสอบเหตุการณ์ข้อมูลรั่วไหล และการแจ้งเหตุละเมิดข้อมูล ทั้งนี้ แม้ประเทศไทยจะมีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งเป็นกฎหมายลำดับรองเพื่อสนับสนุนการปฏิบัติตามพระราชบัญญัติฯ แต่ยังขาดการสื่อสารและถ่ายทอดแนวทางเหล่านั้นในรูปแบบที่เข้าใจง่ายและนำไปใช้ได้จริง ดังนั้น การพัฒนาแนวปฏิบัติที่ชัดเจน เข้าใจง่าย และสามารถประยุกต์ใช้ได้อย่างมีประสิทธิภาพในทุกภาคส่วน จึงเป็นสิ่งจำเป็นต่อการเสริมสร้างการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยให้เกิดผลในทางปฏิบัติอย่างแท้จริง อีกทั้ง ยังมีบทบาทสำคัญในการยกระดับภาพลักษณ์และความน่าเชื่อถือของประเทศไทยในบริบทของเศรษฐกิจดิจิทัล ซึ่งไม่เพียงแต่เพิ่มความเชื่อมั่นของผู้บริโภคภายในประเทศเท่านั้น แต่ยังส่งผลเชิงบวกต่อการดึงดูดนักลงทุนและพันธมิตรทางธุรกิจจากต่างประเทศ ที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นสิ่งสำคัญในโลกปัจจุบัน

4. บทสรุปและข้อเสนอแนะ

การคุ้มครองข้อมูลส่วนบุคคลได้รับความสนใจเป็นอย่างยิ่งในระดับสากล โดยหลายประเทศได้กำหนดกฎหมายและมาตรการเพื่อปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับบริบทและความต้องการเฉพาะของแต่ละภูมิภาค ในประเทศไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ได้ถูกกำหนดขึ้นเพื่อรับมือกับปัญหาการละเมิดข้อมูลและการโจมตีทางไซเบอร์ที่เพิ่มสูงขึ้น อย่างไรก็ตามการบังคับใช้

PDPA ในประเทศไทยยังคงมีข้อจำกัดในการลดปัญหาการละเมิดข้อมูลได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในกรณีการรั่วไหลของข้อมูลลูกค้าในองค์กรต่าง ๆ เช่น True Move H[20], Bangkok Airways[21] และ CP Freshmart[22] ซึ่งเหตุการณ์เหล่านี้ส่งผลให้ข้อมูลส่วนบุคคลถูกนำไปใช้ในทางที่มิชอบ อาจนำมาซึ่งความเสียหายต่อประชาชนและลดทอนความเชื่อมั่นต่อการคุ้มครองข้อมูลจากภาครัฐและองค์กรที่เกี่ยวข้อง

ปัญหาสำคัญที่พบในการบังคับใช้ PDPA ในประเทศไทยรวมถึงความบกพร่องในการรักษาความปลอดภัยของข้อมูล อาทิเช่น การรักษาความปลอดภัยในระบบดิจิทัลที่ยังไม่เข้มงวดเพียงพอ ส่งผลให้ข้อมูลเกิดการรั่วไหลและเสี่ยงต่อการนำไปใช้ในทางที่ไม่เหมาะสม นอกจากนี้ หน่วยงานต่าง ๆ ยังคงพบความท้าทายในการปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูล รวมถึงการขาดความเข้าใจในสิทธิของประชาชนภายใต้ PDPA ซึ่งเป็นอุปสรรคต่อการบรรลุเป้าหมายการคุ้มครองข้อมูลส่วนบุคคลอย่างสมบูรณ์

จากการศึกษาพบว่า การเพิ่มประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลสามารถทำได้โดยการจัดให้มีระบบบันทึกการเข้าถึงข้อมูลของบุคลากร การใช้เทคโนโลยีตรวจจับการเข้าถึงข้อมูลในแบบเรียลไทม์ การกำหนดบทลงโทษทางกฎหมายที่ชัดเจนและเข้มงวด ตลอดจนการบังคับให้หน่วยงานรายงานเหตุการณ์การละเมิดข้อมูล นอกจากนี้ ยังมีข้อเสนอแนะเพิ่มเติมเกี่ยวกับการจัดทำมาตรการรักษาความปลอดภัยข้อมูล ได้แก่ การบันทึก IP Address ของการเข้าถึงข้อมูลภายในองค์กร การจัดเก็บข้อมูลในรูปแบบที่ไม่สามารถระบุตัวบุคคลได้โดยตรง และใช้ระบบเข้ารหัสเพื่อรักษาความปลอดภัย การยืนยันตัวตนด้วยรหัสผ่านอย่างน้อยสองขั้นตอน การจัดทำคู่มือแนวทาง “Key Concepts Guidelines” เพื่อช่วยให้หน่วยงานต่าง ๆ ปฏิบัติตามข้อกำหนดของกฎหมายได้อย่างมีประสิทธิภาพ การประเมินระดับความเสี่ยงของข้อมูลส่วนบุคคลเพื่อนำไปสู่การจัดการข้อมูลตามมาตรการที่เหมาะสม และการจัดทำมาตรการ Resilience เพื่อให้หน่วยงานสามารถฟื้นตัวจากเหตุการณ์ Data Breach ได้อย่างมีประสิทธิภาพ งานวิจัยนี้เสนอแนวทางการประยุกต์ใช้ระบบดิจิทัลที่ต่อยอดจากองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยประกอบด้วย 3 แนวทางหลัก ได้แก่

1) Smart Consent Dashboard แพลตฟอร์มกลางที่เปิดโอกาสให้เจ้าของข้อมูลสามารถเข้าถึง ตรวจสอบ และเพิกถอนความยินยอมในการใช้ข้อมูลได้อย่างโปร่งใส โดยใช้เทคโนโลยีบล็อกเชนเป็นกลไกยืนยันความถูกต้องของกระบวนการ

2) ระบบจำลองสถานการณ์การรับมือเหตุข้อมูลรั่วไหล (Data Breach Response Simulation) เพื่อประเมินความพร้อมของหน่วยงานและบุคลากร รวมถึงเพิ่มขีดความสามารถในการตอบสนองต่อเหตุการณ์จริง

---

[20] ณัชธนัท จุโฬทก, ‘สรุปหลัง TrueMove H ชี้แจงกับ กสทช. เรื่องข้อมูลหลุด ความจริงคืออะไร?’ (Beaetai, 18 เมษายน 2561) https://www.beartai.com/tech/local-news/233905> สืบค้นวันที่ 22 กรกฎาคม 2567

[21] ไทยรัฐออนไลน์, ‘Bangkok Airways แจงกรณี ถูกโจมตีความปลอดภัยทางไซเบอร์’ (26 สิงหาคม 2564) <https://www.thairath.co.th/money/business_marketing/marketing/2177868> สืบค้นวันที่ 22 กรกฎาคม 2567

[22] ถนัดกิจ จันกิเสน, ‘CP Freshmart ยอมรับข้อมูลลูกค้าถูก ‘แฮ็ก’ จริง แต่ย้ำไม่มีข้อมูลบัตรเครดิตหรือข้อมูลด้านการเงินและไม่กระทบต่อธุรกิจ’ (The Standard, 8 กันยายน 2564) <https://thestandard.co/cp-freshmart-admit-customer-account-hacked/> สืบค้นวันที่ 22 กรกฎาคม 2567

3) บริการ Compliance-as-a-Service ระบบสนับสนุนการประเมินความเสี่ยง การบันทึกเหตุการณ์ และการบริหารจัดการสิทธิการเข้าถึง สำหรับองค์กรที่มีข้อจำกัด ด้านทรัพยากร หรือความเชี่ยวชาญ เช่น วิสาหกิจขนาดกลางและขนาดย่อม (SMEs)

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ของประเทศไทยจะมีบทบัญญัติที่สอดคล้องกับหลักการสากลในด้านการคุ้มครองสิทธิของเจ้าของข้อมูล หากแต่ในทางปฏิบัติยังปรากฏข้อจำกัดเชิงโครงสร้างในการบังคับใช้กฎหมาย โดยเฉพาะกลไกในการตรวจสอบเชิงรุกและการดำเนินการก่อนเกิดเหตุที่ยังไม่พัฒนาอย่างเพียงพอ หน่วยงานกำกับดูแลหลักอย่างสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ยังคงทำหน้าที่ในลักษณะของผู้รับเรื่องร้องเรียนมากกว่าการเป็นผู้ควบคุมและกำกับเชิงนโยบายที่มีบทบาทเชิงรุก ทั้งในด้านการเฝ้าระวัง การสืบสวน และการลงโทษ ในทางเปรียบเทียบ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (PDPA) ภายใต้การกำกับดูแลของ Personal Data Protection Commission (PDPC) มีแนวทางการบังคับใช้ที่กระตือรือร้นและมีประสิทธิภาพสูงกว่าอย่างชัดเจน โดย PDPC ดำเนินการเชิงรุก เช่น การล่อซื้อข้อมูลส่วนบุคคลเพื่อพิสูจน์การกระทำผิดและการเปิดเผยรายละเอียดของคดีละเมิดที่ได้รับการวินิจฉัยแล้ว เพื่อเสริมสร้างการปฏิบัติตามกฎหมายในระดับองค์กรและสร้างแรงจูงใจทางสังคม ขณะเดียวกัน GDPR ถือเป็นแบบอย่างของกฎหมายระดับนานาชาติที่มีมาตรฐานทั้งในด้านหลักการ การคุ้มครองสิทธิของเจ้าของข้อมูล และกลไกการบังคับใช้ โดยเฉพาะอำนาจของหน่วยงานกำกับดูแลในแต่ละประเทศสมาชิกมีสถานะอิสระโดยสมบูรณ์ มีอำนาจออกคำสั่ง ตรวจสอบ ปรับเงินในอัตราที่สูง รวมถึงสั่งระงับการประมวลผลข้อมูลได้โดยไม่ต้องรอให้เกิดความเสียหายขึ้นก่อน ความเข้มแข็งของกลไกเหล่านี้ทำให้ GDPR ไม่เพียงแต่เป็นเครื่องมือทางกฎหมาย แต่ยังทำหน้าที่เป็นกรอบบรรทัดฐานสากลที่ประเทศต่าง ๆ รวมถึงประเทศไทยต้องให้ความสำคัญ เมื่อพิจารณาเปรียบเทียบในเชิงโครงสร้างแล้ว จะเห็นได้ว่าปัญหาหลักของไทยอยู่ที่ “กลไกการบังคับใช้” ซึ่งยังขาดทั้งอำนาจ อิสระ และทรัพยากรในการดำเนินการอย่างทันท่วงที ในขณะที่สิงคโปร์และประเทศสมาชิก EU มีแนวทางที่ชัดเจนในการให้ความสำคัญกับการกำกับดูแลที่เข้มแข็งและโปร่งใส ในประเทศไทยก็มีแนวทางในลักษณะเดียวกันผ่านประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งกำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องดำเนินมาตรการรักษาความมั่นคงปลอดภัยทั้งในด้านเทคนิคและการบริหารจัดการตามระดับความเสี่ยงของข้อมูล โดยเน้นหลักการประเมินผลกระทบด้านการคุ้มครองข้อมูลเพื่อพิจารณาความเหมาะสมของมาตรการต่าง ๆ ก่อนการดำเนินการ ทั้งนี้ ประกาศดังกล่าวยังเน้นเรื่องความรับผิดชอบเชิงรุกและการมีแผนรองรับเหตุการณ์ละเมิดข้อมูลซึ่งสะท้อนถึงความพยายามในการยกระดับมาตรฐานให้ใกล้เคียงกับสากล แม้จะยังอยู่ในระยะเริ่มต้นของการบังคับใช้ก็ตาม ดังนั้น หากประเทศไทยมีความมุ่งหวังจะยกระดับการคุ้มครองข้อมูลให้มีมาตรฐานสากล PDPA ควรได้รับการทบทวนทั้งใน ด้านบทบัญญัติรอง โครงสร้างของหน่วยงานกำกับดูแล และมาตรการรักษาความปลอดภัยข้อมูล เพื่อให้สามารถดำเนินการเชิงรุกได้อย่างแท้จริง และไม่ต้องรอให้เกิดความเสียหายขึ้นก่อนจึงจะมีการตอบสนอง

ข้อเสนอแนะในการปรับปรุง PDPA ของไทยให้สอดคล้องกับมาตรฐานสากล:

1. การประเมินความเสี่ยงและการป้องกันเชิงรุก เป็นการเพิ่มมาตรการการประเมิน ผลกระทบจากการใช้ข้อมูล เช่นเดียวกับ DPIA ของ GDPR เพื่อให้การเก็บรวบรวมข้อมูลส่วนบุคคลมีการพิจารณาความเสี่ยงล่วงหน้าและมีมาตรการป้องกันความเสียหายที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

2. การตรวจสอบการใช้งานและควบคุมการเข้าถึงข้อมูลตามความเสี่ยง กล่าวคือ ได้นำเทคโนโลยีมาใช้ในการตรวจจับการเข้าถึงข้อมูลที่ไม่เหมาะสมในแบบ Real-time โดยจัดให้มีการบันทึก IP Address หรือ URL ที่เข้าถึงข้อมูลทุกครั้ง รวมถึงการจำกัดการเข้าถึงข้อมูลตามสิทธิที่ได้รับอนุญาตเพื่อลดความเสี่ยงในการเข้าถึงข้อมูลที่ไม่ถูกต้อง

3. มาตรการการป้องกันข้อมูลส่วนบุคคลตามระดับความเสี่ยง กำหนดมาตรการการป้องกันข้อมูลที่สอดคล้องกับความเสี่ยงของข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูลเพื่อป้องกันไม่ให้สามารถระบุตัวตนได้โดยตรง การกำหนดการยืนยันตัวตนที่เข้มงวดขึ้นโดยใช้การพิสูจน์ตัวตนหลายระดับ (Multi-Factor Authentication - MFA) สำหรับข้อมูลที่มีความเสี่ยงสูง

4. การสร้างความรู้และความเข้าใจในเรื่องสิทธิการคุ้มครองข้อมูล ส่งเสริมความรู้ให้ประชาชนและองค์กรมีความเข้าใจและตระหนักถึงสิทธิของตนในการควบคุมข้อมูลส่วนบุคคล เช่น สิทธิในการขอความยินยอมและสิทธิในการขอเข้าถึงข้อมูล โดยควรจัดทำคู่มือแนวปฏิบัติและการให้คำแนะนำที่ชัดเจนสำหรับผู้ใช้งานทั่วไปและองค์กร แม้ว่าสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) จะได้ออกแนวปฏิบัติและคู่มือเพื่อประกอบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วหลายฉบับ แต่แนวทางเหล่านี้ยังมีลักษณะเป็นคำอธิบายเชิงหลักการ หรือเชิงนโยบายทั่วไป ที่อาจไม่ครอบคลุมกรณีการใช้งานจริงในหลากหลายบริบท โดยเฉพาะในภาคส่วนที่ขาดบุคลากรที่มีความรู้ความเข้าใจด้านกฎหมาย หรือเทคโนโลยี เช่น หน่วยงานรัฐระดับปฏิบัติการ วิสาหกิจขนาดกลางและขนาดย่อม (SMEs) หรือผู้ประกอบการรายย่อย ซึ่งนำไปสู่ความไม่ชัดเจนในการปฏิบัติและความเสี่ยงต่อการตีความผิด อันอาจส่งผลต่อความรับผิดตามกฎหมาย

อีกทั้งการปรับปรุงกฎหมาย PDPA ให้สอดคล้องกับมาตรฐาน GDPR และ PDPA ของสิงคโปร์จะช่วยเพิ่มความมั่นใจให้กับประชาชนในเรื่องความปลอดภัยของข้อมูลส่วนบุคคล ลดความเสี่ยงจากการละเมิดข้อมูลในองค์กรทั้งภาครัฐและเอกชน และส่งเสริมการปฏิบัติตามมาตรการป้องกันข้อมูลที่สอดคล้องกับมาตรฐานสากล อันจะทำให้ระบบการคุ้มครองข้อมูลของไทยมีความเข้มแข็งและน่าเชื่อถือมากยิ่งขึ้น