บทความวิชาการ

ความจำเป็นในการมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*

THE NECESSITY FOR HAVE A PERSONAL DATA PROTECTION ACT, B.E. 2562

วริษา อุบล
Warisa Ubon
สถานีตำรวจนครบาลสายไหม
Sai Mai Police Station, Thailand
นนทนา นิยมรุ่งเรืองชัย
Nonthana Niyomrungrueangchai
กรมธนารักษ์
The Terasury Department, Thailand
Corresponding author E-mail: warisaubon@gmail.com

บทคัดย่อ

ปัจจุบันได้มีพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาในประเทศไทย นับได้ว่าเป็นพระราชบัญญัติที่มีความใหม่และมีความสำคัญ ซึ่งในประเทศไทยได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 เนื่องจากความก้าวหน้าทางเทคโนโลยีที่มีความเปลี่ยนแปลงอย่างรวดเร็วและมีแนวโน้มของการเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวที่เพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยมิชอบ หรือโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล เพื่อประโยชน์ในทางการค้าหรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำความผิดต่างๆ เช่น การฉ้อโกง การหมิ่นประมาท เป็นต้น ปัญหาเหล่านี้ได้ส่งผลกระทบต่อความเชื่อมั่นในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามนโยบายของรัฐบาล ดังนั้น ประเทศไทยจึงเร่งผลักดันให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นมาตรฐานเดียวกัน

* Received 5 February 2023; Revised 18 April 2023; Accepted 26 April 2023

และสอดคล้องกับมาตรฐานที่เป็นสากลและเพื่อแก้ไขปัญหาทางละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ยังครอบคลุมไปถึงข้อมูลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว หรือ Sensitive Personal Data อีกด้วย กฎหมายฉบับนี้จึงเป็นประโยชน์อย่างมาก โดยข้อบังคับกฎหมายนี้จะให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติการทำงาน และข้อมูลส่วนบุคคลประเภทอื่น ๆ เช่น ลายพิมพ์นิ้วมือ บันทึกเสียง เลขบัตรประชาชน หรือข้อมูลการใช้งานเว็บไซต์ เพื่อประโยชน์โดยที่เจ้าของข้อมูลที่มิได้ให้ยินยอม

โดยข้อมูลส่วนบุคคล (Personal Data) นั้นคือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล, ที่อยู่, เลขบัตรประชาชน, ข้อมูลสุขภาพ, หมายเลขโทรศัพท์, e-mail, ประวัติอาชญากรรม เป็นต้น

คำสำคัญ: ข้อมูลส่วนบุคคล, เจ้าของข้อมูลส่วนบุคคล, การละเมิดสิทธิ

Abstract

At present, there is a Personal Data Protection Act B.E. 2562 in Thailand. It can be considered as a new and important Act. In Thailand, the Personal Data Protection Act B.E. 2562 has been announced, effective on June 1, 2022. Due to the advancement. Due to the advancement in technology that is changing rapidly and there is a tendency of infringement of personal data rights and increasing privacy rights, especially the use of personal data for exploitation or unlawful disclosure. Or without the consent of the data subject for commercial purpose or of the benefit of using personal information to commit various offenses such as fraud, defamation, etc. These problems have affected the confidence in digital development for the economy and society according to the government's policies. To create a mechanism to protect personal data as the same standard and in accordance with the standard that is universal and to effectively solve the problem of personal data breach.

The PDPA law also covers information that is sensitive personal data or Sensitive Personal Data as well. This law is therefore beneficial to consumers. The PDPA will protect personal information such as education. financial status, health history work history and other types of personal information such as fingerprints, voice recordings, ID card numbers or website usage data for the benefit without consent of the owner of the information.

Personal data (Personal Data) is information about a person that can be identified either directly or indirectly, such as name-surname, address, ID card number, health information, telephone number, email address, criminal record, etc.

Keywords: Personal Data, Data Subject, Infringement of Personal

บทนำ

สิทธิความเป็นส่วนตัวนั้นเป็นสิทธิหนึ่งในมนุษยชนและเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่ได้รับการรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) ต้องได้รับการคุ้มครองตามกฎหมายแนวคิดในการคุ้มครองสิทธิความเป็นส่วนตัวได้เกิดขึ้นมานานและหลากหลาย แนวคิดหนึ่งที่ได้รับการยอมรับและมีการอ้างอิงถึงอย่างแพร่หลาย คือ แนวคิดของซามูเอล ดี. วอร์เรน (Samuel D. Warren) และหลุยส์ ดี. แบรนดีส (Louis D. Brandeis) ในปี ค.ศ. 1980 ที่ได้ให้ความหมายคำว่า Privacy ในรูปของวลีสั้นๆ ว่า “สิทธิที่จะอยู่ตามลำพัง” หรือ “Right to be let alone” แม้ว่า “ความเป็นส่วนตัว” จะมีความหมายหลายประการ กล่าวคือ ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล ความเป็นส่วนตัวในอาณาเขตหรือสถานที่ของตนเอง ความเป็นส่วนตัวในชีวิตร่างกาย ความเป็นส่วนตัวในการติดต่อสื่อสาร แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญในสังคมยุคใหม่ คือ “ความเป็นส่วนตัวในข้อมูลส่วน บุคคล” เนื่องจากพัฒนาการทางคอมพิวเตอร์โดยเฉพาะอย่างยิ่งเทคโนโลยีอินเทอร์เน็ตที่ได้ส่งผลให้การติดต่อสื่อสารการเผยแพร่ข้อมูลต่างๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่ทำให้การประมวลผล จัดเก็บ หรือการเปิดเผยข้อมูลส่วน บุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว ในทางตรงกันข้ามนั้นจึงอาจมีการนำประโยชน์จากเทคโนโลยีเหล่านี้ไปใช้ในการละเมิดต่อบุคคลอื่นได้

ปัจจุบันได้มีพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาในประเทศไทย นับได้ว่าเป็นพระราชบัญญัติที่มีความใหม่และมีความสำคัญ ซึ่งในประเทศไทยได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 เนื่องจากความก้าวหน้าทางเทคโนโลยีที่มีความเปลี่ยนแปลงอย่างรวดเร็วและมีแนวโน้มของการเกิดการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวที่เพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยมิชอบ หรือโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลเพื่อประโยชน์ในทางการค้าหรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำความผิดต่าง ๆ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act B.E. 2562 (PDPA) เป็นกฎหมายว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคลการสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้อย่างถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลของบุคคลอนุญาต พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจึงมีบทบาทสำคัญและให้สิทธิกับเจ้าของข้อมูลส่วนบุคคลของเราเองรวมถึงได้สร้างมาตรฐานใหม่ให้เกิดขึ้นกับบุคคลหรือนิติบุคคลในการเก็บข้อมูล รวบรวมข้อมูลส่วนบุคคล รวมถึงการใช้ข้อมูลหรือการเปิดเผยข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมายนี้หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามก็จะมีโทษทั้งทางแพ่ง โทษทางอาญาและโทษทางปกครอง

ดังนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA นั้น ไม่ได้ประกาศออกมาเพื่อเป็นกฎหมายให้กับองค์กรภาครัฐ หรือเอกชนปฏิบัติตามเท่านั้น แต่ออกมาเพื่อใช้คุ้มครองข้อมูลส่วนบุคคลให้กับเหล่าประชาชนคนทั่วไปเป็นสำคัญโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุกฎหมายไว้ว่า ห้ามให้หน่วยงานที่มีข้อมูลส่วนบุคคลทั้งภาครัฐ หรือเอกชน เอาข้อมูลส่วนบุคคลไปใช้ในกิจกรรมอื่นหากเจ้าของข้อมูลไม่ยินยอม

พระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act B.E. 2562 (PDPA) ที่ใช้บังคับในประเทศไทยนั้น มีบทบาทในการคุ้มครองและใช้สิทธิที่มีต่อข้อมูลส่วนบุคคลรวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคลในการเก็บข้อมูลส่วนบุคคล, รวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเพื่อเปิดเผยข้อมูลส่วนบุคคล (T-reg.co.Ltd, 2564) ที่จะต้องปฏิบัติตามพระราชบัญญัตินี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA นั้นก็คือ เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคลสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูก

วัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาตและยังเป็นกฎหมายใหม่ที่ออกมาเพื่อแก้ไขปัญหาการถูกล่วงละเมิดข้อมูลส่วนบุคคลที่เพิ่มมากขึ้นเรื่อยๆ ในปัจจุบัน เช่น การซื้อขายข้อมูลเบอร์โทรศัพท์และข้อมูลส่วนตัวอื่นๆ โดยที่เจ้าของข้อมูลไม่ยินยอม โดย PDPA นั้นได้ถอดแบบจากกฎหมายที่เป็นแบบอย่างกฎหมาย GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป วัตถุประสงค์ของการเก็บรักษาข้อมูลส่วนบุคคลของกฎหมายทั้ง 2 ฉบับ ก็เพื่อป้องกันไม่ให้ ผู้ที่ไม่ประสงค์ดีทำการแฮ็กข้อมูลหรือละเมิดความเป็นส่วนตัวนำมาข่มขู่เพื่อหวังผลประโยชน์ทั้งจากตัวเจ้าของข้อมูลเองหรือจากบุคคลที่ดูแลข้อมูล (IT Information Technology, 2565)

ความสำคัญของพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) คือ การทำให้เจ้าของข้อมูลมีสิทธิในข้อมูลส่วนตัวที่ถูกจัดเก็บไปแล้วหรือกำลังจะถูกจัดเก็บมากขึ้น เพื่อสร้างความปลอดภัยและเป็นส่วนตัวให้แก่เจ้าของข้อมูลโดยมีสิทธิที่สำคัญ คือ สิทธิการรับทราบและยิมยอมการเก็บข้อมูลส่วนตัว และสิทธิในการขอเข้าถึงข้อมูลส่วนตัว คัดค้านและเพิกถอนการเก็บและนำข้อมูลไปใช้และสิทธิขอให้ลบหรือทำลายข้อมูลส่วนตัวสิทธิที่เพิ่มขึ้นของเจ้าของข้อมูลทำให้ผู้ประกอบการขององค์กรและบริษัทต่างๆ ต้องปรับเปลี่ยนกระบวนการเก็บรวบรวมและนำข้อมูลส่วนตัวของเจ้าของข้อมูลไม่ว่าจะเป็นลูกค้า พนักงานในองค์กร หรือบุคคลใดๆ ที่เกี่ยวข้องให้เป็นไปตามหลักปฏิบัติของพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (DataThoth.Ltd, 2565)

ผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลในกฎหมาย PDPA แบ่งออกเป็น 3 ประเภท ได้แก่

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (T-reg.co.Ltd, 2564)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right) สรุปได้ดังต่อไปนี้

1. สิทธิได้รับการแจ้งให้ทราบ การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล (ยกเว้นเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว เช่น ไปธนาคารเพื่อจะไปเปิดบัญชี หรือว่าการสมัครใช้ผลิตภัณฑ์หรือบริการต่างๆ) โดยมีรายละเอียดการแจ้งให้ทราบ เช่น เก็บข้อมูลส่วนบุคคลอะไรบ้าง, วัตถุประสงค์การเก็บข้อมูล, การนำไปใช้หรือส่งต่อไปมีให้ใครบ้าง, วิธีเก็บข้อมูลอย่างไร, เก็บข้อมูลนานแค่ไหน, วิธีขอการเปลี่ยนแปลง แก้ไขเพิกถอนข้อมูลส่วนบุคคลที่ให้ไปสามารถทำได้อย่างไรบ้าง (มาตรา 23)

2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิภายใน 30 วันนับจากวันที่ ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ (มาตรา 30)

3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ แต่ต้องไม่ขัดด้วยกฎหมายที่สำคัญยิ่งกว่า หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย หรือข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ (มาตรา 32)

4. สิทธิขอให้ลบหรือทำลาย กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะและผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของได้โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเอง (มาตรา 34)

5. สิทธิในการเพิกถอนความยินยอม ถ้าเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไปแล้ว ต่อมาภายหลังต้องการยกเลิกความยินยอมนั้น ก็สามารถทำเมื่อใดก็ได้ และการยกเลิกความยินยอมนั้นจะต้องทำได้ง่ายเหมือนกับตอนแรกที่เจ้าของข้อมูลให้ความยินยอมด้วย โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้ (มาตรา 19)

6. สิทธิขอให้ระงับการใช้ข้อมูล เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลไม่ว่าจะในกรณีที่เกิดการเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิก็สามารถทำได้ (มาตรา 34)

7. สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้องเป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย (มาตรา 35)

8. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกได้ทำจัดทำข้อมูลส่วนบุคคลของเราไปในอยู่ในรูปแบบต่างๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้ได้ หรือจะขอให้ส่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการและเทคนิค โดยการใช้สิทธินั้นต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น (มาตรา 31)

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ผู้ควบคุมข้อมูลส่วนบุคคล จะส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ต้องตรวจสอบว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้น มีมาตรฐานการคุ้มครองข้อมูล ส่วนบุคคลที่เพียงพอหรือไม่ ยกเว้นว่าจะเป็นไปเพื่อเป็นไปตามกฎหมาย, ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล, จำเป็นเพื่อปฏิบัติตามสัญญา, ป้องกันอันตรายที่จะเกิดต่อเจ้าของข้อมูลที่ไม่สามารถให้ยินยอมในขณะนั้นได้ หรือเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ (T-reg.co.Ltd, 2564)

ความรับผิดและบทลงโทษ

1. ความรับผิดทางแพ่ง ผู้กระทำละเมิดข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือ

ประมาทเลินเล่อหรือไม่ก็ตาม โดยศาลมีอำนาจสั่งให้ชดใช้ค่าสินไหมทดแทนเพิ่มเติมได้สองเท่าของค่าสินไหมทดแทนที่แท้จริง (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562)

2. โทษอาญา กำหนดบทลงโทษทางอาญาไว้สำหรับความผิดร้ายแรง เช่น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยมิชอบ, ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นแล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบต้องระวางโทษสูงสุดจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ หรือในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล กรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นอาจต้องร่วมรับผิดในความผิดอาญาที่เกิดขึ้น

3. โทษทางปกครอง กำหนดโทษปรับทางปกครองสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด มีโทษปรับทางปกครองสูงสุด 5,000,000 บาท เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ, ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล เป็นต้น (สุนทรีย์ ส่งเสริม, 2562)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์

ประเทศสิงคโปร์ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA เช่นเดียวกับของประเทศไทย ซึ่งประเทศสิงคโปร์ได้มีการประกาศใช้ตั้งแต่ปี 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี 2556 โดยมีระยะเวลาในการเตรียมความพร้อมด้วยกัน 18 เดือน โดยระหว่างนั้นได้มีการจัดอบรม เผยแพร่ ความรู้ เพื่อเตรียมความพร้อมให้กับภาคเอกชนและประชาชนอย่างต่อเนื่อง เพื่อสร้างความเข้าใจอันดีเกี่ยวกับข้อดีของ PDPA ที่จะมีผลบังคับใช้ภายในประเทศ นอกจากนี้ประเทศสิงคโปร์ยังมีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ หรือ PDPC มีบทบาทในเรื่องการให้คำปรึกษารวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุเอาไว้และยังจะเป็นการช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มรูปแบบ (Data Wow Co.Ltd, 2565)

พระราชบัญญัตินี้มีวัตถุประสงค์เพื่อควบคุมการรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กรในลักษณะที่คำนึงถึงสิทธิของบุคคลในการปกป้องข้อมูลส่วนบุคคลและความจำเป็นขององค์กรในการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ที่วิญญูชน (reasonable persons) พึงพิจารณาว่าเหมาะสม ไม่บังคับใช้กับบุคคลทั่วไปที่กระทำการไป

ตามความสามารถเฉพาะบุคคลนั้น ไม่ได้เป็นไปในนามขององค์กร รวมถึงลูกจ้างขององค์กร ตัวแทนขององค์กร และไม่บังคับใช้กับผู้ที่เสียชีวิตแล้ว ทั้งยังไม่บังคับใช้กับข้อมูลติดต่อเชิงธุรกิจเว้นแต่มีการระบุไว้อย่างชัดแจ้งในกฎหมายฉบับนี้

PDPA ประเทศสิงคโปร์ มีหลักความสำคัญต่างๆ ดังนี้

1. หลักความยินยอม (consent) กำหนดให้แต่ละองค์กรเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลได้ใน ในกรณีที่มีการให้ความยินยอมโดยเจ้าของข้อมูลก่อนดำเนินการใดๆ และเจ้าของข้อมูลสามารถปฏิเสธ หรือยกเลิกความยินยอมได้ ซึ่งองค์กรไม่อาจกำหนดให้การให้ความยินยอมเป็นเงื่อนไขในการขายสินค้าและบริการในระดับที่เกินกว่าความสมเหตุสมผลต่อการให้บริการนั้น (beyond what is reasonable) องค์กรไม่สามารถขอความยินยอมโดยปลอมแปลงข้อเท็จจริง ความยินยอมที่ได้มาด้วยวิธีการข้างต้นนั้นไม่ถือเป็นความยินยอมที่มีผลใช้ได้ตามกฎหมายฉบับนี้ความยินยอมนั้นอาจเป็นความยินยอมแบบโดยปริยายได้แต่ต้องอยู่ในขอบเขตของ (มาตรา 13,14)

2. หลักวัตถุประสงค์ (purpose) กำหนดให้เก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้ต่อเมื่อวัตถุประสงค์นั้นเหมาะสมกับสถานการณ์และเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ (PERSONAL DATA PROTECTION ACT, 2555 มาตรา 18)

3. การเข้าถึงและแก้ไขข้อมูล (access and correction) กำหนดสิทธิของบุคคลในการเข้าถึงข้อมูลและวิธีการที่ข้อมูลถูกใช้และเปิดเผยออกไปภายในหนึ่งปีตั้งแต่ถูกร้องขอ เว้นแต่การเข้าถึงนั้นจะเป็นอันตรายต่อตัวเจ้าของข้อมูลเองหรือกระทบสิทธิของผู้อื่น และมาตรา 22 กำหนดสิทธิของบุคคลในการร้องขอให้องค์กรแก้ไขข้อมูลของตนเองได้ เว้นแต่จะมีเหตุผลอันสมควร (มาตรา 21)

4. ความถูกต้องของข้อมูล (accuracy) กำหนดให้องค์กรมีหน้าที่จัดการให้ข้อมูลส่วนบุคคลที่เก็บรักษาไว้มีความถูกต้องครบถ้วนถ้าหากข้อมูลนั้นอาจถูกใช้โดยหน่วยงานที่จะตัดสินใจในประเด็นที่ส่งผลกระทบต่อตัวเจ้าของข้อมูลหรือผู้เกี่ยวข้อง หรือในกรณีที่อาจต้องเปิดเผยข้อมูลของบุคคลนั้นให้องค์กรอื่น (มาตรา 23)

5. การรักษาความปลอดภัยของข้อมูล (security) กำหนดให้องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครอง แต่ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษ จึงเป็นหน้าที่ขององค์กรเองที่ต้องจัดให้มีมาตรการในการรักษา

ความปลอดภัยที่เหมาะสมกับลักษณะและการใช้ข้อมูลนั้นๆ และให้ทำลายข้อมูลเมื่อหมดความจำเป็นตามวัตถุประสงค์แล้วและการเก็บข้อมูล (retention) นั้นไม่จำเป็นต่อวัตถุประสงค์เชิงกฎหมายหรือธุรกิจอื่นๆ อีก (มาตรา 24, 25)

6. การส่งข้อมูลไปต่างประเทศ (Transfer) ห้ามการส่งข้อมูลออกไปยังประเทศอื่นยกเว้นกรณีที่องค์กรผู้ดูแลข้อมูลลามารถพิสูจน์ได้ว่า ประเทศอื่นที่มีการส่งออกข้อมูลนั้นมีมาตรฐานด้านความปลอดภัยเทียบเท่าหรือสูงกว่ากฎหมายของสิงคโปร์ Commissioner อาจออกข้อยกเว้นให้กับบางองค์กรที่เห็นว่าเหมาะสมได้ (มาตรา 26)

7. การบังคับใช้และบทลงโทษ เป็นหน้าที่ของคณะกรรมการโดยที่คณะกรรมการมีอำนาจดังต่อไปนี้สั่งให้หยุดการเก็บ การใช้ การเปิดเผยข้อมูลส่วนบุคคลหากพบการกระทำที่ฝ่าฝืนต่อบทบัญญัติของกฎหมายทำลายข้อมูลส่วนบุคคลที่มีการเก็บไว้โดยฝ่าฝืนต่อกฎหมายการฝ่าฝืนกฎหมายอาจมีโทษถึง 100,000 SGD หรือต้องโทษจำคุก ไม่เกิน 12 เดือน หรือทั้งจำทั้งปรับ ทั้งนี้ ผู้อำนวยการและเจ้าหน้าที่ของหน่วยงานสามารถถูกฟ้องร้อง ความรับผิดชอบจากความผิดที่หน่วยงานเป็นผู้กระทำได้ด้วย (มาตรา 51) (Government of Singapore, 2012)

การถ่ายโอนข้อมูล

องค์กรอยู่ภายใต้ข้อผูกพันการจำกัดการโอน องค์กรต้องไม่ถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศหรือดินแดนนอกประเทศสิงคโปร์ ยกเว้นตามข้อกำหนดที่กำหนดภายใต้ PDPA เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ถ่ายโอนจะเป็นไปตามมาตรฐานการป้องกันที่เทียบได้กับภายใต้ PDP ในการดำเนินการดังกล่าวองค์กรต้องตรวจสอบให้แน่ใจโดยทั่วไปว่าผู้รับข้อมูลส่วนบุคคลดังกล่าวมีพันธะผูกพันตามภาระหน้าที่ที่บังคับใช้ได้ตามกฎหมายในการจัดหามาตรฐานการป้องกันให้กับข้อมูลส่วนบุคคลที่ถ่ายโอน นอกจากนี้ องค์กรที่มี 'ใบรับรองที่ระบุ' ซึ่งได้รับหรือรับรองภายใต้กฎหมายของประเทศหรือเขตแดนที่มีการถ่ายโอนข้อมูลส่วนบุคคลไปจะถือว่าผูกพันตามภาระผูกพันที่บังคับใช้ตามกฎหมายดังกล่าว ภายใต้ข้อบังคับการคุ้มครองข้อมูลส่วนบุคคล

“การรับรองที่ระบุ” หมายถึงการรับรองภายใต้ระบบกฎความเป็นส่วนตัวข้ามพรมแดนของความร่วมมือทางเศรษฐกิจในเอเชียแปซิฟิก ('APEC CBPR') และระบบการยอมรับความเป็นส่วนตัวของ APEC สำหรับผู้ประมวลผล ('PRP') ผู้รับจะต้องปฏิบัติตามข้อกำหนดภายใต้ข้อผูกพันการจำกัดการโอน (One Trust Data Guidance, 2566)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น

กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น หรือ Act on the Protection of Personal Information: APPI มีผลบังคับใช้กับผู้ประกอบการทั้งหมดที่เสนอขายสินค้าและบริการที่มีการดำเนินการกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่นซึ่ง APPI ของญี่ปุ่นนั้นประกาศใช้โดยทั่วไปในปี 2546 และ ประกาศใช้อย่างเต็มรูปแบบในปี 2548 อีกทั้งในปี 2562 ทาง EU ก็ได้ทำการรับรองมาตรฐานการคุ้มครองข้อมูลกับประเทศญี่ปุ่นอีกด้วย ทำให้สามารถถ่ายโอนข้อมูลส่วนตัวระหว่างสองเขตเศรษฐกิจได้อย่างอิสระบนพื้นฐานของการรับประกันความคุ้มครอง ข้อมูล ซึ่งการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลระหว่าง EU กับญี่ปุ่นก็จะช่วยให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นมีระดับสูงขึ้นและช่วยเพิ่มขีดความสามารถในการแข่งขันและการทำธุรกิจให้สามารถขยายเข้าไปยังฝั่ง EU ได้มาก (Data Wow Co.Ltd, 2565)

องค์ประกอบสำคัญของกฎหมาย คือ การจำกัดการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้รับตามที่เจ้าของข้อมูลได้รับทราบ เพื่อปกป้องข้อมูลที่ละเอียดอ่อนและจำกัดการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล โดยมีผู้ควบคุมข้อมูลหรือ PIC (Data Controller) ที่ใช้ข้อมูลส่วนบุคคลเฉพาะในขอบเขตที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ของการใช้งานที่ระบุไว้ในหลักและเพื่อพยายามลบข้อมูลส่วนบุคคลเมื่อไม่ต้องการใช้เพื่อวัตถุประสงค์ในการใช้งานอีกต่อไป หรือดำเนินการตามสมควรเพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องและเป็นปัจจุบันเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ในการใช้งานเพื่อใช้มาตรการรักษาความปลอดภัยที่จำเป็นทั้งหมดเพื่อหลีกเลี่ยงการสูญหายหรือการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตและไม่ใช้ข้อมูลส่วนบุคคลในลักษณะที่อาจอำนวยความสะดวกหรือกระตุ้นให้เกิดการกระทำที่ผิดกฎหมายหรือไม่เหมาะสม

การถ่ายโอนข้อมูล

การถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม รวมถึงหน่วยงานในเครือของ PIC โดยไม่ได้รับความยินยอมล่วงหน้าจากตัวการนั้นเป็นสิ่งต้องห้าม เว้นแต่ได้รับอนุญาตตามกฎหมาย หรือการถ่ายโอนตามกฎการยกเลิกจะไม่สามารถใช้ได้สำหรับข้อมูลส่วนบุคคลที่ได้รับด้วยวิธีการฉ้อฉลหรือวิธีอื่นที่ผิดกฎหมายหรือจากผู้โอนรายก่อนหน้าตามกฎการยกเลิก (One Trust Data Guidance, 2023)

ต่อมาเนื่องมาจากการที่มีจำนวนอาชญากรรมทางไซเบอร์และคดีเหตุการละเมิดข้อมูลส่วนบุคคลเพิ่มมากขึ้น ประเทศญี่ปุ่นจึงได้ตรากฎหมาย APPI ฉบับแก้ไขในปี พ.ศ.2563 ที่มีความเข้มงวดมากขึ้นและมีขอบเขตที่กว้างขึ้น เช่น กำหนดกฎเกณฑ์เกี่ยวกับการส่งข้อมูลที่ครอบคลุมมากขึ้น เป็นต้น โดยเฉพาะการส่งข้อมูลไปต่างประเทศและการดำเนินการกรณีมีการละเมิดเกิดขึ้น ทั้งนี้ กฎหมายฉบับดังกล่าวกำหนดให้เริ่มมีผลบังคับใช้ทั้งฉบับเมื่อวันที่ 1 เมษายน พ.ศ.2565 ที่ผ่านมา โดยประเด็นสำคัญที่มีการเปลี่ยนแปลงในกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขในประเด็นที่สำคัญ มีดังนี้

1. การแจ้งการละเมิดข้อมูลส่วนบุคคล ผู้ประกอบการมีหน้าที่แจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Commission – PIPC) และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการละเมิดข้อมูลใดๆ ซึ่งมีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหว การละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์

2. ข้อกำหนดเกี่ยวกับการให้ข้อมูลกับบุคคลที่สามก่อนหน้านี้ เจ้าของข้อมูลต้องได้รับการแจ้งเกี่ยวกับข้อกำหนดการให้ข้อมูลกับบุคคลที่สาม แต่สำหรับกฎหมายใหม่ผู้ประกอบการต้องยืนยันว่าบุคคลที่สามผู้รับข้อมูลได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนที่จะให้ข้อมูลไปโดยต้องมีการระบุรายละเอียดเกี่ยวข้อมูลที่จะมีการให้และต้องเก็บหลักฐานไว้เป็นเวลา 3 ปี

3. การส่งต่อข้อมูลไปยังต่างประเทศ ก่อนที่จะมีการส่งต่อข้อมูลไปยังบุคคลที่สามซึ่งไม่ได้อยู่ในญี่ปุ่นนั้น ต้องมีการแจ้งให้เจ้าของข้อมูลทราบโดยต้องมีการแจ้งข้อมูลทั้งในส่วนของชื่อของประเทศปลายทาง ระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางและมาตรการคุ้มครองข้อมูลที่ผู้นำเข้าข้อมูลใช้ นอกจากนี้ผู้ประกอบการที่จะส่งออกข้อมูลจะต้องดำเนินการตรวจสอบยืนยันสถานะของข้อมูลส่วนบุคคลและระบบที่ใช้ในการดำเนินการกับข้อมูลของผู้นำเข้าข้อมูลการประเมินมาตรการบรรเทาผลกระทบกรณีมีปัญหาใดๆ เกิดขึ้น รวมไปถึงการประเมินมาตรการที่จะใช้เพื่อให้มั่นใจว่าจะมีการดำเนินการกับข้อมูลอย่างเหมาะสม

4. บทกำหนดโทษ มีการปรับแก้ไขเพิ่มเติมโทษให้รุนแรงมากขึ้นไม่น้อย เช่น กรณีฝ่าฝืนคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดโทษบุคคลผู้กระทำผิดจากเดิมโทษจำคุกสูงสุดไม่เกิน 6 เดือน หรือโทษปรับสูงสุดไม่เกินสามล้านเยนเป็นโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือโทษปรับสูงสุดไม่เกินหนึ่งล้านเยนและกำหนดโทษสำหรับนิติบุคคลจาก

เดิมโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ประมาณยี่สิบเจ็ดล้านห้าแสนบาทไทย) หรือ ในกรณีที่มีการส่งข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ก็มีการเปลี่ยนโทษปรับในส่วนของนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินห้าล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ณิชนันท์ คุปตานนท์, 2565)

ประเทศญี่ปุ่นนั้นมีค่านิยมหลักที่แข็งแกร่งในการคุ้มครองสิทธิ์ของบุคคลและหลักการพื้นฐานของกฎหมายคุ้มครองข้อมูลของประเทศญี่ปุ่นคือการคุ้มครองสิทธิ์ในความเป็นส่วนตัว แต่ยังตระหนักถึงขอบเขต ลักษณะ และปริมาณของข้อมูลส่วนบุคคลที่เพิ่มขึ้น การขยายการใช้ข้อมูลส่วนบุคคลในรูปแบบต่างๆ ของธุรกิจ และยังให้ความสำคัญกับการถ่ายโอนข้อมูลข้ามพรมแดนที่ราบรื่นรวมถึงข้อมูลส่วนบุคคล เนื่องจากการเติบโตของกระแสข้อมูลในขณะที่สังคมดิจิทัลดำเนินไปโดยเฉพาะอย่างยิ่งโลกาภิวัตน์ของกิจกรรมทางเศรษฐกิจและสังคมตลอดจนความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร

สรุป

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของประเทศไทยนั้น ให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลที่ทำให้สามารถระบุตัวตนของบุคคลนั้นๆ ได้ทั้งทางตรงและทางอ้อม รวมไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้ปลอดภัยอยู่เสมอและคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ เจ้าของข้อมูลสามารถขอเข้าถึงข้อมูลส่วนบุคคล แก้ไขข้อมูลให้เป็นปัจจุบัน และถอนความยินยอมได้ตลอดเวลา ทั้งยังมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คอยให้คำแนะนำ ตรวจสอบ และประสานงานกับองค์กรเป็นหลัก

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ APPI ของประเทศญี่ปุ่น มีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้ ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครอง โดยเจ้าของข้อมูลมีสิทธิในการตรวจสอบการแก้ไขข้อมูล การไม่ยินยอมให้ประมวลผล เป็นต้น และมีการคุ้มครองข้อมูลละเอียดอ่อน (sensitive data) ซึ่งเป็นข้อมูลได้รับการคุ้มครองพิเศษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของประเทศสิงคโปร์ เป็นการบังคับใช้เฉพาะภาคเอกชนเท่านั้น การขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะเป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต การความคุ้มครองข้อมูลส่วนบุคคลจะต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อ

วัตถุประสงค์ที่ชอบด้วยกฎหมาย ให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ (Data Wow Co.Ltd, 2565)

เห็นได้ว่าทั้งสองประเทศที่ยกตัวอย่างขึ้นมาเปรียบเทียบกับประเทศไทย ไม่ได้มีความแตกต่างกันมากนัก เจตนารมย์ที่สำคัญของการออกกฎหมายนี้เป็นไปเพื่อคุ้มครองข้อมูลส่วนบุคคล ป้องกันการนำไปใช้โดยมิถูกต้อง เป็นการละเมิดสิทธิส่วนบุคคลของประชากรในประเทศนั้นๆ และยกระดับให้เป็นมาตรฐานสากลในการติดต่อการค้าหรือการทำธุรกิจต่างๆ ซึ่งต้องอาศัยข้อมูลเหล่านี้ในการติดต่อสื่อสาร หรือทำกิจกรรมต่างๆ ดังนั้นทุกประเทศไม่ว่าจะเป็นโซนเอเชียหรือแถบทวีปยุโรปได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการจัดเก็บข้อมูลส่วนบุคคลแทบทั้งหมดล้วนจัดเก็บอยู่ในรูปแบบดิจิทัลทำให้สามารถโอนถ่ายข้อมูลส่วนบุคคลนั้นๆ ได้ง่ายและรวดเร็ว และยังเป็นประโยชน์ต่อการวิเคราะห์ วิจัย ทำสถิติ และอีกหลากหลายกิจกรรม แต่ในขณะเดียวกันการรั่วไหลของข้อมูลส่วนบุคคลเข้าสู่มือของมิจฉาชีพหรือธุรกิจที่แอบแฝงผลประโยชน์ต่างๆ ได้ง่ายมากขึ้น จึงมีความจำเป็นในการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น ดังนั้นแล้วข้อดีของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ในประเทศไทยนั้นคือการที่จะช่วยปกป้องข้อมูลของเจ้าของข้อมูลให้มีความปลอดภัยไม่ทำให้ข้อมูลหลุดออกไปโดยไม่ได้รับอนุญาต โดยมีหลักสำคัญอยู่ที่การลดความเสี่ยงจากการถูกละเมิดข้อมูลส่วนบุคคล นอกจากนี้เจ้าของข้อมูลยังมีสิทธิ์ในการรับทราบวัตถุประสงค์ในการให้ข้อมูลจากองค์กร หรือจากหน่วยงานก่อนตัดสินใจให้ข้อมูล รวมไปถึงร้องขอเข้าถึงและขอรับข้อมูลส่วนบุคคลของตนเองจากทางผู้เก็บข้อมูลหรือขอยกเลิกความยินยอมในการเก็บข้อมูล หรือขอยกเลิกการเผยแพร่ข้อมูลส่วนบุคคลของตัวเองได้ทุกเมื่อ ทั้งยังช่วยเพิ่มขีดจำกัดในการทำธุรกิจระหว่างภาคเอกชนด้วยกันเอง รวมถึงภาคประชาชนจะได้เกิดความมั่นใจในการให้ข้อมูลส่วนบุคคลเพื่อนำไปใช้งาน เป็นต้น อีกทั้งช่วยให้ประชานชนมั่นใจและเชื่อมั่นว่าข้อมูลส่วนบุคคลที่ให้ไปจะปลอดภัย แต่ทั้งนี้เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลยังมีความใหม่ มีความจำเป็นที่ภาครัฐจะต้องจัดให้มีการอบรม เผยแพร่ความรู้เกี่ยวกับกฎหมายดังกล่าวให้ประชาชนทั้งภาครัฐและเอกชนมีความเข้าใจในการบังคับใช้ เพื่อให้สอดคล้องเป็นไปตามเจตนารมณ์ของกฎหมาย รวมถึงให้แต่ละหน่วยงานจัดตั้งระบบหรือผู้รับผิดชอบในการปฏิบัติการให้ไปเป็นตามกฎหมายดังกล่าว เพื่อให้มีประสิทธิภาพในการบังคับใช้ และสร้างมาตรฐานให้เทียบเท่าระดับสากล เป็นที่ยอมรับของนานาประเทศ จะยิ่งเพิ่มโอกาสทางการค้า การทำธุรกิจข้ามพรมแดนได้อย่างอิสระและปลอดภัยมากยิ่งขึ้นด้วย

เอกสารอ้างอิง

ณิชนันท์ คุปตานนท์. (2565). กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น. เข้าถึงได้จาก https://www.bangkokbiznews.com/columnist/999304

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. (2562). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. เข้าถึงได้จาก ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์: https://ictlawcenter.etda.or.th/laws/detail/DP-Act-2562

สุนทรีย์ ส่งเสริม. (2562). สรุปสาระสำคัญ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 “PDPA – Privacy for All” . เข้าถึงได้จาก https://laplaehospital.moph.go.th/file/10-11-2020-01-30-07.pdf

Data Wow Co.Ltd. (2565). เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร. เข้าถึงได้จาก https://pdpacore.com/th/blogs/get-to-know-the-difference-between - PDPA-of-3-countries-in-asia

DataThoth.Ltd. (2565). PDPA PRO สรุป PDPA พร้อมแนะนำแนวทาง. เข้าถึงได้จาก https://pdpa.pro/blogs/in-summary-what-is-pdpa

Government of Singapore. (2012). Personal Data Protection Commission SingaPore. Retrieved from https://www-pdpc-gov-sg.translate.goog/Overview-of-PDPA/The Legislation?_x_tr_sl=en&_ x_tr_tl=th&_x_tr_hl=th&_x_tr_pto=sc

IT Information Technology. (2565). 10 เรื่องต้องรู้ ‘กฎหมาย PDPA’ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลก่อนบังคับใช้ 1 มิ.ย.นี้. เข้าถึงได้จาก http://med.swu.ac.th/it/?p=1953

One Trust Data Guidance. (2023). Japan-Data Protection Overview. Retrieved from https://www-dataguidan cecom.translate.goog/notes/japan-data-protection-overview?_x_tr_sl=en&_ x_tr_ tl=th&_ x_tr_hl=th&_x_tr_pto=sc

One Trust Data Guidance. (2566). Singaproe-Data Protection Overview. Retrieved from https://wwwdatagui dancecom. translate. goog /notes/singapore-

data-protection-overview?_x_tr_sl=en&_
x_tr_tl=th&_x_tr_hl=th&_x_tr_pto=sc

T-reg.co.Ltd. (24 พฤษภาคม 2564). PDPA คืออะไร เกี่ยวข้องกับทุกคนอย่างไร. เข้าถึงได้จาก https://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/