บทที่ 3

กฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ของกฎหมายไทยและกฎหมายต่างประเทศ

ในส่วนของบทที่ 3 นี้ จะเป็นการกล่าวถึงกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลทั้งในกฎหมายไทย และกฎหมายต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา โดยแต่ละประเทศมีมาตรการที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแตกต่างกันออกไป ไม่ว่าจะเป็นแนวทางปฏิบัติ หลักเกณฑ์ หรือบทลงโทษต่างๆ โดยรายละเอียดของกฎหมายแต่ละประเทศมีดังต่อไปนี้

3.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของไทยนั้น ได้บัญญัติไว้หลายฉบับ ซึ่งแต่ละฉบับนั้นมีรายละเอียดที่แตกต่างกันออกไป จึงขออธิบายเกี่ยวกับกฎหมายฉบับต่างๆ ดังต่อไปนี้

3.1.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 24 พฤษภาคม 2562 และกฎหมายฉบับดังกล่าวมีผลบังคับใช้อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา และกฎหมายฉบับนี้จะมีผลกระทบทั้งต่อภาคประชาชน หน่วยงานรัฐ และหน่วยงานเอกชน เนื่องจากปัจจุบันมีการล่วงละเมิด สิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว แม้จะมีกฎหมายฉบับนี้ออกมาควบคุมในการรวบรวมและเก็บข้อมูลส่วนบุคคลแล้ว แต่ยังมีประเด็นที่น่าคิดว่าในทางปฏิบัติหรือการบังคับใช้กฎหมายฉบับนี้ เช่น ประเด็นเรื่องการเก็บข้อมูลส่วนบุคคล ซึ่งในส่วนของกฎหมายจะมีข้อมูลที่จำเป็นหรือบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บได้ หรือเป็นกรณี

การให้ความยินยอม (Consent) ของผู้เป็นเจ้าของข้อมูลส่วนบุคคลที่จะยินยอมให้เก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่[1]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถือเป็นกฎหมายกลางที่กำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ สร้างความเป็นไปตามมาตรฐานสากล และมีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดอย่างเหมาะสม เป็นหลักการพื้นฐานที่เกี่ยวกับข้อมูลส่วนบุคคล ซึ่งพยายามให้มีความสอดคล้องกับหลักมาตรฐานสากลตามที่สหภาพยุโรปได้มีการออกกฎระเบียบGeneral Data Protection Regulation (GDPR) เพื่อคุ้มครองประชาชนมิให้ถูกล่วงละเมิดในความเป็นส่วนตัว และนำข้อมูลส่วนบุคคลของประชาชนไปแสวงหาผลประโยชน์ หรือเปิดเผยโดยไม่ได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูลก่อน[2]

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้บัญญัติหลักการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ในมาตรา 37 ดังนี้

มาตรา 37[3] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้” มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด”

---

[1] ทัชชภร มหาแถลง. (2563). การคุ้มครองชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ***, 11(2). หน้า 80-97.

[2] อมรรัตน์ อริยะชัยประดิษฐ์. (2565). การศึกษาเปรียบเทียบโทษทางอาญากับโทษทางปกครองตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารมนุษยศาสตร์ และสังคมศาสตร์ มหาวิทยาลัย มหาสารคาม,*** 41(4). หน้า 129-141.

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

ความหมายของการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งออกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 [4]ได้กำหนดนิยามของคำว่า "การละเมิดข้อมูลส่วนบุคคล" ให้มีความหมายดังต่อไปนี้[5]

"การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด"[6]

เหตุการณ์ที่อาจถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

1) การที่บุคคลที่สามเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ

2) การกระทำ หรือการไม่กระทำการ โดยเจตนาหรือไม่เจตนา ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลข้อมูลส่วนบุคคล

3) การส่งข้อมูลส่วนบุคคลไปยังผู้รับผิดคน

4) การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

5) การสูญเสียความสามารถในการใช้ข้อมูลส่วนบุคคล (Ransomware)

6) เกิดการเจาะระบบ (Hack) ที่บริษัทใช้งาน

หน้าที่แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)[7] กำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่บุคคลตามกรณี ดังต่อไปนี้

1) ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า หรือเท่าที่สามารถกระทำได้ ภายใน 72 ชั่วโมง นับแต่ทราบเหตุแห่งการละเมิดข้อมูล

---

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562. มาตรา 37.

[5] แคทรียา มาลาศรี. (2566). ***สรุปข้อมูลสำคัญที่ Data Controller ต้องรู้ ประกาศใหม่จาก PDPC หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ 2565***. (ออนไลน์). เข้าถึงได้จาก: https://t-reg.co/blog/news/guideline-for-data-breach-report-pdpa-law/. [2566,30 มิถุนายน]

[6] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37(4).

2) แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางเยียวยาโดยไม่ชักช้า[8]

ตารางที่ 1 ตารางระดับของเหตุละเมิดข้อมูลส่วนบุคคล

ระดับของเหตุละเมิดข้อมูลส่วนบุคคล	เงื่อนไข	
	แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ไม่เกิน 72 ชั่วโมงนับแต่ทราบการละเมิดข้อมูลส่วนบุคคล	**แจ้งเจ้าของข้อมูลส่วนบุคคลถึงการบริการจัดการการละเมิดข้อมูลส่วนบุคคล พร้อมกับการแจ้งแนวทางการเยียวยา**
การละเมิดข้อมูลส่วนบุคคลที่อาจมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✘
การละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✓

โดยสำนักงาน สคส. ได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565[9] ซึ่งประกาศฯ

---

[8] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[9] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/

ดังกล่าวเป็นกฎหมายลำดับรองที่ออกตามความในมาตรา 37(4) ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในข้อ 4 ของประกาศดังกล่าว ได้กำหนดไว้ว่า “เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วยเหตุที่เกิดจากเหตุดังต่อไปนี้[10]

1) การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ

2) การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3) ภัยคุกคามทางไซเบอร์

4) ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น

โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

---

default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[10] ชวิน อุ่นภัทร, ปิยะบุตร บุญอร่ามเรือง. (2564). ***แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.*** รายงานการวิจัย. กรุงเทพฯ: ศูนย์วิจัยกฎหมายและการพัฒนาคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทาลายข้อมูลส่วนบุคคล ทาให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ขั้นตอนในการดำเนินงานเมื่อพบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล[11]

ควรพิจารณากำหนดแนวทางหรือวิธีการในการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ชัดเจน ทั้งนี้ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเองว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยพิจารณา

1) มาตรการเชิงองค์กร (organizational measures)

2) มาตรการเชิงเทคนิค (technical measures) และ

3) มาตรการทางกายภาพ (physical measures)

ในส่วนที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล มีรายละเอียดดังต่อไปนี้[12]

1) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการ

---

[11] สมาคมประกันวินาศภัยไทย. (2566). ***แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.*** กรุงเทพฯ: สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. หน้า 154-170.

[12] เรื่องเดียวกัน, หน้า 154-170.

ป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

2) เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

3) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

4) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

อย่างไรก็ตาม หากการละเมิดข้อมูลส่วนบุคคลไม่ก่อให้เกิดความเสี่ยง หรือไม่มีความเสี่ยง ก็ไม่จำเป็นต้องแจ้งทั้งสำนักงาน และเจ้าของข้อมูลส่วนบุคคล แต่ทั้งนี้ ในทางปฏิบัติอาจเป็นการยากที่ผลของการพิจารณาความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลนั้นเป็นกรณีที่ไม่ก่อให้เกิดผลกระทบใดต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

การประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล

ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้[13]

1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

2) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

---

[13] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

3) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

4) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจากัดต่างๆ ด้วยหรือไม่ เพียงใด

5) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

6) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล

7) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

8) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคลรวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

วิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้[14]

[14] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

1) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคล หรือลักษณะและจำนวนรายการของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

4) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากรกระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคาสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน[15]

กรณีแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าเกิน 72 ชั่วโมง

ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่า 72 ชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยเร็ว ทั้งนี้ ต้องไม่เกิน 15 วันนับแต่ทราบเหตุ

---

[15] ปัทมา มัญชุนากร. (2564). ***ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษา กรณีผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ทั้งนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกำหนดเวลาในมาตรา 37 (4)[16] ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อนึ่ง การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่น ๆ ที่เกี่ยวข้อง นั้น ไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

ข้อยกเว้นการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อประกอบการพิจารณาได้ หากผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าเหตุการละเมิดข้อมูลส่วนบุคคลนั้น

1) ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

2) ข้อมูลส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

3) ข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ

4) เหตุอื่นใดที่เชื่อถือได้

ในการยกข้อยกเว้นดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ให้ข้อมูลหรือส่งเอกสารหรือหลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่น ๆ ที่เกี่ยวข้อง พิจารณาด้วย

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล

[16] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37(4).

ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำได้โดยไม่ชักช้า[17]

1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน

3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดข้อมูลส่วนบุคคล

4) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหา

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

ทั้งนี้ การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

การลงโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่[18]

มาตรา 79[19] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทาให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

---

[17] ชวิน อุ่นภัทร, ปิยะบุตร บุญอร่ามเรือง. อ้างแล้วเชิงอรรถที่ 10. หน้า 1.

[18] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

[19] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 79.

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาทหรือทั้งจำทั้งปรับ

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ ”

มาตรา 80 บัญญัติว่า “ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นามาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

1) การเปิดเผยตามหน้าที่

2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ”

มาตรา 81[20] บัญญัติว่า “ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือกระทำการของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และละเว้นไม่สั่งการหรือกระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย ”

การลงโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่[21]

มาตรา 82[22] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 23 มาตรา 30 วรรคสี่ มาตรา 39 วรรคหนึ่ง มาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 19 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรคหก หรือไม่ปฏิบัติตาม

---

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

[21] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

[22] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 82.

มาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 83[23] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสามต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท”

มาตรา 84[24] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสามหรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท”

มาตรา 85[25] บัญญัติว่า “ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 86[26] บัญญัติว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท”

มาตรา 87[27] บัญญัติว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 วรรคหนึ่งหรือวรรคสาม โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท”

มาตรา 88[28] บัญญัติว่า “ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 39 วรรคหนึ่ง ซึ่งได้นามาใช้บังคับโดยอนุโลมตามมาตรา

---

[23] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 83.

[24] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 84.

[25] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 85.

[26] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 86.

[27] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 87.

[28] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 88.

39 วรรคสองและมาตรา 41 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 41 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 89[29] บัญญัติว่า “ผู้ใดไม่ปฏิบัติตามคาสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 75 หรือไม่ปฏิบัติตามมาตรา 76 (1) หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 76 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท”

มาตรา 90[30] บัญญัติว่า “คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองตามที่กำหนดไว้ในส่วนนี้ ทั้งนี้ ในกรณีที่เห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้

ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือพฤติการณ์ต่าง ๆ ประกอบด้วย ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการกำหนด

ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคาสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ให้คณะกรรมการผู้เชี่ยวชาญมีอานาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

คำสั่งลงโทษปรับทางปกครองและคำสั่งในการบังคับทางปกครอง ให้นำความในมาตรา 74 วรรคหก มาใช้บังคับโดยอนุโลม และให้นำความในมาตรา 74 วรรคสี่ มาใช้บังคับกับการบังคับทางปกครองตามวรรคสามโดยอนุโลม”

1) ผู้ควบคุมข้อมูลส่วนบุคคล

เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่แจ้งให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวมข้อมูลตามมาตรา 23 หรือไม่ดำเนินการตามคำขอเข้าถึงและคำขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าของข้อมูลภายใน 30 วัน ตามมาตรา 30 วรรคสี่ หรือไม่บันทึกรายการเพื่อให้เจ้าของข้อมูลตรวจสอบได้ ตามมาตรา 38 หรือไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา40 วรรคหนึ่ง หรือไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา

---

[29] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 89.

[30] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 86.

41 วรรคสอง หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงาน หรือเลิกสัญญาจ้างเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ตามมาตรา 41 วรรคสาม หรือไม่ขอความยินยอมตามแบบที่กำหนด ตามมาตรา 19 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอม ตามมาตรา 19 วรรคห้า หรือไม่ปฏิบัติตามมาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 80[31])

เก็บรวบรวม ใช้ เปิดเผยข้อมูล ไม่เป็นไปตามวัตถุประสงค์ที่แจ้งไว้ต่อเจ้าของข้อมูลตามมาตรา 21 เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมายตามมาตรา 22 หรือไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 24 ไม่เก็บข้อมูลจากเจ้าของข้อมูลโดยตรงตามมาตรา 25 วรรคหนึ่ง ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 27 วรรคหนึ่ง บุคคลหรือนิติบุคคลที่ได้รับข้อมูลจากการเปิดเผยของผู้ควบคุมข้อมูลใช้ หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 27 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังต่างประเทศไม่เป็นไปตามหลักเกณฑ์การให้ความคุ้มครองตามที่คณะกรรมการประกาศกำหนดตามมาตรา 28 ผู้ควบคุมข้อมูลส่วนบุคคลยังดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลได้แจ้ง การคัดค้านให้ทราบแล้ว ตามมาตรา 32 วรรคสอง หรือไม่ดำเนินการตามหน้าที่ที่กำหนดไว้ตามมาตรา 36 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท (มาตรา 81[32])

ฝ่าฝืนเก็บรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิตามมาตรา 26 หรือฝ่าฝืนใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 27 วรรคหนึ่ง บุคคล หรือนิติบุคคลที่ได้รับข้อมูลจากการเปิดเผยของผู้ควบคุมข้อมูล ใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 27 วรรคสองหรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท (มาตรา 82)

2) ผู้ประมวลผลข้อมูลส่วนบุคคล

---

[31] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 80.

[32] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 40 วรรคหนึ่ง หรือไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 วรรคสอง หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาจ้างเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ตามาตรา 41 วรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 83)[33]

ไม่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อปูองกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจและจัดทำาเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ตามมาตรา 39 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรค หนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 36 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 37 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท (มาตรา 84[34])

ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท (มาตรา 85)

3) ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล หรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคล

ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 40 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 40 วรรคสี่ ต้องโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 86)

จะเห็นว่าแนวคิดการลงโทษทางอาญากับการลงโทษทางปกครองมีความแตกต่างกัน กล่าวคือ การลงโทษทางอาญาแก่ผู้กระทำาความผิดเป็นสิ่งที่ผู้มีอำานาจในรัฐต้องกระทำาเพื่อรักษาความสงบเรียบร้อยของรัฐเพื่อมิให้มีการล่วงละเมิดสิทธิของผู้อื่นตามกฎหมาย ซึ่งการจะลงโทษทางอาญาเมื่อมีกฎหมายบัญญัติว่าการกระทำาเป็นความผิดและมีบทลงโทษตามกฎหมายซึ่งตามพระราชบัญญัตินี้กำหนดเพียงโทษจำคุกและปรับ นอกจากนี้ การบังคับใช้กฎหมายอาญาใช้บังคับแก่ทุกคนภายในรัฐอย่างเสมอภาค โทษจะรุนแรงมากหรือน้อยขึ้นอยู่กับการกระทำาความผิดในขณะที่การลงโทษทางปกครองมีขอบเขตจำกัดอยู่เฉพาะบุคคลที่ก่อตั้งนิติสัมพันธ์กับฝ่ายปกครอง การจำกัดสิทธิและเสรีภาพหรือการแทรกแซงสิทธิและเสรีภาพของประชาชน โดยรัฐเกิดขึ้นเมื่อบุคคลที่รัฐเข้าไปแทรกแซงหรือจำกัดสิทธิและเสรีภาพนั้น เป็นบุคคลที่ได้รับการคุ้มครองตามกฎหมาย ซึ่งอาจเป็นกรณีเฉพาะรายหรือในลักษณะทั่วไปตามกฎหมาย ซึ่งในการลงโทษทาง

---

[33] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 15. หน้า 1.

[34] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 84.

ปกครองตามพระราชบัญญัตินี้จะเป็นการปรับด้วยจำนวนเงิน โดยประเทศไทยไม่ได้มีการแบ่งแยกแนวคิดโทษปรับทางปกครองและมาตรการบังคับทางปกครองออกจากกันอย่างชัดเจน กล่าวคือ หากเป็นการปรับในเชิงลงโทษทางปกครองจะเป็นการลงโทษบุคคลด้วยการชำระเงินตามที่เจ้าหน้าที่กำหนดเพื่อลงโทษพฤติกรรมผู้กระทำผิดในอดีต แต่หากเป็นการปรับตามมาตรการบังคับทางปกครองจะกำหนดให้บุคคลที่ฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งทางปกครองชำระเงินจนกว่าจะมีการปฏิบัติตามคำสั่งเพื่อบังคับพฤติกรรมของบุคคลที่จะก่อขึ้นต่อไปในอนาคต บทกำหนดโทษทางปกครองตามกฎหมายนี้จึงเป็นการปรับในเชิงลงโทษทางปกครองและมาตรการบังคับทางปกครอง เพื่อบังคับพฤติกรรมของบุคคลขณะเดียวกัน ซึ่งอาจทำให้เกิดความสับสนได้ นอกจากนี้ในการบังคับโทษปรับทางปกครองจะคำนึงถึงเรื่องประโยชน์สาธารณะ จึงไม่อาจอ้างหลักความเสมอภาคในการใช้กฎเกณฑ์เพื่อมาคุ้มครองปัจเจกชนนั้น

โทษที่เกี่ยวข้อง

หากไม่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด อาจถูกโทษปรับทางปกครองไม่เกิน 3 ล้านบาท ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 83[35] ทั้งนี้ ในกรณีที่บริษัทไม่เห็นด้วยกับการลงโทษทางปกครองข้างต้น บริษัทสามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาความของศาลปกครอง

ข้อเสนอแนะ

องค์กรต่าง ๆ ควรจัดทำบันทึกเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุฯ และข้อยกเว้นกรณีที่ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ใช้อ้างอิงไว้ ไม่ว่าองค์กรจะได้รับยกเว้นให้ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลด้วยหรือไม่ก็ตาม เพื่อเป็นหลักฐาน ในกรณีมีข้อพิพาท

โทษทางอาญาของกรรมการหรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล[36]

ในกรณีที่บริษัทกระทำความผิดที่มีโทษทางอาญาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล[37] นอกจากโทษทางอาญาที่บริษัทอาจจะต้องรับแล้ว กรรมการ หรือผู้จัดการ หรือบุคคลซึ่ง

---

[35] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 83.

[36] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

[37] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 79 และ 80.

รับผิดชอบในการดำเนินงานของบริษัทก็ต้องรับผิดในโทษอาญาเช่นเดียวกับบริษัทด้วย หากพิสูจน์ว่า การกระทำผิดดังกล่าวมีองค์ประกอบ ดังต่อไปนี้ ได้[38]

ผู้กระทำความผิด

ก) กรรมการของบริษัท

ข) ผู้จัดการของบริษัท หรือ

ค) บุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทการกระทำความผิด

ก) การสั่งการ หรือการกระทำการของกรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท หรือ

ข) การละเว้นไม่สั่งการ หรือไม่กระทำการ ในกรณีที่กรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทมีหน้าที่ต้องสั่งการหรือกระทำการ

และการกระทำตาม ก. หรือ ข. นั้นเป็นเหตุให้บริษัทกระทำความผิด

ตัวอย่าง

ผู้รับมอบอำนาจบริษัทสั่งให้นำข้อมูลส่วนบุคคลที่บริษัท เก็บรวบรวมมาภายใต้วัตถุประสงค์ในการพิจารณารับประกันภัยรถยนต์ ไปใช้ประมวลผลข้อมูลภายใต้วัตถุประสงค์เพื่อทำกิจกรรมส่งเสริมการขาย โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่นนี้เป็นกรณีที่บริษัท ผู้ควบคุมข้อมูลส่วนบุคคลกระทำความผิดโดยคำสั่งของบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท ดังนั้น ในกรณีนี้ทั้งบริษัท และผู้รับมอบอำนาจบริษัทจะต้องรับโทษทางอาญาที่เกี่ยวข้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

โทษทางปกครอง

นอกจากโทษทางปกครองที่กำหนดไว้สำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือตัวแทนของบุคคลดังกล่าว ตามที่ได้อธิบายไว้ที่ข้างต้นแล้ว บุคคลใด ๆ (ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงกรรมการ หรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท) ที่ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือเจ้าพนักงานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อาจต้องรับผิดหากบุคคลดังกล่าวกระทำการดังต่อไปนี้[39]

---

[38] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

[39] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%

1) ไม่ปฏิบัติตามคำสั่งให้ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมทั้งไม่มาชี้แจงข้อเท็จจริงต่อคณะกรรมการผู้เชี่ยวชาญ

2) ไม่มาให้ข้อมูล หรือไม่ส่งเอกสารหรือหลักฐาน เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่พนักงานเจ้าหน้าที่ตามหนังสือที่ได้แจ้งไปภายใต้อำนาจหน้าที่

3) ไม่อำนวยความสะดวกตามสมควรแก่พนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่

ตัวอย่าง

1) ในกรณีที่พนักงานเจ้าหน้าที่ได้รับคำสั่งจากศาลที่มีเขตอำนาจ เพื่อเข้าตรวจสอบและรวบรวมข้อเท็จจริง โดยยึด หรืออายัดหลักฐานที่พนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่าใช้เพื่อกระทำความผิด เช่นนี้ หากผู้จัดการสาขา ขัดขวางไม่ให้เจ้าพนักงานยึดเอาหลักฐานนั้นไป ผู้จัดการสาขาคนดังกล่าวอาจจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

2) ในกรณีที่คณะกรรมการผู้เชี่ยวชาญสั่งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของบริษัทไปให้รายละเอียดเรื่องที่มีผู้ร้องเรียนบริษัท เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แต่ DPO ไม่ไปให้ข้อเท็จจริงโดยไม่มีเหตุผล ดังนี้ DPO อาจจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

ข้อสังเกต

1) พนักงานเจ้าหน้าที่ จะเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลได้จะต้องเป็นไปตามเงื่อนไขที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด กล่าวคือ

2) ต้องมีคำสั่งอนุญาตของศาลที่มีเขตอำนาจ

3) เข้าไประหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก หรือในเวลาทำการของสถานที่นั้น

4) แสดงบัตรประจำตัวต่อผู้ที่เกี่ยวข้อง

โทษทางปกครองในกรณีนี้ สามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาคดีปกครอง ตามลำดับ

A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

3.1.2 ประมวลกฎหมายแพ่งและพาณิชย์

ตามประมวลกฎหมายแพ่งและพาณิชย์ของไทยนั้น ได้บัญญัติหลักเกณฑ์เกี่ยวกับความรับผิดทางละเมิดไว้ในบรรพ 2 หนี้ ลักษณะ 5 ละเมิด (มาตรา 420 - 452) ซึ่งในมาตรา 420[40] บัญญัติว่า "ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น" ซึ่งหลักกฎหมายเบื้องต้นในการพิจารณาว่าการกระทำใดเป็นการละเมิดหรือไม่นั้น จะต้องพิจารณาจากองค์ประกอบได้ดังต่อไปนี้

1) มีการกระทำ หมายถึง การเคลื่อนไหวร่างกายโดยรู้สำนึกในการเคลื่อนไหวนั้นและอยู่ในบังคับของจิตใจผู้กระทำ และรวมถึงการงดเว้นการกระทำที่ตนมีหน้าที่ตามกฎหมายที่ต้องกระทำและการงดเว้นนั้นเป็นเหตุให้เกิดความเสียหายขึ้น

2) โดยจงใจหรือประมาทเลินเล่อ

โดยจงใจ หมายถึง รู้สำนึกถึงผลหรือความเสียหายจากการกระทำของตนโดยประมาทเลินเล่อ หมายถึง เป็นการกระทำโดยปราศจากความระมัดระวัง ซึ่งบุคคลในภาวะเช่นนั้นจำต้องมีโดยต้องเปรียบเทียบกับบุคคลที่ต้องมีความระมัดระวังตามพฤติการณ์ และตามฐานะในสังคมเช่นเดียวกับผู้กระทำความเสียหาย

3) โดยผิดกฎหมาย เป็นการกระทำโดยไม่มีอำนาจหรือไม่มีสิทธิหรือโดยมิชอบด้วยกฎหมาย (unlawful) และรวมความถึงการใช้อำนาจที่มีอยู่เกินส่วนหรือใช้อำนาจตามกฎหมายเพื่อกลั่นแกล้งผู้อื่น

4) เกิดความเสียหายแก่บุคคลอื่น

ความเสียหายนั้นจะเป็นความเสียหายที่เกิดแก่ชีวิต ร่างกาย อนามัยเสรีภาพ ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ได้ แต่ต้องเป็นความเสียหายที่แน่นอนไม่ว่าจะเกิดขึ้นแล้วในปัจจุบันหรือจะเกิดขึ้นในอนาคตก็จะต้องเป็นความเสียหายที่จะเกิดขึ้นอย่างแน่นอน และความเสียหายจะต้องเกิดจากผลโดยตรงของผู้กระทำด้วย

ทั้งนี้ จะต้องครบองค์ประกอบดังกล่าวข้างต้นทุกข้อ จึงจะถือว่าเป็นการกระทำ "ละเมิด" ซึ่งผู้ทำละเมิดจะต้องรับผิดชดใช้ค่าสินไหมทดแทนให้แก่ผู้เสียหาย

การคุ้มครองข้อมูลส่วนบุคคลตามหลักกฎหมายแพ่งและพาณิชย์นั้นเป็นการมุ่งคุ้มครองในลักษณะที่จะเป็นการเยียวยาแก้ไขในสิ่งที่บุคคลผู้นั้นได้กระทำลงไปแล้ว โดยให้มีการใช้ค่าสินไหมทดแทนแก่บุคคลผู้ที่ได้รับความเสียหายนั้นๆ โดยมีมาตรา 420 เป็นหลักการทั่วไปในการให้ความคุ้มครองสิทธิส่วนบุคคล

---

[40] ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 420.

อย่างไรก็ดี นอกจากการคุ้มครองสิทธิส่วนบุคคล ตามมาตรา 420 แล้วยังมีการคุ้มครองสิทธิส่วนบุคคลตามมาตรา 423[41] อีกด้วย บัญญัติไว้ว่า “ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสาส์นอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสาส์นนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสาส์นเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่”

ความรับผิดทางแพ่ง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนด ความรับผิดทางแพ่งไว้ในมาตรา 77 เป็นพิเศษแตกต่างไปจากหลักกฎหมายละเมิดทั่วไปตามประมวลกฎหมายแพ่งและพาณิชย์ ดังนั้น ในส่วนนี้จึงจะอธิบายรายละเอียด เช่น องค์ประกอบ ข้อยกเว้น ผลของการฝ่าฝืนหรือไม่ปฏิบัติตาม และอายุความของมาตราดังกล่าว ดังนี้

องค์ประกอบของความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77[42]

1) ผู้กระทำละเมิดมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

2) บุคคลดังกล่าวดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การดำเนินการอันฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

โดยมีข้อแตกต่างของความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77[43] กับหลักกฎหมายละเมิดทั่วไปตามประมวลกฎหมายแพ่งและพาณิชย์ คือ ความรับผิดทางแพ่งข้างต้น ไม่จำเป็นต้องพิสูจน์ว่าการกระทำฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่

---

[41] ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 423.

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 77.

[43] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 77.

ข้อยกเว้นความรับผิด

1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย

2) ความเสียหายเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

3) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ตัวอย่าง

เจ้าพนักงานควบคุมโรคติดต่อ มีหนังสือให้บริษัทเปิดเผยข้อมูลส่วนบุคคลของผู้เอาประกันภัยอุบัติเหตุการเดินทาง ที่เดินทางไปและกลับจากประเทศที่เป็นกลุ่มเสี่ยงโรคติดต่ออันตราย เพื่อใช้ประกอบการควบคุมโรคติดต่ออันตราย ตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 กรณีนี้แม้ว่าบริษัทจะไม่ได้ปฏิบัติตามหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด บริษัทก็ได้รับยกเว้นความรับผิดทางแพ่ง

ผลของการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เมื่อผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ฝ่าฝืนหรือไม่ปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องรับผิดทางแพ่งและต้องชำระค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล

ทั้งนี้ ค่าสินไหมทดแทน หมายความรวมถึง ค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

นอกจากนี้ ค่าสินไหมทดแทนข้างต้น ที่เป็นค่าสินไหมทดแทนที่แท้จริงแล้ว ศาลยังมีอำนาจกำหนดค่าสินไหมทดแทนเพื่อการลงโทษ[44] ตามที่ศาลเห็นสมควรด้วย แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง โดยในการกำหนดค่าสินไหมทดแทนเชิงการลงโทษนั้น ศาลจะคำนึงถึงพฤติการณ์ต่าง ๆ เช่น [45]

1) ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ

2) ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ

3) สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

---

[44] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 78.

[45] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

4) การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น

5) การที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

ข้อสังเกต

ค่าสินไหมทดแทนสำหรับความรับผิดทางแพ่งภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลนี้ อาจจะมีปัญหาในทางปฏิบัติเกี่ยวกับการคำนวณค่าสินไหมทดแทน เพราะหากความเสียหายที่เกิดขึ้น เกิดแต่เพียงความเสียหายจากการละเมิดสิทธิความเป็นส่วนตัว แต่ไม่ได้เกิดความเสียหายต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล จะเป็นการยากที่จะคำนวณค่าสินไหมทดแทนเป็นตัวเงิน

อายุความฟ้องเรียกค่าสินไหมทดแทน[46]

สิทธิค่าเสียหายในทางแพ่งนี้จะหมดอายุความเมื่อพ้น 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิด หรือเมื่อพ้น 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

ในส่วนนี้จะกล่าวถึงหลักกฎหมายระหว่างประเทศและต่างประเทศ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดาที่เกี่ยวข้องกับการคุ้มครองการจัดเก็บข้อมูลส่วนบุคคล รวมถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ได้แก่ กฎหมายที่คุ้มครองข้อมูลส่วนบุคคลโดยตรง และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไป โดยมีรายละเอียดดังต่อไปนี้

3.2.1 กฎหมายของสหภาพยุโรป General data Protection Regulation (GDPR)

หลักการคุ้มครองข้อมูลตามกฎหมาย General Data Protection Regulation 2016 ที่สำคัญมีดังนี้[47]

1) ขอบเขตการบังคับใช้เชิงพื้นที่กฎหมาย GDPR บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ใน EU ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน กล่าวคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลใน EU ไม่ว่าการประมวลผลจะทำใน EU หรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง EU

---

[46] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 78.

[47] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นใน EU หากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิก EU (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนใน EU ด้วย

2) บทลงโทษ กรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4 % ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่น กรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบ การไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำ Privacy Impact Assessment

3) การให้ความยินยอม หลักความยินยอมมีความเข้มแข็งมากขึ้นในรูปแบบที่เข้าใจได้และสามารถเข้าถึงได้สะดวก (Intelligible and easily access) ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอคำยินยอม การขอความยินยอมต้องมีความชัดเจนและใช้ภาษาที่ง่ายต่อการเข้าใจ นอกจากนี้ การยกเลิกการให้ความยินยอมต้องก็ต้องดำเนินการได้ด้วยความสะดวก

3.2.1.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของสหภาพยุโรป (EU: European Union)

General Data Protection Regulation (หรือที่เรียกว่า GDPR) เป็นกฎหมายของสหภาพยุโรป (EU: European Union) ที่มีวัตถุประสงค์เพื่อให้ บริษัท หรือธุรกิจที่จัดเก็บและจัดการข้อมูลส่วนบุคคลจะต้องเพิ่มมาตรการการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลตามฐานที่ชอบด้วยกฎหมาย

3.2.1.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล หรือ Data breach notification ถือเป็นหน้าที่ตามกฎหมายที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคลในทุก ๆ ประเทศ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้วางหลักในเรื่องการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลไว้ในทิศทางเดียวกันกับ GDPR[48]

1) ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงหลังจากได้รับเรื่องแล้ว การแจ้งในกรณีที่มีการ

---

[48] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

ละเมิดข้อมูลส่วนบุคคลต้องแจ้งต่อหน่วยงานที่มีหน้าที่กำกับดูแลภายใต้อำนาจตามมาตรา 55 เว้นแต่การละเมิดข้อมูลส่วนบุคคลจะไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ในกรณีที่การแจ้งเตือนไปยังหน่วยงานที่มีหน้าที่กำกับดูแล ไม่ได้ดำเนินการภายใน 72 ชั่วโมงจะต้องมีให้เหตุผลสำหรับเหตุที่เกิดความล่าช้า

2) หน่วยประมวลผลจะแจ้งให้ผู้ตรวจสอบทราบโดยไม่ชักช้าหลังจากรับเหตุการละเมิดข้อมูลส่วนบุคคล

3) การแจ้งกรณีที่มีการละเมิดข้อมูลส่วนบุคคลตามข้อ 1 จะต้องประกอบด้วย[49]

1) อธิบายลักษณะของการละเมิดข้อมูลส่วนบุคคล รวมถึงการให้ข้อมูลที่เกี่ยวข้อง ควรระบุรายละเอียดหรือสามารถจำแนกเป็นหมวดหมู่หรือระบุจำนวนตัวเลขได้โดยประมาณ

2) ระบุชื่อและรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลหรือวิธีติดต่ออื่น ๆ ที่สามารถรับข้อมูลเพิ่มเติมได้

3) อธิบายถึงผลที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

4) อธิบายถึงมาตรการที่ดำเนินการหรือเสนอให้ผู้ตรวจสอบดำเนินการ เพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลรวมถึงมาตรการที่เหมาะสมเพื่อบรรเทาผลกระทบที่อาจจะเกิดขึ้น

5) ควรให้ข้อมูลในขณะที่เกิดเหตุเท่าที่จะพอได้ในเวลานั้น เพื่อจะสามารถดำเนินการในขั้นตอนต่อไปได้โดยไม่ล่าช้า

6) ผู้ตรวจสอบจะต้องบันทึกข้อมูลการละเมิดข้อมูลส่วนบุคคล ซึ่งประกอบด้วยข้อเท็จจริงที่เกี่ยวข้องกับการละเมิดผลกระทบและการดำเนินการแก้ไข และนำส่งเอกสารอื่น ๆที่เกี่ยวข้องให้หน่วยงานที่กำกับดูแลสามารถตรวจสอบได้ [50]

ข้อมูลส่วนบุคคลที่ถูกละเมิด

---

[49] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

[50] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

1) เมื่อการละเมิดข้อมูลส่วนบุคคลมีแนวโน้มที่จะส่งผลให้มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ผู้ตรวจสอบจะต้องแจ้งข้อมูลการละเมิดให้ทราบโดยไม่ชักช้า

2) การแจ้งข้อมูลในทราบตามข้อ 1 จะต้องอธิบายในภาษาที่ชัดเจนและเข้าใจง่าย ลักษณะของการละเมิดข้อมูลส่วนบุคคลและจะต้องมีข้อมูลอย่างน้อย ตามมาตรการในข้อ 3

3) การสื่อสารให้ทราบเรื่องข้อมูลตามข้อ 1 จะไม่จำเป็นหากตรงตามเงื่อนไขใด ๆ ต่อไปนี้

ผู้ตรวจสอบ องค์กร ได้ใช้มาตรการป้องกันทางเทคนิคที่เหมาะสมและมาตรการเหล่านั้นถูกนำไปใช้กับข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิด โดยเฉพาะอย่างยิ่งสิ่งที่ทำให้ข้อมูลส่วนบุคคลไม่สามารถเข้าใจได้สำหรับบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึง เช่น การเข้าใช้รหัส ผู้ตรวจสอบจะต้องดำเนินตามมาตรการ ซึ่งทำให้มั่นใจได้ว่าจะไม่เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่ระบุไว้ในข้อ ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล เจ้าของข้อมูลควรจะต้องมีการสื่อสารต่อสาธารณชนหรือมาตรการที่ได้รับหลังการแจ้งเหตุเพื่อให้ผู้อื่นได้รับความคุ้มครองอย่างมีประสิทธิภาพและเท่าเทียมกัน และหากผู้ตรวจสอบไม่แจ้งการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่กำกับดูแลได้พิจารณาซึ่งจะทำให้เกิดความเสี่ยงสูง ที่อาจจะต้องให้ดำเนินการหรือให้เป็นไปตามเงื่อนไขในข้อ [51]

---

[51] GDPR Chapter 4 Controller and processor

Art. 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

เมื่อบริษัทฯ พบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลข้างต้น การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยที่การดำเนินการตรวจสอบข้อเท็จจริงของการละเมิดข้อมูลส่วนบุคคลตามที่ระบุไว้ในกฎหมายลำดับรองนั้นจะต้องดำเนินการภายในระยะเวลา 72 ชั่วโมงด้วยเช่นกัน อย่างไรก็ดีตามหลักการที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR[52] มีการขยายความชัดเจนในเรื่องนี้ออกไปอีก โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ช่วงระยะเวลาไม่นานในการตรวจสอบข้อเท็จจริงและทำการยืนยันว่าเหตุละเมิดข้อมูลส่วนบุคคลที่พบหรือรับแจ้งนั้นได้เกิดขึ้นจริงหรือไม่ และภายในช่วงระยะเวลาไม่นานนั้นยังถือไม่ได้ว่าบริษัทฯได้ 'รับทราบ' การละเมิดข้อมูลส่วนบุคคลแล้ว

ดังนั้น จากการพิจารณาการตีความ GDPR ดังกล่าว บริษัทฯ ย่อมสามารถจัดให้มีระบบงานหรือขั้นตอนภายในซึ่งมีกระบวนการที่ใช้ระยะเวลาไม่นานนัก โดยคำนึงถึงโครงสร้างองค์กรของตนเพื่อการตรวจสอบยืนยันการเกิดเหตุตามข้อเท็จจริงดังกล่าว และช่วงเวลานั้นบริษัทฯ ยังไม่สามารถพิจารณาได้ว่าได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเพื่อเริ่มนับกำหนดระยะเวลา 72 ชั่วโมงที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ และหน่วยงานรัฐที่เกี่ยวข้อง[53]

3.2.2 กฎหมายของสาธารณรัฐสิงคโปร์ (The Personal Data Protection Act.)

3.2.2.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศสิงคโปร์

ประเทศสิงคโปร์มีการบังคับใช้รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2555 (Personal Data Protection Act 2012) โดยได้ผ่านการรับรองจากรัฐสภาเมื่อวันที่ 15 กุมภาพันธ์ 2555 และผ่านการรับรองจากประธานาธิบดีเมื่อวันที่ 20 พฤศจิกายน พ.ศ. 2555

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA ตั้งแต่ปี 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี 2556

4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [2]That documentation shall enable the supervisory authority to verify compliance with this Article.

Art. 34 GDPR Communication of a personal data breach to the data subject

[52] Guidelines 9/2022 on personal data breach notification under GDPR

[53] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

2) ตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ PDPC ให้คำปรึกษา รวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล ช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มที่

ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสาธารณรัฐสิงคโปร์ บังคับใช้เฉพาะภาคเอกชนเท่านั้น

1) การขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต

2) คุ้มครองข้อมูลส่วนบุคคลต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมาย

3) ให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

สำหรับประเทศอย่างสาธารณรัฐสิงคโปร์ นั้น ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA เช่นเดียวกับของประเทศไทย ซึ่งที่นี่ประกาศใช้ตั้งแต่ปี 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี 2556 โดยมีระยะเวลาเตรียมความพร้อมถึง 18 เดือนด้วยกัน โดยระหว่างนั้นได้มีการจัดอบรม เผยแพร่ความรู้ เพื่อเตรียมความพร้อมให้กับภาคเอกชนและประชาชนอย่างต่อเนื่อง เพื่อสร้างความเข้าใจอันดีเกี่ยวกับข้อดีของ PDPA ที่จะมีผลบังคับใช้ภายในประเทศ

นอกจากนี้ สาธารณรัฐสิงคโปร์ยังมีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ PDPC ซึ่งถือเป็นอีกหนึ่งข้อดีของการนำ PDPA เข้ามาบังคับใช้ โดย PDPC จะเข้ามามีบทบาทในเรื่องการให้คำปรึกษา รวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุเอาไว้ นอกจากนี้ยังจะเป็นการช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มที่

ข้อกำหนดที่น่าสนใจของ PDPA

1) เป็นการบังคับใช้เฉพาะภาคเอกชนเท่านั้น

2) การขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะเป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต

3) การความคุ้มครองข้อมูลส่วนบุคคลจะต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมาย

4) ให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์[54]

3.2.2.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

สิทธิในการร้องเรียนต่อคณะกรรมการด้านข้อมูลส่วนบุคคลเป็นมาตรการเยียวยาเจ้าของข้อมูล จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย[55]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสาธารณรัฐสิงคโปร์ หรือไม่ ถือว่าอยู่ภายใต้กฎหมายดังกล่าว

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลต้องได้รับความยินยอม จากเจ้าของข้อมูลก่อนทำการเก็บบันทึก การใช้ และการเปิดเผยข้อมูลส่วนบุคคล และจะต้องใช้ข้อมูลนั้น เพื่อวัตถุประสงค์ตามที่แจ้งเท่านั้น รวมถึงจะต้องจัดให้เจ้าของข้อมูลเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลได้ และจะต้องยุติหรือหยุดการจัดเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็น

กรณีของสาธารณรัฐสิงคโปร์ ในหลักของความยินยอม กฎหมายกำหนดให้การทำความยินยอมควรจะทำ เป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ และเจ้าของข้อมูล

---

[54] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

[55] ลัฐกา เนตรทัศน์. (2566). ***สรุปภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย สิงคโปร์ และฟิลิปปินส์.*** (ออนไลน์). เข้าถึงได้จาก: https://lawforasean.krisdika.go.th/File/files/dataprotectionoverview.pdf

สามารถถอนหรือยกเลิกการให้ ความยินยอมในการใช้ข้อมูลเมื่อใดก็ได้ด้วยการแจ้งต่อองค์กรที่จัดเก็บข้อมูลประกอบเหตุผลในการถอน ความยินยอม[56]

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลจะต้อง มีการจัดการเพื่อรักษาความปลอดภัยอย่างเหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลและเพื่อป้องกัน การเข้าถึง การจัดเก็บ การใช้การเปิดเผย การคัดลอก การแก้ไข การลบข้อมูลหรือความเสี่ยงอื่นในทำนอง เดียวกัน ซึ่งกระทำโดยมิชอบด้วยกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2555 (Personal Data Protection Act 2012)

การแจ้งเตือนการละเมิดข้อมูล

“บุคคลที่ได้รับผลกระทบ” หมายถึง บุคคลใดๆ ที่ข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิดข้อมูลที่เกี่ยวข้อง

“การละเมิดข้อมูล” ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล หมายถึง

(ก) การเข้าถึง รวบรวม ใช้ เปิดเผย คัดลอก แก้ไข หรือกำจัดข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือ

(ข) การสูญเสียสื่อหรืออุปกรณ์จัดเก็บข้อมูลใด ๆ ที่ข้อมูลส่วนบุคคลถูกเก็บไว้ในสถานการณ์ที่การเข้าถึงโดยไม่ได้รับอนุญาต การรวบรวม การใช้ การเปิดเผย การคัดลอก การปรับเปลี่ยนหรือการกำจัดข้อมูลส่วนบุคคลที่มีแนวโน้มจะเกิดขึ้น[57]

การละเมิดข้อมูลที่แจ้งให้ทราบ[58]

การละเมิดข้อมูล คือ การละเมิดข้อมูลที่สามารถแจ้งได้หากการละเมิดข้อมูล

---

[56] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

[57] Interpretation of this Part26A. In this Part, unless the context otherwise requires

“affected individual” means any individual to whom anypersonal data affected by a data breach relates;

“data breach”, in relation to personal data, means

[58] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

1) ส่งผลให้เกิดหรือมีแนวโน้มที่จะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ หรือเป็นหรือมีแนวโน้มว่าจะมีขนาดที่มีนัยสำคัญ

2) โดยไม่จำกัดส่วนย่อยการละเมิดข้อมูลจะถือว่าส่งผลเสียต่อบุคคลอย่างมีนัยสำคัญหากการละเมิดข้อมูลเกี่ยวข้องกับข้อมูลส่วนบุคคลที่กำหนดไว้หรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้น หรือในกรณีอื่น ๆ ที่กำหนด

3) โดยไม่จำกัดส่วนย่อย (1)(b) การละเมิดข้อมูลถือว่ามีนัยสำคัญหากการละเมิดข้อมูลส่งผลกระทบไม่น้อยกว่าจำนวนที่กำหนดของผู้ได้รับผลกระทบ หรือ

(b) ในกรณีอื่น ๆ ที่กำหนด

4) แม้จะมีส่วนย่อย (1) (2) และ (3) การละเมิดข้อมูลที่เกี่ยวข้องกับการเข้าถึง รวบรวม ใช้ เปิดเผย คัดลอกหรือแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตเฉพาะภายในองค์กรจะถือว่าไม่สามารถแจ้งได้ การละเมิดข้อมูล[59]

หน้าที่ดำเนินการประเมินการละเมิดข้อมูล

1) ส่วนนี้ใช้กับการละเมิดข้อมูลที่เกิดขึ้นในหรือหลังวันที่ 1 กุมภาพันธ์ พ.ศ. 2564

2) ภายใต้หัวข้อย่อย (3) เมื่อองค์กรมีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลซึ่งส่งผลกระทบต่อข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรืออยู่ภายใต้การควบคุมขององค์กร องค์กรต้องดำเนินการประเมินอย่างสมเหตุสมผลและรวดเร็วว่า การละเมิดข้อมูลถือเป็นการละเมิดข้อมูลที่สามารถแจ้งได้

3) เมื่อตัวกลางข้อมูล (นอกเหนือจากตัวกลางข้อมูลที่กล่าวถึงในมาตรา 26E) มีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลเกิดขึ้นเกี่ยวกับข้อมูลส่วนบุคคลที่ตัวกลางข้อมูลกำลังดำเนินการในนามของและเพื่อวัตถุประสงค์ขององค์กรอื่น

(ก) ตัวกลางข้อมูลต้องแจ้งให้องค์กรอื่นทราบถึงการละเมิดข้อมูลโดยไม่ชักช้า และ

(ข) ว่าองค์กรอื่นจะต้องดำเนินการเมื่อได้รับแจ้งจากตัวกลางข้อมูล

(ค) ว่าองค์กรอื่นจะต้องดำเนินการประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่ได้รับแจ้งหรือไม่ เมื่อได้รับแจ้งจากตัวกลาง

(4) องค์กรต้องดำเนินการประเมินตามข้อ (2) หรือ (3)(b) ตามข้อกำหนดที่กำหนดไว้[60]

---

[59] Notifiable data breaches Personal Data Protection Act 2012 26B.

(1) A data breach is a notifiable data breach if the data breach

[60] Duty to conduct assessment of data breach26C.

หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล มีรายละเอียดที่ต้องแจ้งดังนี้[61]

1) ในกรณีที่องค์กรประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่แจ้งได้ องค์กรต้องแจ้งให้คณะกรรมการทราบทันทีที่ทำได้ แต่ไม่ช้ากว่า 3 วัน ตามปฏิทินหลังจากวันที่องค์กรทำการประเมินนั้น

2) ภายใต้หัวข้อย่อย (5), (6) และ (7) ในหรือหลังจากแจ้งต่อคณะกรรมาธิการตามอนุมาตรา (1) แล้ว องค์กรต้องแจ้งบุคคลที่ได้รับผลกระทบแต่ละรายที่ได้รับผลกระทบจากการละเมิดข้อมูลที่ต้องแจ้งให้ทราบซึ่งกล่าวถึงในลักษณะใด ๆ ที่สมเหตุสมผลในสถานการณ์

3) ประกาศตามอนุมาตรา (1) หรือ (2) ต้องมีข้อมูลทั้งหมดที่แจ้งต่อคณะกรรมการหรือผู้ได้รับผลกระทบ (แล้วแต่กรณี) เท่าที่ทราบและความเชื่อขององค์กรอย่างดีที่สุด กำหนดไว้เพื่อการนี้

4) การแจ้งตามอนุมาตรา (๑) ต้องทำตามแบบและยื่นตามที่คณะกรรมการกำหนด

5) หมวดย่อย (2) ใช้ไม่ได้กับองค์กรที่เกี่ยวข้องกับบุคคลที่ได้รับผลกระทบหากองค์กร

(a) ในหรือหลังจากการประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่สามารถแจ้งได้ ดำเนินการใดๆ ตามข้อกำหนดที่กำหนดไว้ ซึ่งทำให้ไม่น่าเป็นไปได้ที่การละเมิดข้อมูลที่แจ้งจะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ หรือ

(b) ได้ดำเนินการ ก่อนเกิดการละเมิดข้อมูลที่สามารถแจ้งได้ มาตรการทางเทคโนโลยีใดๆ ที่ทำให้ไม่น่าเป็นไปได้ที่การละเมิดข้อมูลที่แจ้งได้จะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ

6) องค์กรต้องไม่แจ้งบุคคลที่ได้รับผลกระทบตามอนุมาตรา (2) หาก

(ก) หน่วยงานบังคับใช้กฎหมายที่กำหนดเพื่อสั่ง หรือ

(b) คณะกรรมาธิการสั่งเช่นนั้น

7) ในการสมัครเป็นลายลักษณ์อักษรขององค์กร คณะกรรมาธิการอาจสละข้อกำหนดในการแจ้งให้บุคคลที่ได้รับผลกระทบทราบภายใต้มาตราย่อย (2) ภายใต้เงื่อนไขใด ๆ ที่คณะกรรมการเห็นสมควร

8) องค์กรไม่ได้แจ้งต่อคณะกรรมการตามอนุมาตรา (1) หรือบุคคลที่ได้รับผลกระทบตามอนุมาตรา (2) ด้วยเหตุผลเพียงอย่างเดียวเท่านั้น ให้ถือว่าละเมิด

---

[61] ลัฐกา เนตรทัศน์. (2566). ***สรุปภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย สิงคโปร์ และฟิลิปปินส์.*** (ออนไลน์). เข้าถึงได้จาก: https://lawforasean.krisdika.go.th/File/files/dataprotectionoverview.pdf

(ก) หน้าที่หรือภาระผูกพันใด ๆ ตามกฎหมายที่เป็นลายลักษณ์อักษรหรือหลักนิติธรรม หรือสัญญาใด ๆ เกี่ยวกับความลับหรือข้อจำกัดอื่น ๆ ในการเปิดเผยข้อมูล หรือ

(b) กฎความประพฤติทางวิชาชีพใด ๆ ที่ใช้กับองค์กร

9) ส่วนย่อย (1) และ (2) ใช้ควบคู่ไปกับภาระผูกพันขององค์กรภายใต้กฎหมายที่เป็นลายลักษณ์อักษรอื่น ๆ เพื่อแจ้งให้บุคคลอื่น (รวมถึงหน่วยงานสาธารณะใด ๆ) ทราบถึงการละเมิดข้อมูลหรือเพื่อให้ข้อมูลใด ๆ ที่เกี่ยวข้องกับ การละเมิดข้อมูล

ภาระหน้าที่ของตัวกลางข้อมูลของหน่วยงานของรัฐ

1) เป็นตัวกลางในการประมวลผลข้อมูลส่วนบุคคลในนามของและเพื่อวัตถุประสงค์ของหน่วยงานสาธารณะ และ

2) มีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลเกิดขึ้นเกี่ยวกับข้อมูลส่วนบุคคลนั้น องค์กรต้องแจ้งให้หน่วยงานสาธารณะทราบถึงการละเมิดข้อมูลโดยไม่ชักช้า[62]

3.2.3 กฎหมายของประเทศญี่ปุ่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคงของประเทศญี่ปุ่น หรือที่เรียกว่า “Act on the Protection of Personal Information (APPI)” เวอร์ชันเริ่มต้นซึ่งพัฒนาขึ้นในปี 2546 เป็นหนึ่งในกฎหมายคุ้มครองข้อมูลฉบับแรกที่เริ่มใช้ในเอเชีย APPI ได้รับการแก้ไขอย่างมีนัยสำคัญในปี 2559 และฉบับแก้ไขมีผลบังคับใช้ในวันที่ 30 พฤษภาคม 2560 หนึ่งปีต่อมาในวันที่ 25 พฤษภาคม 2561 ซึ่ง GDPR มีผลบังคับใช้

การอภิปรายเกี่ยวกับการตัดสินใจที่เพียงพอเริ่มขึ้นหลังจากนั้นไม่นานระหว่างคณะกรรมาธิการยุโรป และคณะกรรมาธิการการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่น หลังจากนั้นก็เริ่มออกกฎหมายเพิ่มเติมเพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคล เมื่อวันที่ 23 มกราคม 2019 ญี่ปุ่นกลายเป็นประเทศแรกในเอเชียที่ได้รับสถานะความเพียงพอจากคณะกรรมาธิการยุโรป การตัดสินใจนี้ระบุว่า APPI ร่วมกับบทบัญญัติที่เกี่ยวข้องอื่นๆ ในกฎหมายญี่ปุ่น ให้การคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกันโดยพื้นฐาน เช่นเดียวกับ GDPR

---

[62] Personal Data Protection Act 2012: Obligations of data intermediary of public agency 26E. Where an organisation

(a) is a data intermediary processing personal data on behalf of and for the purposes of a public agency; and

(b) has reason to believe that a data breach has occurred in relation to that personal data, the organisation must, without undue delay, notify the public agency of the occurrence of the data breach.

โดยกฎหมายทั้งสองฉบับมีข้อกำหนดสำหรับข้อมูลพิเศษหรือข้อมูลที่ละเอียดอ่อน กำหนดให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่สามารถใช้ในการระบุตัวบุคคล รวมถึงขอบเขตนอกอาณาเขต และกำหนดข้อผูกพันสำหรับผู้ปฏิบัติงานหรือผู้ควบคุม/ผู้ประมวลผลที่จัดการข้อมูลส่วนบุคคล นอกจากนี้ APPI และ GDPR ให้รายละเอียดเกี่ยวกับสิทธิ์ของเจ้าของข้อมูล รวมถึงสิทธิ์ในการลบ การได้รับแจ้ง การคัดค้าน การเข้าถึงข้อมูลส่วนบุคคล และการระบุความยินยอมเป็นหลักการสำคัญ กฎหมายทั้งสองยังกำหนดให้มีหน่วยงานกำกับดูแลและการออกมาตรการลงโทษทางการเงิน

อย่างไรก็ตาม ในขณะเดียวกัน APPI และ GDPR มีความแตกต่างกันอย่างมีนัยสำคัญ ในกรณีที่ GDPR ระบุความแตกต่างระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผล APPI จะอ้างถึงเฉพาะผู้ประกอบการธุรกิจที่จัดการข้อมูลส่วนบุคคลเท่านั้น GDPR แสดงคำจำกัดความโดยละเอียดของการประมวลผล แต่ APPI ชี้แจงเฉพาะว่านำไปใช้กับข้อมูลส่วนบุคคล ฐานข้อมูลข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่เก็บไว้ ข้อกำหนดบางประการใน APPI ใช้กับข้อมูลส่วนบุคคลที่เก็บไว้ดังกล่าว ในขณะที่ GDPR ไม่ได้สร้างความแตกต่างนี้ ในทางตรงกันข้าม GDPR มีบทบัญญัติเกี่ยวกับเด็ก ข้อมูลที่ใช้นามแฝง การประมวลผลเพื่อวัตถุประสงค์ในการวิจัย และข้อกำหนดเกี่ยวกับวิธีขอความยินยอม ซึ่งไม่ได้ระบุไว้ใน APPI[63]

GDPR ใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ซึ่งอาจเป็นธุรกิจหน่วยงานสาธารณะ สถาบัน และไม่ใช่สำหรับองค์กรที่แสวงหาผลกำไร APPI ใช้กับผู้ควบคุมข้อมูลส่วนบุคคล (PIC) ซึ่งถูกกำหนดให้เป็น 'บุคคลที่ให้ข้อมูลส่วนตัวฐานข้อมูลสารสนเทศ ฯลฯ เพื่อใช้ในธุรกิจ' กฎหมายทั้ง 2 ฉบับให้ความคุ้มครองบุคคลที่ยังมีชีวิตอยู่โดยคำนึงถึงการใช้ข้อมูลส่วนบุคคลของตน GDPR กำหนดว่าบุคคลได้รับการคุ้มครองโดยไม่คำนึงถึงสัญชาติและ/หรือถิ่นที่อยู่ ในขณะที่ APPI ไม่ได้กล่าวถึงประเด็นนี้อย่างชัดเจน

ขอบเขตอาณาเขต ทั้ง GDPR และ APPI มีขอบเขตนอกอาณาเขต โดยเฉพาะอย่างยิ่ง GDPR ใช้กับองค์กรนอกสหภาพยุโรปหากมีการเสนอสินค้าหรือบริการเพื่อหรือติดตามพฤติกรรมของบุคคลภายในสหภาพยุโรป ข้อกำหนดบางประการของ APPI ใช้บังคับกับผู้ประกอบธุรกิจที่เกี่ยวข้องกับการจัดหาสินค้าหรือบริการแก่บุคคลในประเทศญี่ปุ่น ได้รับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลในญี่ปุ่นและจัดการในต่างประเทศ

ขอบเขตของวัสดุGDPR ใช้กับการประมวลผลข้อมูลส่วนบุคคล ในขณะที่ APPI ใช้กับการจัดการข้อมูลส่วนบุคคลสำหรับธุรกิจวัตถุประสงค์ ทั้ง GDPR และ APPI ใช้กับข้อมูลส่วน

---

[63] Comparing privacy laws: GDPR v. APPI

บุคคลและข้อมูลส่วนบุคคลตามลำดับ อย่างไรก็ตาม เฉพาะ APPI เท่านั้นรวมถึงข้อมูลที่ประมวลผลโดยไม่ระบุตัวตนภายในขอบเขตของมัน[64]

APPI ใช้กับ 'ข้อมูลส่วนบุคคล' ซึ่งกำหนดไว้เป็น 'ข้อมูลเกี่ยวกับบุคคลที่มีชีวิต' (ดูหัวข้อ 2.1.) APPI ยังกำหนดข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลประกอบเป็นฐานข้อมูลข้อมูลส่วนบุคคล APPI กำหนดข้อมูลส่วนบุคคลที่ต้องการเป็นพิเศษดูแลและจัดเตรียมข้อกำหนดเฉพาะสำหรับการจัดการ APPI ใช้กับ PIC ที่ใช้ข้อมูลส่วนบุคคลในธุรกิจ

APPI ไม่ได้กำหนดว่ากิจกรรมใดเป็นส่วนหนึ่งของ การจัดการข้อมูลส่วนบุคคล มันชี้แจงว่า APPI ใช้กับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่เก็บไว้และ 'ฐานข้อมูลข้อมูลส่วนบุคคล' ซึ่งหมายถึง 'ส่วนรวม' เนื้อหาประกอบด้วยข้อมูลส่วนบุคคล

ทั้ง GDPR และ APPI รวมคำจำกัดความของ 'ข้อมูลส่วนบุคคล' และ 'ข้อมูลส่วนบุคคล' ตามลำดับ นอกจากนี้ APPIกำหนด 'ข้อมูลส่วนบุคคล' เกี่ยวกับฐานข้อมูลข้อมูลส่วนบุคคลและ 'ข้อมูลส่วนบุคคลที่เก็บไว้

ข้อมูลส่วนตัว (ข้อมูลส่วนบุคคล)

GDPR ให้คำจำกัดความของข้อมูลที่ละเอียดอ่อน ('ข้อมูลส่วนบุคคลประเภทพิเศษ') และห้ามไม่ให้มีการประมวลผล เว้นแต่หนึ่งในนั้นข้อยกเว้นมีผลบังคับใช้ ภายใต้ APPI ข้อมูลส่วนบุคคลที่ต้องการการดูแลเป็นพิเศษอาจได้รับการจัดการตามที่ผู้ว่าจ้างมอบให้ยินยอมหรือเมื่อมีการยกเว้น APPI ใช้กับข้อมูลที่ประมวลผลโดยไม่ระบุชื่อ ในขณะที่ GDPR ไม่รวมข้อมูลที่ไม่ระบุตัวตนอย่างชัดเจนจากขอบเขตของมันของการสมัคร[65]

ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลต้องปฏิบัติตามคำขอการใช้สิทธิของเจ้าของข้อมูล เช่น สิทธิในการลบ สิทธิ์ในการแก้ไข สิทธิ์ในการเข้าถึง ฯลฯ เว้นแต่จะใช้ข้อยกเว้น ผู้ประมวลผลข้อมูลต้องปฏิบัติตามด้วยสิทธิ์ของเจ้าของข้อมูลหากผู้ควบคุมข้อมูลต้องการผู้ควบคุมข้อมูลต้องปฏิบัติตามข้อจำกัดของวัตถุประสงค์และหลักความถูกต้องและแก้ไขข้อมูลของเจ้าของข้อมูลข้อมูลส่วนบุคคลหากไม่ถูกต้องหรือไม่ครบถ้วน ผู้ควบคุมข้อมูลต้องดำเนินการทางเทคนิค และมาตรการรักษาความปลอดภัยขององค์กร

PICs ต้องตอบสนองต่อความต้องการของ การหยุดใช้งานหรือการลบข้อมูลส่วนบุคคลที่เก็บไว้ข้อมูล ฯลฯ ในกรณีที่กฎหมายกำหนดPICs ต้องมั่นใจว่าข้อมูลส่วนบุคคลนั้นถูกต้องและ

---

[64] สมชาย ธรรมสุทธิวัฒน์และคณะ. (2563). รูปแบบความ ร่วมมือและยกระดับการป้องกันการทุจริตในประเทศไทย โดยศึกษาประสบการณ์ประเทศญี่ปุ่น และเกาหลีใต้. ***วารสารวิชาการธรรมทรรศน์***, 20(1). หน้า 1-10.

[65] เรื่องเดียวกัน, หน้า 1-10.

ทันสมัยวันที่เพื่อให้บรรลุวัตถุประสงค์การใช้งานและแก้ไขใดๆเก็บรักษาข้อมูลส่วนบุคคลของตัวการที่ไม่เป็นข้อเท็จจริง PICs จะต้องดำเนินการที่จำเป็นและเหมาะสมสำหรับความปลอดภัยของข้อมูลส่วนบุคคลรวมถึงการป้องกันไม่ให้การรั่วไหล สูญหาย หรือเสียหายของข้อมูลส่วนบุคคลที่จัดการ[66]

ภาระหน้าที่อื่นๆ ที่กำหนดไว้ใน PIC รวมถึง: การลบข้อมูลส่วนบุคคลโดยไม่ชักช้าเมื่อมีการใช้งานไม่จำเป็น ใช้การดูแลที่จำเป็นและเหมาะสมเหนือบุคคลที่ได้รับมอบหมายเพื่อดูแลความปลอดภัยการควบคุมข้อมูลส่วนบุคคลที่ได้รับการจัดการมอบหมายเปิดเผยข้อมูลส่วนบุคคลที่เก็บไว้แก่เจ้าหน้าที่โดยไม่ล่าช้าตามวิธีการที่คณะรัฐมนตรีกำหนดเว้นแต่การเปิดเผยข้อมูลจะอยู่ภายใต้มาตรา 28(2)(i) ถึง (iii) จัดการข้อร้องเรียนเกี่ยวกับการจัดการอย่างเหมาะสมและเหมาะสมข้อมูลส่วนบุคคล; และมุ่งสร้างระบบที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวภายใต้มาตรา 35(1)

ไม่มีคำจำกัดความของผู้ประมวลผลข้อมูลภายใต้ APPI ซึ่งแตกต่างกับ GDPR ที่ผู้ประมวลผลข้อมูลเป็นบุคคลธรรมดาหรือนิติบุคคล สาธารณะอำนาจหน้าที่ หน่วยงานหรือหน่วยงานอื่นที่ดำเนินการข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

GDPR โปรเซสเซอร์ควรช่วยเหลือข้อมูลผู้ควบคุมจะทำการประเมินผลกระทบของการปกป้องข้อมูลก่อนดำเนินการ การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล('DPO'): โปรเซสเซอร์ต้องกำหนด DPO เมื่อจำเป็นโดยกฎหมาย รวมถึงกรณีที่ผู้ประมวลผลประมวลผลข้อมูลส่วนบุคคลในขนาดใหญ่ การแจ้งให้ผู้ควบคุมข้อมูลทราบถึงข้อมูลใด ๆการละเมิด: โปรเซสเซอร์จำเป็นต้องแจ้งให้ผู้ควบคุมทราบการละเมิดโดยไม่ชักช้าเกินควรหลังจากทราบการละเมิด[67]

ภาระหน้าที่อื่นๆ ที่กำหนดไว้ใน PIC รวมถึง: การลบข้อมูลส่วนบุคคลโดยไม่ชักช้าเมื่อมีการใช้งานไม่จำเป็น ใช้การดูแลที่จำเป็นและเหมาะสมเหนือบุคคลที่ได้รับมอบหมายเพื่อดูแลความปลอดภัยการควบคุมข้อมูลส่วนบุคคลที่ได้รับการจัดการมอบหมายเปิดเผยข้อมูลส่วนบุคคลที่เก็บไว้แก่เจ้าหน้าที่โดยไม่ล่าช้า ตามวิธีการที่คณะรัฐมนตรีกำหนดเว้นแต่การเปิดเผยข้อมูลจะอยู่ภายใต้มาตรา 28(2)(i) ถึง (iii) จัดการข้อร้องเรียนเกี่ยวกับการจัดการอย่างเหมาะสมและเหมาะสมข้อมูลส่วนบุคคล; และมุ่งสร้างระบบที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวภายใต้มาตรา 35(1)

GDPR หน่วยงานคุ้มครองข้อมูลมีอำนาจแก้ไขซึ่งได้แก่ 'ว่ากล่าวตักเตือน สั่งการผู้ควบคุมและตัวประมวลผลให้ปฏิบัติตาม สั่งผู้ควบคุมเพื่อสื่อสารการละเมิดข้อมูลไปยังเจ้าของ

---

[66] Comparing privacy laws: GDPR v. APPI

[67] ธวัชชัย งามเลิศ. (2563). ***แนวทางป้องปรามผู้ประกอบวิชาชีพสื่อมวลชนในการละเมิดสิทธิส่วนบุคคล***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา, คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม. หน้า 1.

ข้อมูลกำหนดห้ามการประมวลผลสั่งการแก้ไขหรือลบข้อมูล ระงับการถ่ายโอนข้อมูล แต่ PPC มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษา[68]

3.2.3.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศประเทศญี่ปุ่น

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่น เรียกว่า Act on the Protection of Personal Information: APPI โดยบังคับใช้กับผู้ประกอบธุรกิจทั้งหมด ที่มีการเก็บข้อมูลส่วนบุคคล มีการประกาศใช้ในปี 2546 และประกาศใช้อย่างเต็มรูปแบบทุกภาคส่วนในปี 2548 ซึ่งปี 2562 ทางสหภาพยุโรป (EU) ได้รับรองมาตรฐานการคุ้มครองข้อมูลกับประเทศญี่ปุ่น ให้สามารถถ่ายโอนข้อมูลส่วนตัวระหว่างสองเขตเศรษฐกิจได้อย่างอิสระ ช่วยให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นสูงขึ้น ถือเป็นการเพิ่มขีดความสามารถในการแข่งขันและการทำธุรกิจ[69]

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นมีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้ ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครอง เจ้าของข้อมูลมีสิทธิในการตรวจสอบ การแก้ไขข้อมูล การไม่ยินยอมให้ประมวลผล คุ้มครองข้อมูลละเอียดอ่อน (sensitive data)[70]

ญี่ปุ่นได้ตรากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Act on Protection of Personal Information - APPI) มาตั้งแต่ปี พ.ศ.2546 และมีผลบังคับใช้กับผู้ประกอบการทั้งหมดที่เสนอขายสินค้าและบริการที่มีการดำเนินการกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่น ไม่ว่าจะมีที่ตั้งอยู่ในญี่ปุ่นหรือไม่ก็ตาม และหลังจากที่ได้มีการบังคับใช้ ก็ได้มีการตรากฎระเบียบอื่น ๆ เพื่อให้สอดคล้องกับ APPI รวมถึงได้มีการเปลี่ยนแปลงแก้ไข APPI เพื่อให้ทันต่อสถานการณ์และการพัฒนาทางเทคโนโลยีที่เปลี่ยนแปลงไป จึงนับได้ว่า ญี่ปุ่นมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ก้าวหน้ามากที่สุดประเทศหนึ่ง

---

[68] Comparing privacy laws: GDPR v. APPI

[69] ธวัชชัย งามเลิศ. อ้างแล้วเชิงอรรถที่ 67. หน้า 1.

[70] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

ล่าสุด สืบเนื่องมาจากการที่มีจำนวนอาชญากรรมทางไซเบอร์และคดีเหตุการละเมิดข้อมูลส่วนบุคคลเพิ่มมากขึ้น ญี่ปุ่นจึงได้ตรากฎหมาย APPI ฉบับแก้ไขในปี พ.ศ.2563 ซึ่งมีความเข้มงวดมากขึ้น และมีขอบเขตที่กว้างขึ้น เช่น กำหนดกฎเกณฑ์เกี่ยวกับการส่งข้อมูลที่ครอบคลุมมากขึ้น[71]

3.2.3.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การดำเนินการกรณีมีการละเมิดเกิดขึ้น ทั้งนี้ กฎหมายฉบับดังกล่าวกำหนดให้เริ่มมีผลบังคับใช้ทั้งฉบับเมื่อวันที่ 1 เมษายน พ.ศ.2565 ที่ผ่านมา

ประเด็นสำคัญที่มีการเปลี่ยนแปลงในกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขและเราควรให้ความสนใจนั้นมีมากมาย ในที่นี้จะได้กล่าวถึงเฉพาะประเด็นที่สำคัญ ดังนี้[72]

1) การแจ้งการละเมิดข้อมูลส่วนบุคคลผู้ประกอบการมีหน้าที่แจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Commission – PIPC) และ เจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการละเมิดข้อมูลใดๆ ซึ่งมีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูล ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหว การละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์

2) ข้อกำหนดเกี่ยวกับการให้ข้อมูลกับบุคคลที่สามก่อนหน้านี้ เจ้าของข้อมูลต้องได้รับการแจ้งเกี่ยวกับข้อกำหนดการให้ข้อมูลกับบุคคลที่สาม แต่สำหรับกฎหมายใหม่ผู้ประกอบการต้องยืนยันว่าบุคคลที่สามผู้รับข้อมูลได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนที่จะให้ข้อมูลไป โดยต้องมีการระบุรายละเอียดเกี่ยวข้อมูลที่จะมีการให้ด้วย และต้องเก็บหลักฐานไว้เป็นเวลา 3 ปี

3) การส่งต่อข้อมูลไปยังต่างประเทศก่อนที่จะมีการส่งต่อข้อมูลไปยังบุคคลที่สามซึ่งไม่ได้อยู่ในญี่ปุ่นนั้น ต้องมีการแจ้งให้เจ้าของข้อมูลทราบ โดยต้องมีการแจ้งข้อมูลทั้งในส่วนของชื่อของประเทศปลายทาง ระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง และมาตรการคุ้มครองข้อมูลที่ผู้นำเข้าข้อมูลใช้

นอกจากนี้ ผู้ประกอบการที่จะส่งออกข้อมูล จะต้องดำเนินการตรวจสอบยืนยันสถานะของข้อมูลส่วนบุคคลและระบบที่ใช้ในการดำเนินการกับข้อมูลของผู้นำเข้าข้อมูล

---

[71] ฉิชนันท์ คุปตานนท์. (2565). ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/999304

[72] ธวัชชัย งามเลิศ. อ้างแล้วเชิงอรรถที่ 67. หน้า 1.

การประเมินมาตรการบรรเทาผลกระทบกรณีมีปัญหาใด ๆ เกิดขึ้น รวมไปถึงการประเมินมาตรการที่จะใช้เพื่อให้มั่นใจว่าจะมีการดำเนินการกับข้อมูลอย่างเหมาะสม

4) โทษ

ภายใต้ APPI ฉบับแก้ไขนั้น ได้มีการปรับแก้ไขเพิ่มเติมโทษให้รุนแรงมากขึ้นไม่น้อย เช่น กรณีฝ่าฝืนคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดโทษบุคคลผู้กระทำผิด จากเดิมโทษจำคุกสูงสุดไม่เกิน 6 เดือน หรือโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษจำคุกสูงสุดไม่เกิน 1 ปี

หรือโทษปรับสูงสุดไม่เกินหนึ่งล้านเยน และกำหนดโทษสำหรับนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ประมาณยี่สิบเจ็ดล้านห้าแสนบาทไทย)

หรือ ในกรณีที่มีการส่งข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ก็มีการเปลี่ยนโทษปรับในส่วนของนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินห้าล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน จะเห็นได้ว่า แนวกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของญี่ปุ่น ได้กำหนดโทษที่หนักขึ้นกรณีมีการดำเนินการกับข้อมูลที่ไม่ถูกต้องตามกฎหมาย และสร้างกฎเกณฑ์ที่เข้มงวดมากขึ้นเพื่อให้องค์กรต่าง ๆ ซึ่งมีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่นต้องปฏิบัติตาม ดังนั้นแล้ว ผู้ประกอบการไทยที่ทำการค้ากับผู้ประกอบการในญี่ปุ่น จึงควรศึกษากฎหมายฉบับนี้ไว้ให้มากด้วย[73]

หน่วยงานกำกับดูแล ทั้ง GDPR และ APPI กำหนดให้มีการจัดตั้งหน่วยงานที่มีอำนาจสอบสวนและแก้ไขเพื่อกำกับดูแลการบังคับใช้กฎหมาย และเพื่อช่วยให้องค์กรต่างๆ เข้าใจและปฏิบัติตามกฎหมาย GDPR ยังให้อำนาจดังกล่าวด้วย มีอำนาจในการกำหนดบทลงโทษทางการเงิน ในขณะที่ PPC ที่ควบคุมโดย APPI ไม่มีอำนาจในการออกตัวเงิน

บทลงโทษ นอกจากนี้ ในสหภาพยุโรป หน่วยงานคุ้มครองข้อมูลแห่งชาติยังเป็นส่วนหนึ่งของ European Data Protection Board ซึ่งเป็นหน่วยงานที่รับรองการใช้ GDPR อย่างสม่ำเสมอทั่วยุโรปหน่วยงานคุ้มครองข้อมูลมีหน้าที่ในการส่งเสริมการรับรู้และการจัดทำคำแนะนำเกี่ยวกับ GDPR

GDPR ระบุว่าหน่วยงานคุ้มครองข้อมูลต้องดำเนินการ ความเป็นอิสระอย่างสมบูรณ์เมื่อปฏิบัติงาน หน่วยงานคุ้มครองข้อมูลมีอำนาจสอบสวนซึ่งรวมถึงความสามารถในการดำเนินการตรวจสอบการปกป้องข้อมูลเข้าถึงข้อมูลส่วนบุคคลทั้งหมดที่จำเป็นสำหรับการ

---

[73] ฉิชนันท์ คุปตานนท์. (2565). ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/999304

ปฏิบัติงานของงานได้รับการเข้าถึงสถานที่ใด ๆ ของข้อมูลผู้ควบคุมและผู้ประมวลผล รวมทั้งอุปกรณ์และวิธีการหน่วยงานคุ้มครองข้อมูลมีอำนาจแก้ไขซึ่ง ได้แก่ ว่ากล่าวตักเตือน สั่งการผู้ควบคุมและตัวประมวลผลให้ปฏิบัติตาม สั่งผู้ควบคุมเพื่อสื่อสารการละเมิดข้อมูลไปยังเจ้าของข้อมูลกำหนดห้ามการประมวลผลสั่งการแก้ไขหรือลบข้อมูล ระงับการถ่ายโอนข้อมูล GDPR ไม่ได้ควบคุมวิธีการที่หน่วยงานคุ้มครองข้อมูลได้รับทุน ซึ่งปล่อยให้ประเทศสมาชิกเป็นผู้ตัดสินใจ[74]

มีหน้าที่จัดทำแนวทางและPPC ส่งเสริมการใช้ APPI APPI ระบุว่าประธานและคณะกรรมาธิการใช้อำนาจอย่างเป็นทางการของตนโดยอิสระ'กปปส. มีอำนาจสอบสวนซึ่งรวมถึงความสามารถเพื่อขอข้อมูลและดำเนินการตรวจสอบในสถานที่PPC มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษา[75]

ได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) เริ่มมีผลบังคับใช้ในปี พ.ศ. 2548 ซึ่งเป็นการเปลี่ยนแปลงครั้งสำคัญในวิธีการปกป้องข้อมูลส่วนบุคคล เดิมทีผู้ประกอบการเอกชนหรือภาครัฐ หากได้มีการกระทำการข้อมูลส่วนบุคคลของบุคคลอื่นให้เกิดความเสียหาย บุคคลผู้ได้รับความเสียหายจะขอชดใช้ค่าเสียหายตามจะต้องครบองค์ประกอบความผิดตามกฎหมายละเมิด แต่เมื่อมีการบัญญัติถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้วนั้น จึงต้องมาใช้พระราชบัญญัติดังกล่าวแทน การกำหนดว่าการถ่ายโอนข้อมูล โดยทั่วไปแล้วการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม เป็นกรณีที่เจ้าของข้อมูลไม่ได้รับ ความยินยอมล่วงหน้าจากหน่วยงานจะไม่สามารถกระทำได้เว้นแต่จะมีข้อยกเว้น ดังนี้

1) การโอนที่ได้รับอนุญาตตามกฎหมาย หากเป็นกรณีที่ได้รับอนุญาตแล้วไม่จำเป็นต้อง ได้รับความยินยอมล่วงหน้าจากเจ้าของหลักในการถ่ายโอนข้อมูลส่วนบุคคล (รวมถึงข้อมูลที่มีลักษณะละเอียดอ่อน

2) กรณีที่จำต้องได้รับความยินยอมจากเจ้าของข้อมูล ที่ถือว่าเป็นข้อกำหนดหรือได้รับอนุญาตโดยเฉพาะตามกฎหมายหรือข้อบังคับของญี่ปุ่น จะต้องเป็นกรณีที่มีความจำเป็นสำหรับ การปกป้องชีวิต สุขภาพ หรือทรัพย์สินของบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลเป็นการยากเท่าที่จำเป็น

---

[74] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 15. หน้า 1.

[75] Onetrust Data Guidance

3) มีความจำเป็นสำหรับการพัฒนาด้านสาธารณสุขและสุขอนามัย หรือการส่งเสริม การเลี้ยงดูที่ดีและการได้รับความยินยอมจากผู้ปกครองหรือบิดา มารดานั้นทำได้ยาก เท่าที่จำเป็น ซึ่งจะเห็นได้ว่าสำหรับกฎหมายในเรื่องการแบ่งปันข้อมูลส่วนบุคคลในประเทศญี่ปุ่นนั้น ถือได้ว่ามีหลักการคือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อน แต่อย่างไรก็ตาม หากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถาการณ์นั้นที่เกิดเหตุขึ้น[76]

3.2.4 กฎหมายของประเทศแคนาดา

3.2.4.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศแคนาดา

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2 ฉบับ คือ Privacy Act ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลในความครอบครองของหน่วยงานของรัฐ กับ Personal Information Protection and Electronic Document Act (PIPEDA) ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลในความครอบครองของเอกชนและมีเอกสารอิเล็กทรอนิกส์ด้วย ดังนั้น จึงได้ศึกษาเฉพาะหลักกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองของเอกชนซึ่งอยู่ใน Part 1 ของ PIPEDA ดังนี้

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) ซึ่งเป็นกฎหมายของรัฐบาลกลางแคนาดาที่มีผลบังคับใช้ในการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลในระหว่างการทำกิจกรรมทางการค้าในทุกจังหวัดของแคนาดา โดยมีกฎหมายความเป็นส่วนตัวที่คล้ายกันช่วยเติมเต็มในอัลเบอร์ตา บริติชโคลัมเบีย และควิเบก นอกจากนี้ PIPEDA ยังบังคับใช้กับการโอนย้ายข้อมูลส่วนบุคคลระหว่างประเทศและระหว่างจังหวัดอีกด้วย เนื่องจาก AWS ไม่สามารถมองเห็นหรือรับทราบเกี่ยวกับสิ่งที่ลูกค้าอัปโหลดไปยังเครือข่ายนั้นได้ ไม่ว่าข้อมูลดังกล่าวถือว่าอยู่ภายใต้กฎหมาย PIPEDA หรือไม่ ลูกค้าจึงมีความรับผิดชอบต่อการปฏิบัติตามกฎหมาย PIPEDA ของตนเอง

PIPEDA หรือ Canadian law relating to data privacy เป็นข้อกำหนดที่เกิดขึ้นและจะต้องปฏิบัติตามกฎหมายในประเทศแคนาดา โดย PIPEDA นี้จะถูกนำมาใช้ภายใต้องค์กรต่างๆ ในประเทศ ซึ่งสามารถแบ่งออกอย่างง่ายๆ ได้ 2 ประเภท คือ

---

[76] พงษ์มนัส ดีอด และคณะ. (2566). ***รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/article/article-4/

1) องค์กรเอกชนที่มีการเก็บข้อมูลส่วนบุคคล นำข้อมูลส่วนบุคคลไปใช้ ตลอดจนการเปิดเผยข้อมูลส่วนบุคคลตามกิจกรรมเชิงพาณิชย์ ที่ซึ่งกฎหมายระบุเอาไว้ว่า เป็นการทำธุรกรรมใดๆ ที่มีลักษณะเกี่ยวข้องกับการค้าขาย แลกเปลี่ยน การเช่า รวมถึงการเป็นสมาชิกในการระดมทุน

2) องค์กรต่างๆ ที่ทำงานอยู่ภายใต้รัฐบาลกลางของประเทศแคนาดา ไม่ว่าจะเป็นสนามบิน ท่าอากาศยาน สายการบิน ธนาคาร บริษัทขนส่งระหว่างเขตหรือระหว่างประเทศ บริษัทที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม ตลอดจนวิทยุและโทรทัศน์องค์กรที่ว่ามาทั้งหมดนี้ หากจะต้องดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จะต้องได้รับการยินยอมจากเจ้าของข้อมูลเสียก่อน ซึ่งข้อมูลส่วนบุคคลจะนำมาใช้ได้ตามจุดประสงค์ที่ระบุไว้ตอนขอเก็บข้อมูลเท่านั้น หากจะนำไปใช้ในจุดประสงค์อื่นๆ จะต้องขอความยินยอมใหม่ และรายละเอียดต่างๆ ของข้อมูลที่เจ้าของข้อมูลให้ไปนั้นจะต้องได้รับการป้องกันอย่างเหมาะสม ที่สำคัญเจ้าของข้อมูล หรือประชาชนในประเทศแคนาดามีสิทธิ์ที่จะตรวจสอบความปลอดภัยในการเข้าถึงข้อมูลส่วนบุคคลเหล่านั้นได้อีกด้วยอนึ่ง PIPEDA มีหลักการที่เป็นหัวใจหลักๆ ของกฎหมายอยู่ 10 ข้อ[77]

(1) องค์กรต่างๆ มีหน้าที่รับผิดชอบต่อข้อมูลส่วนบุคคลภายใต้การควบคุมขององค์กร

(2) การเก็บข้อมูลทุกครั้งจะต้องมีจุดประสงค์ที่ชัดเจน

(3) ต้องมีการยินยอมจากเจ้าของข้อมูลในการเก็บ ใช้ และเปิดเผย ข้อมูลส่วนตัว

(4) ข้อมูลที่ใช้ได้ต้องเป็นไปตามจุดประสงค์ที่ขอความยินยอมในตอนแรก ถ้าจะใช้มากกว่านั้นต้องขอใหม่

(5) ต้องเก็บข้อมูลไว้จนกว่าจะบรรลุจุดประสงค์ตามที่ขอยินยอม

(6) ข้อมูลต้องถูกรักษาอย่างปลอดภัยและอัปเดตเท่าที่เป็นไปได้

(7) ต้องได้รับการป้องกันที่เหมาะสมกับระดับความอ่อนไหวของข้อมูล

(8) ต้องมีนโยบายที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลบอกแก่สาธารณะ

(9) เมื่อมีการเรียกร้องต้องเปิดให้ดู

---

[77] พงษ์มนัส ดีอด และคณะ. (2566). ***รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/article/article-4/

(10) บุคคลสามารถตรวจสอบความปลอดภัยของข้อมูลได้ทุกเมื่อตามที่ต้องการ[78]

Personal Information Protection and Electronic Documents Act (PIPEDA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ หรือ (PIPEDA) เป็นกฎหมายของรัฐบาลกลางแคนาดาที่เกี่ยวข้องกับความเป็นส่วนตัวของข้อมูล และมีบทบัญญัติต่างๆ เพื่ออำนวยความสะดวกในการใช้เอกสารอิเล็กทรอนิกส์

PIPEDA เริ่มใช้ครั้งแรกเมื่อวันที่ 13 เมษายน พ.ศ. 2543 และมีผลบังคับใช้เป็นขั้นๆ โดยเริ่มตั้งแต่วันที่ 1 มกราคม พ.ศ. 2544 และขยายไปยังองค์กรต่างๆ ในแคนาดาตั้งแต่วันที่ 1 มกราคม พ.ศ. 2547 PIPEDA ซึ่งเป็นที่รู้จักในปัจจุบัน ควบคุมวิธีที่ธุรกิจในแคนาดาสามารถรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ในการดำเนินกิจกรรมเชิงพาณิชย์ ทั่วทั้งแคนาดา PIPEDA ยังนำไปใช้กับข้อมูลส่วนบุคคลที่ข้ามพรมแดนระดับจังหวัดหรือระดับประเทศ โดยไม่คำนึงว่าข้อมูลดังกล่าวจะอาศัยอยู่ในจังหวัดหรือเขตแดนใด

3.2.4.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ข้อกำหนดการแจ้งเตือนการละเมิดข้อมูล

ข้อกำหนดการแจ้งเตือนการละเมิดภายใต้ PIPEDA มีผลบังคับใช้เมื่อวันที่ 1 พฤศจิกายน 2018 ขณะนี้องค์กรจำเป็นต้องแจ้งให้บุคคล OPC และองค์กรอื่นๆ ทราบเกี่ยวกับการละเมิดข้อมูล เช่น องค์กรบังคับใช้กฎหมายหรือองค์กรที่ประมวลผลการชำระเงิน การแจ้งเตือนการละเมิดจะต้องเกิดขึ้นโดยเร็วที่สุดหลังจากที่องค์กรพิจารณาว่ามีการละเมิดเกิดขึ้นภายใต้ PIPEDA องค์กรต่างๆ จะต้องเก็บรักษาบันทึกการละเมิดข้อมูลทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (สค. 2543, ค. 5)

ส่วนที่ 1 การคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชน (ต่อ)

ส่วนที่ 1.1 การละเมิดการป้องกันความปลอดภัย

รายงานต่อ Commissioner

10.1 (1) องค์กรต้องรายงานต่อคณะกรรมาธิการถึงการละเมิดมาตรการรักษาความปลอดภัยใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุม หากมีเหตุอันสมควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงจริง ๆ ที่จะก่อให้เกิดอันตรายร้ายแรงต่อบุคคล[79]

---

[78] สุธาทิพย์ อุปสุข. (2566). ***'เท่าที่เราจะอนุญาต' ชวนสำรวจ PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยและต่างแดน.*** (ออนไลน์). เข้าถึงได้จาก: https://creativetalklive.com/global-gpda-privacy-law/

[79] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

ข้อกำหนดของรายงาน

(2) รายงานจะต้องมีข้อมูลที่กำหนดและต้องทำในรูปแบบและวิธีการที่กำหนดโดยเร็วที่สุดหลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[80]

การแจ้งเตือนไปยังบุคคล

(3) เว้นแต่กฎหมายจะห้ามไว้เป็นอย่างอื่น องค์กรต้องแจ้งให้บุคคลหนึ่งทราบถึงการละเมิดมาตรการรักษาความปลอดภัยใดๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลภายใต้การควบคุมขององค์กร หากมีเหตุอันควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงอย่างแท้จริงต่ออันตรายที่มีนัยสำคัญต่อเฉพาะบุคคล.[81]

เนื้อหาของการแจ้งเตือน

(4) การแจ้งเตือนจะต้องมีข้อมูลที่เพียงพอเพื่อให้บุคคลเข้าใจถึงความสำคัญของการละเมิดและดำเนินการ (หากเป็นไปได้) เพื่อลดความเสี่ยงของอันตรายที่อาจเกิดขึ้นจากการละเมิดหรือเพื่อบรรเทาอันตรายนั้น ให้ประกอบด้วยข้อมูลอื่นที่กำหนดด้วย[82]

รูปแบบและลักษณะ

(5) การแจ้งต้องเห็นได้ง่ายและแจ้งแก่บุคคลนั้นโดยตรงตามแบบและลักษณะที่กำหนด เว้นแต่ในกรณีที่กำหนดไว้ให้แจ้งโดยอ้อมตามแบบและลักษณะที่กำหนด[83]

PART 1 Protection of Personal Information in the Private Sector (continued)

DIVISION 1.1 Breaches of Security Safeguards Report to Commissioner

10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

[80] Report requirements

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

[81] Notification to individual

(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

[82] Contents of notification

(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.

[83] Form and manner

ระยะเวลาการแจ้งเตือน

(6) การแจ้งเตือนจะได้รับทันทีที่ทำได้หลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[84]

คำจำกัดความของอันตรายที่มีนัยสำคัญ

(7) สำหรับวัตถุประสงค์ของมาตรานี้ อันตรายที่มีสาระสำคัญรวมถึงการทำร้ายร่างกาย ความอัปยศอดสู ความเสียหายต่อชื่อเสียงหรือความสัมพันธ์ การสูญเสียการจ้างงาน โอกาสทางธุรกิจหรืออาชีพ การสูญเสียทางการเงิน การขโมยข้อมูลประจำตัว ผลกระทบในทางลบต่อประวัติเครดิต และความเสียหายต่อหรือสูญหาย ของทรัพย์สิน.[85]

ความเสี่ยงที่แท้จริงของอันตรายที่มีนัยสำคัญ - ปัจจัยต่างๆ

(8) ปัจจัยที่เกี่ยวข้องในการพิจารณาว่าการละเมิดมาตรการรักษาความปลอดภัยก่อให้เกิดความเสี่ยงอย่างแท้จริงต่ออันตรายต่อบุคคลหรือไม่ ได้แก่

(a) ความละเอียดอ่อนของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด;

(b) ความเป็นไปได้ที่ข้อมูลส่วนบุคคลจะถูกนำไปใช้ หรือจะถูกนำไปใช้ในทางที่ผิด; และ

(c) ปัจจัยที่กำหนดอื่นใด[86]

2558 ค. 32, ส. 10

---

(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.

[84] Time to give notification

(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

[85] Definition of *significant harm*

(7) For the purpose of this section, *significant harm* includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

[86] Real risk of significant harm — factors

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information involved in the breach;

(b) the probability that the personal information has been, is being or will be misused; and

(c) any other prescribed factor.

การแจ้งเตือนไปยังองค์กร

10.2 (1) องค์กรที่แจ้งบุคคลเกี่ยวกับการละเมิดการป้องกันความปลอดภัยภายใต้หัวข้อย่อย 10.1(3) จะต้องแจ้งองค์กรอื่น สถาบันของรัฐ หรือส่วนหนึ่งของสถาบันของรัฐเกี่ยวกับการละเมิด หากองค์กรที่แจ้งเตือนเชื่อว่าองค์กรอื่น หรือหน่วยงานของรัฐหรือหน่วยงานที่เกี่ยวข้องอาจสามารถลดความเสี่ยงของอันตรายที่อาจเป็นผลจากอันตรายนั้นหรือบรรเทาอันตรายนั้นลงได้ หรือหากเป็นไปตามเงื่อนไขที่กำหนดไว้[87]

ระยะเวลาแจ้งเตือน

(2) การแจ้งเตือนจะได้รับทันทีที่ทำได้หลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[88]

การเปิดเผยข้อมูลส่วนบุคคล

(3) นอกเหนือจากสถานการณ์ที่กำหนดไว้ในส่วนย่อย 7(3) เพื่อวัตถุประสงค์ของข้อ 4.3 ของตารางที่ 1 และแม้จะมีหมายเหตุที่มาพร้อมกับข้อนั้น องค์กรอาจเปิดเผยข้อมูลส่วนบุคคลโดยที่บุคคลนั้นไม่ทราบหรือยินยอม ถ้า

(ก) มีการเปิดเผยต่อองค์กรอื่น สถาบันของรัฐ หรือส่วนหนึ่งของสถาบันของรัฐที่ได้รับแจ้งการละเมิดภายใต้มาตราย่อย (1) และ

(b) การเปิดเผยนี้จัดทำขึ้นเพื่อจุดประสงค์ในการลดความเสี่ยงของอันตรายต่อบุคคลซึ่งอาจเป็นผลมาจากการละเมิดหรือบรรเทาอันตรายนั้นเท่านั้น[89]

---

[87] Notification to organizations

10.2 (1) An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

[88] Time to give notification

(2) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

[89] Disclosure of personal information

(3) In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if

การเปิดเผยโดยไม่ได้รับความยินยอม

(4) แม้จะมีข้อ 4.5 ของตาราง 1 องค์กรอาจเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่รวบรวมไว้ในสถานการณ์ที่กำหนดไว้ในหัวข้อย่อย (3)

(2015, ค. 32, น. 10.)[90]

บันทึก

10.3 (1) ตามข้อกำหนดที่กำหนดไว้ องค์กรจะต้องเก็บและเก็บรักษาบันทึกการละเมิดมาตรการรักษาความปลอดภัยที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุมขององค์กร

ข้อกำหนดให้ผบ.ตร

(2) องค์กรต้องจัดให้มีการเข้าถึงหรือสำเนาบันทึกแก่คณะกรรมาธิการเมื่อได้รับการร้องขอ (2558, ค. 32, น. 10)[91]

จากการศึกษาข้อมูลข้างต้น และพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พบว่าในต่างประเทศมีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล โดยสามารถสรุปข้อมูลได้ดังต่อไปนี้

1) สหภาพยุโรป

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU: European Union) หรือ General data Protection Regulation (GDPR) ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยการแจ้งในกรณีที่มีการละเมิดข้อมูลส่วน

(a) the disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and

(b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

[90] Disclosure without consent

(4) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3).

[91] Records

10.3 (1) An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

Provision to Commissioner

(2) An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.

บุคคลต้องแจ้งต่อหน่วยงานที่มีหน้าที่กำกับดูแลภายใต้อำนาจตามมาตรา 55 เว้นแต่การละเมิดข้อมูลส่วนบุคคลจะไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ในกรณีที่การแจ้งเตือนไปยังหน่วยงานที่มีหน้าที่กำกับดูแล ไม่ได้ดำเนินการภายใน 72 ชั่วโมงจะต้องมีให้เหตุผลสำหรับเหตุที่เกิดความล่าช้า และหน่วยงานประมวลผลข้อมูลจะต้องแจ้งให้ผู้ตรวจสอบทราบโดยไม่ชักช้าหลังจากรับเหตุการละเมิดข้อมูลส่วนบุคคล

อย่างไรก็ดี ตามหลักการที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR มีการขยายความชัดเจนในเรื่องนี้ออกไปอีกโดยผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ช่วงระยะเวลาไม่นานในการตรวจสอบข้อเท็จจริงและทำการยืนยันว่าเหตุละเมิดข้อมูลส่วนบุคคลที่พบหรือรับแจ้งนั้น ได้เกิดขึ้นจริงหรือไม่ และภายในช่วงระยะเวลาไม่นานนั้นยังถือไม่ได้ว่าบริษัทฯได้ “รับทราบ” การละเมิดข้อมูลส่วนบุคคลแล้ว

2) สาธารณรัฐสิงคโปร์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ Personal Data Protection Act: PDPA โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสิงคโปร์หรือไม่ ถือว่าอยู่ภายใต้กฎหมายดังกล่าว ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลต้องได้รับความยินยอม จากเจ้าของข้อมูลก่อนทำการเก็บบันทึก การใช้ และการเปิดเผยข้อมูลส่วนบุคคล และจะต้องใช้ข้อมูลนั้น เพื่อวัตถุประสงค์ตามที่แจ้งเท่านั้น รวมถึงจะต้องจัดให้เจ้าของข้อมูลเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลได้ และจะต้องยุติหรือหยุดการจัดเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็น ทั้งนี้ กรณีของสาธารณรัฐสิงคโปร์ในหลักของความยินยอม กฎหมายกำหนดให้การทำความยินยอมควรจะทำ เป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ และเจ้าของข้อมูลสามารถถอนหรือยกเลิกการให้ ความยินยอมในการใช้ข้อมูลเมื่อใดก็ได้ด้วยการแจ้งต่อองค์กรที่จัดเก็บข้อมูลประกอบเหตุผลในการถอน ความยินยอม

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลจะต้องมีการจัดการเพื่อรักษาความปลอดภัยอย่างเหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคล และเพื่อป้องกัน การเข้าถึง การจัดเก็บ การใช้การเปิดเผย การคัดลอก การแก้ไข การลบข้อมูลหรือความเสี่ยงอื่นในทำนอง เดียวกัน ซึ่งกระทำโดยมิชอบด้วยกฎหมาย ในส่วนของ สิทธิใน

การร้องเรียนต่อคณะกรรมการด้านข้อมูลส่วนบุคคลเป็นมาตรการเยียวยาเจ้าของข้อมูล จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย

3) ประเทศญี่ปุ่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น หรือ Act on the Protection of Personal Information: APPI โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูล ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงการละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์ ทั้งนี้ ต้องแจ้งโดยไม่ชักช้าตามวิธีการที่คณะรัฐมนตรีกำหนด และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PPC) มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษาอีกด้วย

4) ประเทศแคนาดา

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการ ถึงการละเมิดมาตรการรักษาความปลอดภัยใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุม หากมีเหตุอันสมควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงจริง ๆ ที่จะก่อให้เกิดอันตรายร้ายแรงต่อบุคคล โดยการละเมิดจะต้องเกิดขึ้นโดยเร็วที่สุดหลังจากที่องค์กรพิจารณาว่ามีการละเมิดเกิดขึ้นภายใต้ PIPEDA องค์กรต่างๆ จะต้องเก็บรักษาบันทึกการละเมิดข้อมูลทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ตารางที่ 2 ตารางการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของกฎหมายต่างประเทศ

ประเทศ	การแจ้งเหตุละเมิด
สหภาพยุโรป	แจ้งเหตุเมื่อพบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
สาธารณรัฐสิงคโปร์	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งบังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสิงคโปร์ หรือมีถิ่นที่อยู่ในสิงคโปร์หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้
ประเทศญี่ปุ่น	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เพียงแต่กำหนดหลักเกณฑ์ไว้ว่า จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่
ประเทศแคนาดา	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

ทั้งนี้ จากการศึกษากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของประเทศไทย และต่างประเทศ ในส่วนบทบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้น มีหลักการที่สำคัญที่ยังคงยังคงประสบปัญหากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเป็นปัญหาการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงปัญหาบทลงโทษทางอาญา จึงจำเป็นต้องมีการแก้ไขเพิ่มเติมกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อไป