บททั่วไป

ภาพรวมกฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ”) ได้มีการประกาศบังคับใช้อย่างเต็มรูปแบบในวันที่ 1 มิถุนายน พ.ศ. 2565 และได้มีการออกประกาศกฎหมายลำดับรองออกมากำหนดรายละเอียด ในเรื่องต่าง ๆ เช่น มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565 และหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เป็นต้น

โดยแนวปฏิบัตินี้จะกล่าวถึงแนวทางการคุ้มครองข้อมูลส่วนบุคคลสำหรับหน่วยงานภาครัฐและภาคเอกชนตามแต่ละกลุ่มอุตสาหกรรมในการดำเนินการให้สอดคล้องกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

[Material Scope] ก่อนการพิจารณาหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล พึงต้องพิจารณาขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลว่าหน่วยงานหรือองค์กรมีหน้าที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ตามมาตรา 4 ที่ว่าด้วยขอบเขตการบังคับใช้เชิงเนื้อหา (Material Scope) ดังนี้

1) การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3) กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
4) การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว
5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต
7) ลักษณะ กิจการ หรือหน่วยงาน ตามที่กำหนดในพระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ บางส่วนมาใช้บังคับ

[Territorial Scope] นอกจากนี้ ในเชิงพื้นที่ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ในกรณีต่อไปนี้

1) ผู้ประกอบการมีบริษัทหรือสาขาที่จัดตั้งในประเทศไทย ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะเกิดขึ้นในประเทศไทยหรือไม่ก็ตาม
2) ผู้ประกอบการที่ไม่มีบริษัทหรือสาขาที่จัดตั้งในประเทศไทย แต่
    - เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลในประเทศไทยไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม หรือ
    - มีการติดตามและจัดเก็บข้อมูลพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลในประเทศไทย ตราบเท่าที่พฤติกรรมที่จัดเก็บนั้นเกิดขึ้นในประเทศไทย

อย่างไรก็ดี แม้หน่วยงานหรือองค์กรจะได้รับยกเว้นไม่ให้นำพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาบังคับใช้ตามมาตรา 4 แล้ว แต่หน่วยงานหรือองค์กรก็ยังคงมีหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย

2. ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลภายใต้พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ โดยภายใต้แนวปฏิบัตินี้ได้แบ่งข้อมูลส่วนบุคคลออกเป็น 2 ประเภท ได้แก่ ข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลอ่อนไหว

2.1 ข้อมูลส่วนบุคคลทั่วไป

ข้อมูลส่วนบุคคลทั่วไป หมายถึง ข้อมูลซึ่งสามารถสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตัวอย่างเช่น ชื่อ นามสกุล ที่อยู่ ที่อยู่อีเมล เบอร์โทรศัพท์ หมายเลขบัตรประจำตัวประชาชน หมายลขหนังสือเดินทาง IP Address (เมื่อระบุตัวตนได้) Cookie ID Device ID ข้อมูลตำแหน่ง (Location) รูปภาพ เสียง (ที่ระบุตัวตนได้) ทะเบียนรถ หมายเลขบัญชีธนาคาร เป็นต้น

[นิยามอย่างกว้างข้อมูลส่วนบุคคล] ข้อมูลส่วนบุคคลไม่ได้จำกัดอยู่เพียงชื่อ นามสกุล หรือเลขบัตรประชาชน ในความเป็นจริงแล้ว ข้อมูลที่ดูเหมือนไม่มีความอ่อนไหว เช่น วันเกิด เพศ และรหัสไปรษณีย์ เมื่อนำมารวมกันกลับสามารถระบุตัวตนของบุคคลได้อย่างแม่นยำ หรือบางกรณี แม้ข้อมูลจะถูก ถอดรหัสระบุ

ตัวตน (De-identification) ไปแล้ว ก็ยังสามารถถูกเชื่อมโยงกลับ (Re-identification) เพื่อระบุตัวบุคคลได้ผ่านสิ่งที่เรียกว่า Quasi-identifier หรือ ตัวบ่งชี้ทางอ้อม ซึ่งหมายถึงชุดข้อมูลที่แม้แต่ละตัวจะดูไม่สำคัญ แต่เมื่อรวมกันแล้วกลับทำหน้าที่เสมือน "ลายนิ้วมือดิจิทัล" ของแต่ละบุคคล

สังคมปัจจุบันมีการเก็บสะสมข้อมูลเชิงบุคคลในปริมาณมหาศาลและกระจายอยู่ในฐานข้อมูลจำนวนมาก เมื่อข้อมูลเหล่านี้ถูกเชื่อมโยงเข้าด้วยกัน มันจะสร้างเงาอิเล็กทรอนิกส์ (electronic shadow) ของบุคคลที่สามารถระบุตัวตนได้อย่างชัดเจน เปรียบเสมือนลายนิ้วมือ แม้ว่าข้อมูลนั้นจะไม่มีชื่อหรือหมายเลขโทรศัพท์อยู่เลยก็ตาม

ข้อมูลเพียง 3 ประเภทระบุตัวคนอเมริกันได้ 87%

นักวิจัยได้ใช้ข้อมูลสำมะโนประชากรสหรัฐฯ ปี 1990 วิเคราะห์พบว่า ด้วยข้อมูลเพียง 3 ประเภท คือ รหัสไปรษณีย์ 5 หลัก เพศ และวันเดือนปีเกิดก็สามารถระบุตัวตนได้ถึง 87% ของประชากรสหรัฐฯ หากใช้เพียงข้อมูลเมืองที่อยู่อาศัย ประกอบกับเพศและวันเกิดก็ระบุตัวตนได้ 53% และแม้จะใช้แค่ข้อมูลอำเภอ ประกอบกับเพศและวันเกิดก็ยังระบุได้ถึง 18% ของประชากรทั้งหมด[1]

2.2 ข้อมูลส่วนบุคคลอ่อนไหว

ข้อมูลส่วนบุคคลอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด[2]

ทั้งนี้ การพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลอ่อนไหวหรือไม่ ต้องคำนึงถึงวัตถุประสงค์และวิธีการประมวลผลเป็นสำคัญ ไม่ใช่เพียงรูปแบบหรือประเภทของข้อมูลที่ปรากฏเท่านั้น กล่าวคือข้อมูลส่วนบุคคลนั้นถูกประมวลผลด้วยวัตถุประสงค์ในลักษณะที่อาจส่งผลต่อการเลือกปฏิบัติแก่เจ้าของข้อมูลส่วนบุคคล และหากเป็นข้อมูลชีวภาพจะต้องมีการใช้เทคนิคหรือเทคโนโลยีเพื่อทำให้สามารถยืนยันตัวตนของบุคคลได้

นอกจากนี้ ผลของการประมวลผลเป็นอีกหนึ่งปัจจัยที่ต้องพิจารณา กล่าวคือ ข้อมูลส่วนบุคคลที่ถูกนำไปใช้อนุมานลักษณะอ่อนไหวของบุคคลย่อมถือเป็นข้อมูลส่วนบุคคลอ่อนไหวเช่นกัน แม้ข้อมูลต้นทางจะไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหวโดยตรง ตัวอย่างเช่น ข้อมูลธุรกรรมทางการเงินซึ่งโดยปกติเป็นเพียงข้อมูลส่วนบุคคลทั่วไป แต่หากธุรกรรมนั้นเปิดเผยได้ว่าบุคคลบริจาคเงินให้พรรคการเมืองหรือองค์กรศาสนา ข้อมูล

[1] Latanya Sweeney, Computational disclosure control : a primer on data privacy protection, 2001, http://dspace.mit.edu/handle/1721.1/8589

[2] มาตรา 26 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ดังกล่าวก็มีผลเท่ากับการเปิดเผยความคิดเห็นทางการเมืองหรือความเชื่อทางศาสนาของบุคคลนั้น และต้องได้รับการคุ้มครองในฐานะข้อมูลส่วนบุคคลอ่อนไหวแม้ข้อมูลต้นทางจะไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหวโดยตรง[3]

2.2.1 นิยามและหลักการพิจารณาข้อมูลส่วนบุคคลอ่อนไหวแต่ละประเภท

2.2.1.1 เชื้อชาติ เผ่าพันธุ์ (Racial and Ethnic Origin)

เชื้อชาติ (Racial Origin) หมายถึง ลักษณะทางสายเลือดหรือกำเนิด ซึ่งครอบคลุมถึงข้อมูลที่เปิดเผยหรือบ่งชี้เชื้อชาติ (personal data revealing racial origin)[4] ไม่ใช่เพียงข้อมูลที่ระบุโดยตรง ทั้งนี้ ข้อมูลต่อไปนี้อาจเข้าข่ายเป็นข้อมูลเชื้อชาติโดยอ้อม หากถูกนำไปใช้เพื่ออนุมานเชื้อชาติของบุคคล

- ชื่อหรือนามสกุลที่มีลักษณะเฉพาะของกลุ่มชาติพันธุ์
- ข้อมูลสัญชาติ ภาษาแม่ หรือถิ่นกำเนิด ในบริบทที่ใช้เพื่อจัดหมวดหมู่เชื้อชาติ

ในทำนองเดียวกัน เผ่าพันธุ์ (Ethnic Origin) ก็ครอบคลุมข้อมูลที่เปิดเผยหรือบ่งชี้ เผ่าพันธุ์ (personal data revealing ethnic origin) เช่นกัน โดยเผ่าพันธุ์ หมายถึงกลุ่มที่มีวัฒนธรรม ประเพณี หรือภาษาร่วมกันเฉพาะ เช่น กลุ่มชาติพันธุ์ชนกลุ่มน้อย เป็นต้น[5]

2.2.1.2 ความคิดเห็นทางการเมือง (Political Opinions)

ข้อมูลความคิดเห็นทางการเมืองมีขอบเขตที่กว้าง เนื่องจากไม่จำกัดเพียงข้อมูลที่เจ้าของข้อมูลส่วนบุคคลแสดงออกหรือระบุด้วยตนเองเท่านั้น แต่ครอบคลุมถึงข้อมูลที่ได้รับจากบุคคลที่สาม และข้อมูลที่ได้จากการอนุมานแล้วนำมาเชื่อมโยงกับบุคคลนั้น[6] กล่าวคือ แม้บุคคลจะไม่เคยเปิดเผยความคิดเห็นทางการเมืองของตนโดยตรง แต่หากมีการนำข้อมูลอื่นมาใช้อนุมานจุดยืนดังกล่าว ข้อมูลที่ได้ก็ถือเป็นข้อมูลความคิดเห็นทางการเมืองเช่นกัน

หลักการดังกล่าวมีนัยสำคัญในทางปฏิบัติ เนื่องจากทำให้ขอบเขตของข้อมูลความคิดเห็นทางการเมืองขยายออกไปครอบคลุมข้อมูลที่ดูเหมือนเป็นกลางในตัวเอง เช่น พฤติกรรมการบริโภคสื่อ รูปแบบการบริจาค หรือข้อมูลตำแหน่งที่อยู่ เป็นต้น หากข้อมูลเหล่านั้นถูกนำมาประมวลผลเพื่ออนุมาน

---

[3] EDPB, Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR, Version 2.0 (15 December 2020), para. 53.

[4] GDPR, Article 9(1)

[5] GDPR, Recital 51

[6] ICO, Guidance on Political Campaigning — Can political parties process political opinions?, UK GDPR Article 9(2)(g)

ความเชื่อทางการเมืองของบุคคล การประมวลผลนั้นย่อมอยู่ภายใต้บังคับของมาตรการคุ้มครองข้อมูลส่วนบุคคลอ่อนไหวทันที ข้อมูลต่อไปนี้อาจเปิดเผยความคิดเห็นทางการเมืองโดยอ้อม

- ประวัติการลงคะแนนเสียง หรือการเป็นสมาชิกพรรคการเมือง
- ธุรกรรมการบริจาคให้พรรคการเมืองหรือองค์กรที่มีแนวทางทางการเมือง
- พฤติกรรมการบริโภคสื่อที่ถูกนำไปอนุมานจุดยืนทางการเมือง

อย่างไรก็ตาม ก่อนนำมาตรา 26 มาใช้ ต้องตรวจสอบก่อนว่าข้อมูลนั้นเป็นข้อมูลส่วนบุคคลตามมาตรา 6 หรือไม่ ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น สถิติรวมจำนวนสมาชิกพรรค หรือสัดส่วนผู้มาใช้สิทธิโดยไม่ระบุชื่อ ไม่อยู่ภายใต้การคุ้มครองของกฎหมาย สำหรับข้อมูลที่ระบุตัวบุคคลได้ เช่น บัญชีรายชื่อผู้มีสิทธิเลือกตั้ง การที่จะเป็นข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 ขึ้นอยู่กับวัตถุประสงค์ที่ผู้ควบคุมข้อมูลส่วนบุคคลนำไปประมวลผล ข้อยกเว้นเดียวที่อาจพ้นจากข้อห้ามตามมาตรา 26 คือข้อมูลสังกัดพรรคของผู้สมัครรับเลือกตั้งที่เปิดเผยต่อสาธารณะโดยสมัครใจ ซึ่งไม่ครอบคลุมสมาชิกพรรคหรือผู้มีสิทธิทั่วไป

2.2.1.3 ความเชื่อในลัทธิ ศาสนา หรือปรัชญา (Religious or Philosophical Beliefs)

ความเชื่อในลัทธิ ศาสนา หรือปรัชญา ครอบคลุมข้อมูลที่เปิดเผยหรือบ่งชี้ความเชื่อของบุคคลในมิติดังกล่าว โดยไม่จำกัดเฉพาะศาสนาหลักที่เป็นที่รู้จักทั่วไป แต่ขยายออกไปถึงความเชื่อทางโลกที่มีน้ำหนักและความจริงจังในระดับเดียวกัน เช่น แนวคิดสันติวิธี (Pacifism) แนวคิดสังคมนิยม (Socialism) รวมถึงการไม่นับถือศาสนา (Atheism/Agnosticism) และการนับถือกลุ่มความเชื่อนอกกระแสหลัก เช่น ลัทธิธรรมชาติหรือมานุษยปรัชญา (Anthroposophy) ความเชื่อในเรื่องการเปลี่ยนแปลงสภาพภูมิอากาศ (belief in climate change)[7] เช่นเดียวกับข้อมูลส่วนบุคคลอ่อนไหวประเภทอื่น ขอบเขตของข้อมูลประเภทนี้ไม่จำกัดเพียงข้อมูลที่ระบุความเชื่อโดยตรง แต่ครอบคลุมถึงข้อมูลที่ "เปิดเผยหรือบ่งชี้" ความเชื่อดังกล่าวโดยอ้อมด้วย โดยขยายความว่าหากมีการนำข้อมูลที่สังเกตได้มาใช้จัดหมวดหมู่ผู้ใช้ว่ามีความเชื่อในลัทธิ ศาสนา หรือปรัชญา ไม่ว่าการจัดหมวดหมู่นั้นจะถูกต้องหรือไม่ก็ตาม ถือเป็นการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวทันที

นอกจากนี้ ข้อมูลที่ดูเป็นกลางในตัวเองก็อาจเข้าข่ายเป็นข้อมูลส่วนบุคคลอ่อนไหวได้ หากถูกนำไปใช้เพื่ออนุมานความเชื่อทางศาสนาหรือปรัชญาของบุคคล ตัวอย่างเช่น ธุรกรรมการบริจาคให้โบสถ์ มัสยิด หรือองค์กรศาสนา ชื่อบุคคลหรือรูปแบบการแต่งกายก็อาจเชื่อมโยงกับศาสนาเฉพาะได้ และหากนำไปใช้เพื่ออนุมานความเชื่อทางศาสนา ข้อมูลนั้นย่อมถือเป็นข้อมูลส่วนบุคคลอ่อนไหว

[7] WP29, Advice Paper on Special Categories of Data ("Sensitive Data").

2.2.1.4 พฤติกรรมทางเพศ (Sexual Behaviour)

พฤติกรรมทางเพศครอบคลุมข้อมูลที่เปิดเผยหรือบ่งชี้พฤติกรรม กิจกรรม หรือการแสดงออกทางเพศของบุคคล รวมถึงรสนิยมทางเพศและข้อมูลที่เกี่ยวกับชีวิตทางเพศ ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ใช้ถ้อยคำว่า "พฤติกรรมทางเพศ" ซึ่งมีขอบเขตกว้างกว่า GDPR Article 9(1) ที่บัญญัติเฉพาะ "data concerning a natural person's sex life or sexual orientation"[8] เช่นเดียวกับข้อมูลส่วนบุคคลอ่อนไหวประเภทอื่น ขอบเขตของข้อมูลประเภทนี้ไม่จำกัดเพียงข้อมูลที่ระบุพฤติกรรมทางเพศโดยตรง แต่ครอบคลุมถึงข้อมูลที่สามารถนำไปอนุมานลักษณะดังกล่าวได้โดยอ้อมด้วย ตัวอย่างเช่น ข้อความที่ระบุว่านาย X แต่งงานกับนาย Y ย่อมเปิดเผยข้อมูลรสนิยมทางเพศของบุคคลทั้งสองได้ชัดเจน[9] การเป็นผู้ใช้ที่ลงทะเบียนในแอปพลิเคชัน LGBTQ+ social networking app ถือเป็นข้อมูลส่วนบุคคลอ่อนไหวเกี่ยวกับรสนิยมทางเพศ[10]

ทั้งนี้ ข้อมูล "เพศ" ในเชิงทะเบียน (ชาย หญิง หรือ "ไม่ระบุเพศ") ไม่ถือเป็นพฤติกรรมทางเพศตามมาตรา 26 แต่เป็นข้อมูลส่วนบุคคลทั่วไปตามมาตรา 24 โดยตัวเลือก "ไม่ระบุเพศ" เป็นการใช้สิทธิไม่เปิดเผยข้อมูล จึงยิ่งไม่อาจตีความว่าบ่งชี้รสนิยมหรือพฤติกรรมทางเพศ อย่างไรก็ดี ข้อมูลเพศไม่ว่าค่าใด หากถูกนำไปอนุมานหรือจัดกลุ่มเพื่อบ่งชี้รสนิยมหรือพฤติกรรมทางเพศของบุคคล ย่อมกลายเป็นข้อมูลส่วนบุคคลอ่อนไหวตาม มาตรา 26

2.2.1.5 ประวัติอาชญากรรม (Criminal Records)

ประวัติอาชญากรรม หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับการสืบสวนสอบสวนการกระทำความผิดอาญา การดำเนินคดีอาญา หรือการรับโทษทางอาญา ที่เป็นข้อมูลที่ทางการหรือหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมายเกี่ยวกับการดำเนินการดังกล่าวรับรอง ทั้งนี้ ไม่ว่าการดำเนินการนั้นจะถึงที่สุดแล้วหรือไม่ก็ตาม[11]

ข้อมูลในการบันทึกประวัติอาชญากรรมจะบันทึกข้อมูลเฉพาะความผิดที่มีโทษทางอาญา เช่น ความผิดเกี่ยวกับชีวิตและร่างกาย ความผิดเกี่ยวกับทรัพย์ ความผิดเกี่ยวกับเพศ และ ความผิดเกี่ยวกับ

---

[8] GDPR, Article 9(1); พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ, มาตรา 26 วรรคหนึ่ง

[9] ICO, What is Special Category Data?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/

[10] Norwegian Data Protection Authority v. Grindr LLC, Case No. 20/02136-17.

[11] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566, ข้อ 3

การปลอมแปลงเอกสาร เป็นต้น โดยต้องมีประวัติอยู่ระหว่างการดำเนินคดีหรือมีประวัติจากการต้องโทษ ซึ่งสามารถอ้างอิงข้อมูลได้จากกองทะเบียนประวัติอาชญากรรม

ทั้งนี้ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566 ได้กำหนดหลักเกณฑ์สำคัญไว้ดังนี้

- วัตถุประสงค์ที่อนุญาต ได้แก่ (1) การพิจารณารับบุคคลเข้าทำงานหรือตรวจสอบคุณสมบัติสำหรับตำแหน่งใด (2) การตรวจสอบคุณสมบัติในการออกใบอนุญาตต่าง ๆ โดยหน่วยงานของรัฐหรือผู้ได้รับมอบหมาย และ (3) การตรวจสอบคุณสมบัติในการอนุญาตอื่น ๆ โดยผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น
- [ฐานทางกฎหมาย] ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานทางกฎหมายรองรับ และต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบตั้งแต่ขั้นตอนแรกของกระบวนการ
- [ระยะเวลาการเก็บรักษา] เมื่อประมวลผลเสร็จแล้วสามารถเก็บข้อมูลต่อได้ไม่เกิน 6 เดือน เว้นแต่มีกฎหมายกำหนดเป็นอย่างอื่นหรือมีฐานทางกฎหมายรองรับ

จากประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญา กรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566 ประวัติอาชญากรรมที่มีการบันทึกเกี่ยวกับโจทก์ถอนฟ้อง อัยการสั่งไม่ฟ้อง พิพากษาให้รอลงอาญา หรืออยู่ระหว่างการอุทธรณ์ ถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม แต่การที่จัดเก็บเอกสารที่ระบุว่า ไม่พบประวัติอาชญากรรม หรือข้อความอื่น ๆ ในทำนองเดียวกัน ไม่ถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ซึ่งการเก็บรวบรวมข้อมูลประวัติอาชญากรรมที่ไม่ต้องขอความยินยอม เช่น บันทึกการจับกุม บันทึกคำพิพากษา ฐานข้อมูลผู้ต้องขัง บันทึกการสอบสวน และฐานข้อมูลผู้ถูกคุมความประพฤติ แต่ข้อมูลที่ต้องขอความยินยอมโดยชัดแจ้ง เช่น บันทึกเหตุการณ์ทุจริตของพนักงานที่ถูกแจ้งความ เข้าข่ายข้อมูลส่วนบุคคลอ่อนไหวก่อนส่งข้อมูลไปตรวจสอบ และแบบฟอร์มสมัครงานที่ถามว่าเคยถูกดำเนินคดีอาญาหรือไม่ หากคำตอบของผู้สมัครคือใช่หรือไม่ จะเข้าข่ายเป็นข้อมูลส่วนบุคคลอ่อนไหว

ข้อควรพิจารณาเกี่ยวกับข้อมูลประวัติอาชญากรรม

- การบันทึกว่าพบประวัติอาชญากรรม แม้ไม่ได้ปรากฏข้อเท็จจริงหรือการรับโทษทางอาญา ถือได้ว่าเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม
- ข้อมูลอาชญากรรมที่กระทำต่อเหยื่อที่ระบุตัวตนได้ เป็นข้อมูลส่วนบุคคลของเหยื่อ แต่ไม่ถือเป็นข้อมูลความผิดทางอาญา จึงไม่เป็นข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม
- การบันทึกว่าไม่พบประวัติอาชญากรรม หรือ ข้อความอื่นในทำนองเดียวกัน ไม่ถือเป็นข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566
- หน่วยงาน ICO ของสหราชอาณาจักร ตีความว่า การไม่มีประวัติการกระทำความผิด ตัวเอกสารหรือตัวข้อมูลยังถูกจัดเป็นข้อมูลประวัติอาชญากรรม ซึ่งรวมไปถึงการยกฟ้องหรือการตัดสินว่าไม่มีความผิดในชั้นศาล[13]

2.2.1.6 ข้อมูลสุขภาพ ความพิการ (Health Data)

ข้อมูลสุขภาพ หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับสุขภาพกายหรือจิตใจของบุคคล รวมถึงการให้บริการสาธารณสุข ซึ่งเปิดเผยสถานะสุขภาพของบุคคลนั้น[14] และขยายความถึงข้อมูลทั้งหมดที่เกี่ยวกับสถานะสุขภาพของบุคคล ซึ่งเปิดเผยข้อมูลเกี่ยวกับสุขภาพกายหรือจิตใจในอดีต ปัจจุบัน หรืออนาคตของบุคคลนั้น[15] ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 26 วรรคหนึ่งบัญญัติครอบคลุมทั้งข้อมูลสุขภาพ ความพิการไว้ด้วยกัน ทั้งนี้ ข้อมูลสุขภาพครอบคลุมข้อมูลจากแหล่งต่อไปนี้

- **ข้อมูลจากกระบวนการรับบริการสุขภาพ:** ข้อมูลที่เก็บรวบรวมในระหว่างการลงทะเบียนหรือการรับบริการสาธารณสุข รายละเอียดนัดหมาย การแจ้งเตือน หรือใบแจ้งหนี้ที่เปิดเผยข้อมูลสุขภาพของบุคคล โดยต้องพิจารณาบริบทประกอบ ตัวอย่างเช่น นัดพบแพทย์หรือโรงพยาบาลเพียงครั้งเดียวอาจไม่เปิดเผยข้อมูลสุขภาพใด แต่รายชื่อนัดหมายที่คลินิกกายภาพบำบัดหรือใบแจ้งหนี้สำหรับการรักษาต่อเนื่องย่อมสามารถอนุมานข้อมูลสุขภาพได้อย่างสมเหตุสมผล[16]

[13] What is criminal offence data? | ICO Section 11(2) of the DPA 2018

[14] GDPR, Article 4(15)

[15] GDPR, Recital 35

[16] ICO, What is Special Category Data?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/; cf. GDPR, Recital 35

- **รหัสหรือสัญลักษณ์เพื่อระบุตัวตนทางสุขภาพ:** หมายเลข สัญลักษณ์ หรือรายการเฉพาะที่กำหนดให้กับบุคคลเพื่อระบุตัวตนในบริบทด้านสุขภาพ เช่น เลขที่ผู้ป่วย
- **ข้อมูลจากการตรวจทางการแพทย์:** ข้อมูลที่ได้จากการตรวจสอบหรือวิเคราะห์ส่วนหนึ่งส่วนใดของร่างกายหรือสารชีวภาพ รวมถึงข้อมูลพันธุกรรมและตัวอย่างชีวภาพ
- **ข้อมูลเกี่ยวกับสภาวะสุขภาพ ไม่ว่าจะมาจากแหล่งใด:** ได้แก่ ข้อมูลเกี่ยวกับโรค ความพิการ ความเสี่ยงต่อโรค ประวัติการรักษา การรักษาทางคลินิก หรือสภาวะทางสรีรวิทยาหรือชีวการแพทย์ ไม่ว่าจะได้มาจากแพทย์ ผู้เชี่ยวชาญด้านสุขภาพอื่น โรงพยาบาล อุปกรณ์การแพทย์ การทดสอบวินิจฉัย[17] หรือข้อมูลจาก fitness trackers[18]

2.2.1.7 ข้อมูลสหภาพแรงงาน (Trade Union Membership)

ข้อมูลสหภาพแรงงานครอบคลุมข้อมูลที่เปิดเผยการเป็นสมาชิกสหภาพแรงงานหรือองค์กรลูกจ้างของบุคคล รวมถึงข้อมูลที่ระบุการเป็นสมาชิกโดยตรง และข้อมูลที่สามารถเปิดเผยหรือบ่งชี้สถานะดังกล่าวโดยอ้อม เช่นเดียวกับข้อมูลส่วนบุคคลอ่อนไหวประเภทอื่น ขอบเขตของข้อมูลสหภาพแรงงานไม่จำกัดเพียงเอกสารหรือทะเบียนสมาชิกอย่างเป็นทางการเท่านั้น โดยปกติข้อมูลทางการเงินไม่ถือเป็นข้อมูลส่วนบุคคลอ่อนไหว แต่หากการเป็นสมาชิกสหภาพแรงงานสามารถอนุมานได้จากข้อมูลธุรกรรมการชำระเงิน เช่น การหักค่าสมาชิกสหภาพแรงงานรายปีจากบัญชีธนาคารของบุคคล ซึ่งแม้จะเป็นเพียงธุรกรรมทางการเงินธรรมดา แต่ย่อมเปิดเผยสถานะสมาชิกสหภาพแรงงานของบุคคลนั้นได้โดยอ้อม[19]

นอกจากนี้ ข้อมูลสหภาพแรงงานมีความอ่อนไหวเป็นพิเศษในบริบทของนายจ้างและลูกจ้าง เนื่องจากอาจนำไปสู่การเลือกปฏิบัติหรือกระทบต่อสิทธิในการรวมตัวของลูกจ้างได้ โดยความอ่อนไหวของข้อมูลสหภาพแรงงานอาจแตกต่างกัน ขึ้นอยู่กับบริบทแรงงานสัมพันธ์ในแต่ละประเทศ[20]

[17] GDPR, Recital 35

[18] ICO, What is Special Category Data?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/; cf. GDPR, Recital 35

[19] EDPB, Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR, Version 2.0 (15 December 2020), para. 53

[20] WP29, Advice Paper on Special Categories of Data ("Sensitive Data"), Ref. Ares(2011)444105 (20 April 2011), Section 3.2.1

2.2.1.8 ข้อมูลพันธุกรรม (Genetic Data)

ข้อมูลพันธุกรรม หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับลักษณะทางพันธุกรรมที่ถ่ายทอดหรือได้รับมาของบุคคล ซึ่งให้ข้อมูลเฉพาะเกี่ยวกับสรีรวิทยาหรือสุขภาพของบุคคลนั้น และได้มาจากการวิเคราะห์ตัวอย่างชีวภาพของบุคคลดังกล่าวโดยเฉพาะ[21] โดยขยายความครอบคลุมถึงการวิเคราะห์โครโมโซม DNA (Deoxyribonucleic acid) หรือ RNA (Ribonucleic acid) รวมถึงการวิเคราะห์ประเภทอื่นที่ให้ข้อมูลเทียบเท่ากัน[22] ดังนั้นขอบเขตของข้อมูลพันธุกรรมจึงไม่จำกัดเพียงการวิเคราะห์ DNA เท่านั้น แต่ครอบคลุมกระบวนการใดก็ตามที่สามารถให้ข้อมูลที่มีลักษณะเทียบเท่าได้

ตัวอย่างข้อมูลพันธุกรรม

- ข้อมูลพันธุกรรมอาจได้มาจากการวิเคราะห์ตัวอย่างชีวภาพ เช่น การวิเคราะห์โครโมโซม DNA หรือ RNA รวมถึงการวิเคราะห์ประเภทอื่นที่ให้ข้อมูลเทียบเท่า ในทางปฏิบัติ ตัวอย่างที่ชัดเจน ได้แก่ ECS
- ผลการตรวจ DNA เพื่อวินิจฉัยโรคทางพันธุกรรม เช่น โรค Huntington หรือ BRCA mutation ที่บ่งชี้ความเสี่ยงมะเร็ง
- ผลการตรวจ Direct-to-Consumer (DTC) genetic testing เช่น บริการตรวจสายเลือดหรือประวัติบรรพบุรุษ ซึ่งอาจเปิดเผยความเสี่ยงต่อโรคและข้อมูลเชื้อชาติไปพร้อมกัน
- ตัวอย่างชีวภาพที่เก็บในธนาคารชีวภาพ (Biobank) สำหรับการวิจัยทางการแพทย์ ซึ่งเมื่อวิเคราะห์และเชื่อมโยงกับบุคคลแล้วถือเป็นข้อมูลพันธุกรรมทันที

2.2.1.9 ข้อมูลชีวภาพ (Biometric Data)

ข้อมูลชีวภาพ (Biometric Data) หมายถึง ข้อมูลส่วนบุคคลที่ได้จากการประมวลผลทางเทคนิคเฉพาะซึ่งเกี่ยวกับลักษณะเด่นทางกายภาพ สรีรวิทยา หรือพฤติกรรมของบุคคล ที่ช่วยให้ระบุหรือยืนยันตัวตนของบุคคลที่ไม่เหมือนกับบุคคลอื่นได้[23] อย่างไรก็ตาม ไม่ใช่ข้อมูลทุกประเภทที่เกี่ยวข้องกับกายภาพ สรีรวิทยา หรือพฤติกรรมจะถือเป็นข้อมูลชีวภาพในทางกฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจากข้อมูลชีวภาพจะถือเป็นข้อมูลส่วนบุคคลอ่อนไหวก็ต่อเมื่อผ่านการประมวลผลด้วยวิธีการทางเทคนิคเฉพาะ (specific technical means)

ดังนั้น การที่ข้อมูลส่วนบุคคลจะเข้าข่ายเป็น “ข้อมูลชีวภาพ” และเป็นข้อมูลส่วนบุคคลอ่อนไหว จะต้องพิจารณาองค์ประกอบสำคัญอย่างน้อย 3 ประการ ได้แก่

[21] GDPR, Article 4(13)

[22] GDPR, Recital 34

[23] มาตรา 26 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

1) **ลักษณะของข้อมูล (Nature of data)**: เป็นข้อมูลที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา หรือพฤติกรรมของบุคคล
2) **วิธีการประมวลผล (Means of processing)**: ต้องผ่าน “การประมวลผลทางเทคนิคเฉพาะ” (specific technical processing) เช่น การสกัดคุณลักษณะเฉพาะ (feature extraction) หรือการสร้าง template
3) **วัตถุประสงค์ (Purpose)**: ต้องมีวัตถุประสงค์เพื่อใช้ในการระบุตัวบุคคลโดยเฉพาะ (uniquely identifying a natural person)

ตัวอย่างข้อมูลชีวภาพ

- ภาพใบหน้าที่ถูกประมวลผลเพื่อสร้างเทมเพลตชีวมิติ (biometric template) สำหรับระบุตัวตนบุคคล
- ข้อมูลลายนิ้วมือที่ใช้แสกนเพื่อเข้าสถานที่หรือยืนยันตัวตน
- ข้อมูลม่านตา หรือเสียง ที่ใช้ระบุตัวตน

2.2.2 แนวทางการลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว

ในการบริหารจัดการข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ซึ่งเป็นข้อมูลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องพึงตระหนักและปฏิบัติตามหลักการลดการ

กระบวนการตรวจสอบประวัติอาชญากรรม สำหรับผู้สมัครงานหรือบุคลากรเข้าใหม่ จะมีสถานะเป็นข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 ซึ่งจะมีความเสี่ยงสูงหากข้อมูลเกิดการรั่วไหล

[แนวทางปฏิบัติ] เพื่อลดความเสี่ยงทางกฎหมายและภาระในการจัดเก็บรักษาข้อมูลที่มีความอ่อนไหวสูง องค์กรสามารถเลือกใช้วิธีการตรวจสอบและบันทึกผลแทนการจัดเก็บเอกสารต้นฉบับ ดังนี้

1.กระบวนการตรวจสอบ: ให้ฝ่ายทรัพยากรบุคคลดำเนินการตรวจสอบความถูกต้องของหนังสือผลการตรวจสอบประวัติอาชญากรรมอย่างถี่ถ้วน

2.การบันทึกสถานะ: ให้เจ้าหน้าที่ผู้มีอำนาจทำการบันทึกเฉพาะสถานะหรือผลการประเมินลงในทะเบียนประวัติบุคลากรว่า "ผ่านการตรวจสอบประวัติอาชญากรรมเป็นที่เรียบร้อยแล้ว" โดยห้ามลงบันทึกรายละเอียดพฤติการณ์หรือฐานความผิดใดๆ ไว้ในระบบ

3. การทำลายเอกสาร: เมื่อเสร็จสิ้นกระบวนการยืนยันและบันทึกผลข้างต้น ให้ดำเนินการลบ ทำลาย หรือส่งคืนเอกสารผลการตรวจสอบประวัติอาชญากรรมฉบับดังกล่าวทันทีด้วยวิธีการที่ปลอดภัย (Secure Disposal) โดยไม่มีการจัดเก็บสำเนาเอกสารดังกล่าวไว้ในแฟ้มประวัติ หรือระบบฐานข้อมูลขององค์กรอีกต่อไป

ประมวลผลข้อมูลเท่าที่จำเป็น (Data Minimization) และการจำกัดการเข้าถึงข้อมูล (Privacy by Design and Default) โดยมีกรณีศึกษาดังต่อไปนี้

3. หน้าที่ของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

ก่อนจะพิจารณาหน้าที่ของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล พึงต้องพิจารณาบทบาทของหน่วยงานว่ามีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเสียก่อน

[พิจารณาบทบาทตามความเป็นจริง] สถานะของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลถือเป็นแนวคิดเชิงหน้าที่ (Functional Concept) ซึ่งมุ่งเน้นการจัดสรรความรับผิดชอบตามบทบาทที่เกิดขึ้นจริง ในทางปฏิบัติ การพิจารณาสถานะทางกฎหมายจึงต้องยึดตามข้อเท็จจริงในแต่ละกิจกรรม (Case-by-case Basis) มากกว่าข้อความที่ระบุไว้ในข้อตกลงหรือสัญญา ทั้งนี้ บทบาทดังกล่าวถูกกำหนดโดยพฤติการณ์จริงของการดำเนินงาน จึงไม่สามารถเจรจาต่อรองเพื่อเปลี่ยนแปลงสถานะให้ขัดต่อความเป็นจริงได้

[ผู้ควบคุมข้อมูลส่วนบุคคล] ความเป็นผู้ควบคุมข้อมูลส่วนบุคคลประกอบด้วย 3 องค์ประกอบหลักดังต่อไปนี้

1) บุคคลธรรมดาหรือนิติบุคคล (Natural or Legal Person)
2) มีอำนาจหน้าที่ตัดสินใจ (Determines)
3) วัตถุประสงค์และวิธีการเกี่ยวกับการประมวลผล (Purposes and Means)

หน้าที่สำคัญที่หน่วยงานต้องปฏิบัติเมื่อมีบทบาทผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

หน้าที่ของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล		
ลำดับ	**หน้าที่**	**มาตราที่เกี่ยวข้อง**
1	การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA)	39
2	การแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล (Privacy Notice)	23, 25
3	การขอความยินยอม (Consent)	19, 20
4	การส่งต่อหรือโอนข้อมูลไปยังต่างประเทศ	28, 29

หน้าที่ของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล		
ลำดับ	**หน้าที่**	**มาตราที่เกี่ยวข้อง**
5	การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)	40
6	การจัดให้มีช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	30 - 36
7	การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	37 (4)
8	การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	41
9	การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	37 (1)

ตาราง 1 หน้าที่ของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

3.1 การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

การดำเนินงานใด ๆ ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องมีการบันทึกลงในบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) โดยอาจแบ่งตามการดำเนินงานของแต่ละหน่วยงานภายในองค์กรเพื่อให้สามารถตรวจสอบรายละเอียดการใช้ข้อมูลในแต่ละกิจกรรมนั้นได้อย่างครบถ้วน ตัวอย่างเช่นกิจกรรมใด ๆ ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องมีการบันทึกลงในรายการกิจกรรม โดยแบ่งแยกตามแผนกงาน เพื่อให้สามารถตรวจสอบรายละเอียดการใช้ข้อมูลในแต่ละกิจกรรมนั้นได้

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) โดยต้องมีรายละเอียดและรูปแบบตามที่กฎหมายกำหนด ดังต่อไปนี้

[รายละเอียด RoPA] หน่วยงานจะต้องบันทึกข้อมูลสำคัญอย่างน้อย 8 รายการ ประกอบด้วยหน่วยงานต้องบันทึกรายการอย่างน้อย ดังต่อไปนี้[24]

1) รายการข้อมูลส่วนบุคคล: ระบุข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2) วัตถุประสงค์ในการใช้งาน: ระบุเหตุผลหรือวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล: รายละเอียดเกี่ยวกับหน่วยงาน ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

[24] มาตรา 39 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล: ระบุว่าจะเก็บรักษาข้อมูลไว้เป็นระยะเวลาเท่าใด
5) การเข้าถึงข้อมูล: รายละเอียดเกี่ยวกับสิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6) การใช้หรือเปิดเผยข้อมูลส่วนบุคคล: รายละเอียดการใช้งานหรือการส่งต่อข้อมูลให้บุคคลภายนอก
7) การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล: บันทึกการปฏิเสธคำขอหรือการคัดค้านต่าง ๆ ที่มาจากเจ้าของข้อมูลส่วนบุคคล
8) มาตรการรักษาความปลอดภัย: คำอธิบายเกี่ยวกับวิธีหรือมาตรการที่ใช้รักษาความมั่นคงปลอดภัยของข้อมูล

ทั้งนี้ รายการทั้ง 8 รายการข้างต้นเป็นเพียงรายการขั้นต่ำที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำขึ้น

[รูปแบบ] การบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องจัดทำเป็นลายลักษณ์อักษร ซึ่งสามารถจัดทำได้ทั้งในรูปแบบกระดาษ หรือรูปแบบขอมูลอิเล็กทรอนิกส์ก็ได้ตามความเหมาะสม[25]

ฐานทางกฎหมาย

ฐานทางกฎหมาย คือ เหตุที่ชอบด้วยกฎหมายที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย การระบุฐานทางกฎหมายใน RoPA มีความสำคัญอย่างยิ่ง เนื่องจากช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถแสดงให้เห็นว่าการประมวลผลข้อมูลแต่ละกิจกรรมมีความชอบธรรมและเป็นไปตามที่กฎหมายกำหนด ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุฐานทางกฎหมายให้ครบถ้วนและถูกต้องสำหรับข้อมูลแต่ละประเภทที่มีการประมวลผลก่อนการเก็บรวบรวมข้อมูลและไม่สามารถเปลี่ยนฐานได้ภายหลังโดยไม่แจ้ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 24 กำหนดฐานทางกฎหมายทั่วไปไว้ 7 ฐาน ได้แก่

1. ความยินยอม (Consent)

เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตน ทั้งนี้ ความยินยอมต้องเป็นไปโดยอิสระ เฉพาะเจาะจง แจ้งให้ทราบ และไม่คลุมเครือ เช่น การขอความยินยอมในการส่งอีเมลการตลาดหรือจดหมายข่าวให้กับลูกค้า

[25] มาตรา 39 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

อย่างไรก็ตาม ความยินยอมมีความเสี่ยงสูงในการใช้เป็นฐานในการประมวลผล เนื่องจากยึดโยงกับความสมัครใจของเจ้าของข้อมูลส่วนบุคคล จึงอาจต้องหยุดการประมวลผลเมื่อไรก็ได้ตามที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม ก่อนใช้ฐานนี้ควรพิจารณาก่อนว่ามีฐานอื่นที่เหมาะสมกว่าหรือไม่

2. การจัดทำเอกสารประวัติศาสตร์ การศึกษาวิจัย หรือสถิติ (Historical Document, Research, Statistics)

จำเป็นเพื่อวัตถุประสงค์เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัย หรือสถิติ โดยต้องมีมาตรการปกป้องที่เหมาะสม เช่น การวิจัยทางการแพทย์หรือการสำรวจสถิติประชากรแห่งชาติ

3. ประโยชน์สำคัญต่อชีวิต (Vital Interests)

จำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ใช้ได้เฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ในขณะนั้น (กรณีฉุกเฉินที่ไม่อาจขอความยินยอมได้ทันการณ์ ไม่ใช้กับสถานการณ์ที่สามารถวางแผนขอความยินยอมล่วงหน้าได้และ ไม่มีวิธีอื่นใดที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลข้อมูลนี้แล้ว เช่น การแบ่งปันข้อมูลสุขภาพในสถานการณ์ฉุกเฉินทางการแพทย์

4. ฐานสัญญา (Contract)

จำเป็นเพื่อการปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อดำเนินการตามคำขอก่อนเข้าทำสัญญา เช่น การเก็บข้อมูลพนักงานเพื่อการจ่ายเงินเดือนตามสัญญาจ้างงาน หรือการเก็บข้อมูลผู้ซื้อเพื่อการจัดส่งสินค้าตามสัญญาซื้อขาย

ฐานสัญญาครอบคลุมเฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญากับผู้ควบคุมข้อมูลส่วนบุคคลโดยตรงเท่านั้น หากต้องประมวลผลข้อมูลของบุคคลอื่นที่ไม่ได้เป็นคู่สัญญา (คู่สมรสผู้เอาประกันผู้รับผลประโยชน์ ผู้ประสานงานของคู่สัญญา) ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ฐานทางกฎหมายอื่น เช่น ฐานความยินยอม หรือฐานประโยชน์โดยชอบด้วยกฎหมายแทน ทั้งนี้ ฐานนี้ไม่สามารถใช้กับข้อมูลส่วนบุคคลอ่อนไหวได้

5. ภารกิจเพื่อประโยชน์สาธารณะ (Public Task)

จำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ เช่น การประมวลผลข้อมูลสุขภาพเพื่อการเฝ้าระวังโรคระบาดโดยหน่วยงานสาธารณสุข โดยทั่วไปฐานนี้จะใช้โดยเจ้าหน้าที่หรือองค์กรของรัฐ แต่เอกชนสามารถใช้ฐานทางกฎหมายนี้ได้หากได้รับมอบหมายจากรัฐเพื่อประโยชน์สาธารณะ

6. ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interests)

จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก โดยประโยชน์ดังกล่าวต้องมีน้ำหนักเหนือกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล เช่น การใช้ข้อมูลของลูกค้าเพื่อป้องกันการทุจริต, รักษาความปลอดภัยของระบบสารสนเทศ หรือ การติดต่อประสานงาน

ก่อนอ้างฐานนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำ **การประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interests Assessment: LIA)** ซึ่งเป็นเอกสารบันทึกเหตุผลที่แสดงให้เห็นว่าการประมวลผลผ่านทั้ง 3 ขั้นตอนต่อไปนี้

- **การทดสอบวัตถุประสงค์ (Purpose Test):** ประโยชน์ที่ต้องการบรรลุชอบด้วยกฎหมายและมีความชัดเจนเพียงพอหรือไม่
- **การทดสอบความจำเป็น (Necessity Test):** จำเป็นต้องประมวลผลข้อมูลจริงหรือไม่ หรือมีวิธีอื่นที่กระทบสิทธิเจ้าของข้อมูลส่วนบุคคลน้อยกว่า
- **การทดสอบการชั่งน้ำหนัก (Balancing Test):** ประโยชน์ที่ได้รับมีน้ำหนักเหนือกว่าสิทธิและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลหรือไม่ โดยพิจารณาด้วยว่าเจ้าของข้อมูลส่วนบุคคลน่าจะคาดได้ว่าข้อมูลของตนถูกนำไปใช้เช่นนี้หรือไม่

ตัวอย่างการประเมินประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interests Assessment: LIA)

➢ **กรณีตัวอย่างที่ 1: สามารถอ้างฐาน Legitimate Interest ได้**

ร้านค้าต้องการส่ง SMS สิทธิพิเศษครบรอบปี ไปยังลูกค้าเดิมที่เคยซื้อสินค้าหรือใช้บริการของร้านค้าอยู่แล้ว โดยใช้เพียงข้อมูลชื่อและช่องทางการติดต่อพื้นฐาน เช่น ที่อยู่ หรือเบอร์โทรศัพท์ ที่ลูกค้าเคยให้ไว้ขณะซื้อสินค้า โดยที่สินค้าหรือบริการนั้นมีลักษณะเดียวกับสินค้าหรือบริการที่ลูกค้าเคยมีนิติสัมพันธ์อยู่ด้วย

<u>การประเมินและพิจารณาผ่าน 3 ขั้นตอน (LIA)</u>

1. การทดสอบวัตถุประสงค์ (Purpose Test)

วัตถุประสงค์คือการส่งเสริมการขายแก่ฐานลูกค้าเดิม ซึ่งถือเป็นประโยชน์โดยชอบด้วยกฎหมายและเป็นสิทธิในการดำเนินธุรกิจเชิงพาณิชย์ทั่วไปของร้านค้า

2. การทดสอบความจำเป็น (Necessity Test)

มีความจำเป็นเพื่อรักษาความสัมพันธ์อันดีกับลูกค้า (Customer Retention) และแจ้งสิทธิประโยชน์ที่ลูกค้าควรได้รับ การส่งไปยังข้อมูลติดต่อที่ลูกค้าให้ไว้โดยตรงเป็นช่องทางที่มีประสิทธิภาพ และร้านค้าจำกัดการใช้ข้อมูลเฉพาะเท่าที่จำเป็นเพื่อการติดต่อเท่านั้น ไม่ได้นำข้อมูลไปส่งต่อให้ผู้อื่น

3. การทดสอบการชั่งน้ำหนัก (Balancing Test)

เมื่อนำมาชั่งน้ำหนักแล้ว การส่งข่าวสารทั่วไปแก่ลูกค้าเดิม ไม่ได้ส่งผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐานของลูกค้าอย่างรุนแรง และในบริบทนี้ "ลูกค้ามีความคาดหมายโดยชอบธรรม (Reasonable Expectation)" อยู่แล้วว่า การที่ตนเองเป็นลูกค้าของร้านนี้ น่าจะได้รับข้อความประชาสัมพันธ์หรือสิทธิพิเศษจากร้านค้า เนื่องจากเป็นสินค้าหรือบริการที่มีลักษณะประเภทเดียวกันกับที่ตนเองเคยซื้อหรือเคยใช้บริการ (มีนิติสัมพันธ์ร่วมกันอยู่)

กิจกรรมการส่ง SMS สิทธิพิเศษครบรอบปี ไปยังลูกค้าเดิมนี้ จึงสามารถอ้างฐาน Legitimate Interest ได้ โดยไม่ต้องขอความยินยอม (Consent) *แต่ร้านค้าต้องจัดให้มีช่องทางที่ชัดเจนและง่ายดาย เพื่อให้ลูกค้าเลือกปฏิเสธการรับข่าวสาร (Opt-out / Unsubscribe) ได้ทุกเมื่อตามสิทธิกฎหมาย*

➢ **กรณีตัวอย่างที่ 2: ไม่สามารถอ้างฐาน Legitimate Interest ได้**

ร้านค้าต้องการนำประวัติประเภทสินค้าที่ลูกค้าเคยซื้อ ไปใช้ในการวิเคราะห์พฤติกรรม (Profiling) เพื่อส่งโฆษณาเสนอขายสินค้าชิ้นใหม่ที่ตรงใจลูกค้าคนนั้นโดยเฉพาะ (Direct Marketing / Personalized Ads)

<u>การประเมินและพิจารณาผ่าน 3 ขั้นตอน (LIA)</u>

1. การทดสอบวัตถุประสงค์ (Purpose Test)

วัตถุประสงค์คือการทำการตลาดและการเพิ่มยอดขายของบริษัท ซึ่งถือเป็นผลประโยชน์ในเชิงพาณิชย์ที่ชอบด้วยกฎหมายทั่วไปของธุรกิจ

2. การทดสอบความจำเป็น (Necessity Test)

แม้บริษัทจะอยากเพิ่มยอดขาย แต่ "ไม่มีความจำเป็นเชิงบังคับ" ที่ต้องเอาประวัติพฤติกรรมเชิงลึกของลูกค้าไปประมวลผลเพื่อการนั้น บริษัทสามารถใช้วิธีการตลาดทั่วไปที่ไม่เจาะจงรายบุคคล หรือเลือกใช้วิธีส่งโฆษณาแบบกว้างๆ ซึ่งกระทบสิทธิ์ลูกค้าน้อยกว่าได้

3. การทดสอบการชั่งน้ำหนัก (Balancing Test)

สิทธิในความเป็นส่วนตัวของลูกค้า (Privacy Rights) มีน้ำหนักเหนือกว่าประโยชน์ทางเศรษฐกิจของบริษัท และในบริบทนี้ "ลูกค้าไม่ได้คาดหมาย (No Reasonable Expectation)" ว่าการเข้ามาซื้อของ จะทำให้ตนเองถูกติดตามพฤติกรรมและถูกยิงโฆษณาในภายหลังโดยไม่ถามความสมัครใจ

กิจกรรมการวิเคราะห์พฤติกรรมของลูกค้านี้ จึงไม่สามารถอ้างฐาน Legitimate Interest ได้ และอาจต้องพิจารณาขอความยินยอม (Consent)

7. การปฏิบัติตามกฎหมาย (Legal Obligation)

จำเป็นเพื่อการปฏิบัติตามกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติตาม เช่น การจัดเก็บข้อมูลพนักงานตามกฎหมายคุ้มครองแรงงาน หรือการจัดเก็บข้อมูลทางการเงินตามกฎหมายภาษีอากร

ผู้ที่ไม่ต้องจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2567 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลในกลุ่มดังต่อไปนี้ได้รับยกเว้นไม่ต้องจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ดังนี้[26]

1) วิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลาง (SMEs) ตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
2) วิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน
3) วิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม
4) สหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์
5) มูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรเอกชนที่ไม่แสวงหากำไร
6) นิติบุคคลอาคารชุดตามกฎหมายว่าด้วยอาคารชุด หรือนิติบุคคลหมู่บ้านจัดสรรตามกฎหมายว่าด้วยการจัดสรรที่ดิน
7) กิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน
8) กิจการที่ดำเนินการโดยผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นบุคคลธรรมดา

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับการยกเว้นข้างต้นต้องไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (1) (2) และ (3) แห่งประราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับการยกเว้นข้างต้นยังคงต้องจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลอยู่ หากปรากฏว่ามีการประมวลผลข้อมูลส่วนบุคคลในลักษณะ ดังต่อไปนี้

1) การประมวลผลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

[26] ข้อ 4 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2567

2) การประมวลผลข้อมูลที่มีลักษณะเป็นประจำ ไม่มีใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว

3) มีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ตามมาตรา 26

ข้อแนะนำสำหรับการบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ในการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลแนะนำให้แบ่งบันทึกเป็นรายกิจกรรม โดยพิจารณาจากวัตถุประสงค์หลักของแต่ละกิจกรรมเป็นสำคัญ หากเป็นกิจกรรมที่มีวัตถุประสงค์เหมือนหรือคล้ายกัน อาจบันทึกรวมกิจกรรมได้โดยไม่จำเป็นต้องแยกบันทึกเป็นรายครั้งที่มีการจัดกิจกรรม และจัดกลุ่มกิจกรรมไว้ภายใต้หน่วยงานภายในที่รับผิดชอบ เช่น งานบุคคล งานการเงิน งานบริการ งานรักษาความปลอดภัย

[กิจกรรมที่ควรพิจารณาเขียนแยก] สิ่งที่ต้องพิจารณาเป็นหลัก คือ กิจกรรมมีวัตถุประสงค์ต่างกันหรือเป็นการประมวลผลที่แตกต่างกันอย่างชัดเจน นอกจากนี้ อาจมีปัจจัยอื่นที่สามารถมาใช้พิจารณาประกอบได้ในกรณีที่ยังไม่ชัดว่ากิจกรรมนั้นมีวัตถุประสงค์เหมือนหรือต่างกัน ได้แก่ ฐานทางกฎหมาย (กิจกรรมเดียวกันอาจมีได้มากกว่าหนึ่งฐาน), การมีข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 (เป็นปัจจัยที่ต้องให้ความสำคัญและมาตรการรักษาความมั่นคงปลอดภัยเป็นพิเศษ) และระดับความเสี่ยงที่มีความต่างกัน โดยเฉพาะกิจกรรมที่ต้องมีการจัดทำ DPIA ทั้งนี้ การมีกลุ่มเจ้าของข้อมูลส่วนบุคคลที่หลากหลายกลุ่ม ระยะเวลาการจัดเก็บหลายช่วง หรือผู้รับข้อมูลหลายราย สามารถบันทึกไว้ใน 1 กิจกรรมเดียวได้

ตัวอย่างกิจกรรมการประมวลผลที่สามารถรวมกิจกรรมได้

ในกิจกรรมการประชุมของหน่วยงานซึ่งมีการจัดขึ้นทุกเดือน หากซึ่งข้อมูลที่ใช้ในการจัดการประชุมจะเป็นข้อมูลชุดเดิม และมีวิธีการเก็บรวบรวม การบันทึก หรือการนำมาใช้เหมือนกันทุกครั้ง ดังนั้นสามารถบันทึก ในกิจกรรมการประชุมนี้จึงสามารถบันทึกเป็น 1 กิจกรรม คือได้แก่ การจัดการประชุม ในบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล โดยไม่จำเป็นต้องบันทึกในทุกครั้งที่มีการจัดประชุม เนื่องจากรายละเอียดในการประมวลผลข้อมูลเหมือนกัน หากในการประชุมครั้งใดมีการปรับเปลี่ยนหรือเพิ่มเติมรายละเอียดบางส่วนเพิ่มเติม ก็สามารถแก้ไขเปลี่ยนแปลง และเพิ่มเติมรายละเอียดที่บันทึกกิจกรรมการประชุมนี้ได้ เพื่อให้บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีความถูกต้องและเป็นปัจจุบัน

ทั้งนี้ หากการประชุมบางประเภทมีลักษณะต่างไปอย่างมีนัยสำคัญ เช่น มีการบันทึกภาพหรือเสียงเพื่อเผยแพร่ มีการส่งข้อมูลผู้เข้าร่วมไปต่างประเทศ หรือมีการใช้ข้อมูลส่วนบุคคลอ่อนไหว ให้แยกบันทึกเป็นกิจกรรมต่างหาก

ตัวอย่างกิจกรรมการประมวลผลควรแยกจากกัน

ในกิจกรรมการประชุม อบรม สัมมนา หน่วยงานมีการจ้างวิทยากร และจำเป็นต้องขอข้อมูลส่วนบุคคลและเอกสารหลักฐานต่าง ๆ เพื่อใช้ในการเบิกค่าวิทยากร กรณีเช่นนี้ หน่วยงานอาจพิจารณาแยกกิจกรรมการเบิกจ่ายค่าวิทยากรออกจากกิจกรรมการจัดประชุม อบรม สัมมนา

3.2 การแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดการนำข้อมูลไปประมวลผล เมื่อได้รับขอมูลสวนบุคคลไม่ว่าจะได้รับข้อมูลมาโดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่น และไม่ว่าจะอาศัยฐานทางกฎหมายการประมวลผลใดในการประมวลผล[27]

[เนื้อหาการแจ้ง] ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดเตรียมรายละเอียดข้อมูลที่สำคัญและแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคล โดยข้อมูล (Information) ที่ต้องจัดเตรียมและแจ้งมีดังนี้

1) วัตถุประสงค์และฐานทางกฎหมาย: แจ้งเจ้าของข้อมูลส่วนบุคคลว่านำข้อมูลไปใช้เพื่อวัตถุประสงค์ใด และ ใช้สิทธิตามกฎหมายข้อใดในการจัดการข้อมูล
2) ประเภทของข้อมูลส่วนบุคคล: ระบุรายการข้อมูลส่วนบุคคลที่มีการจัดเก็บ
3) ระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล: ระบุว่าจะจัดเก็บข้อมูลไว้เป็นระยะเวลาเท่าใด
4) การโอนข้อมูลส่วนบุคคล: แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบหากมีการโอนข้อมูลให้ผู้อื่นหรือส่งไปยังต่างประเทศ
5) มาตรการรักษาความมั่นคงปลอดภัย: ระบุวิธีดูแลรักษาข้อมูลให้มั่งคงปลอดภัย
6) สิทธิของเจ้าของข้อมูลส่วนบุคคล: แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิอะไรบ้างตามกฎหมาย
7) ข้อมูลการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล: ข้อมูลสำหรับการติดต่อหน่วยงาน ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

[ระยะเวลาการแจ้ง] นอกจากที่ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำถึงถึงข้อมูลที่ต้องจัดเตรียมและแจ้งแล้ว ยังต้องคำนึงถึงระยะเวลาการแจ้ง โดยขึ้นอยู่กับแต่ละกรณี ดังนี้[28]

1) กรณีเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

[27] TDPG 3.0 p.104

[28] TDPG 3.0 p.106

2) กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาที่เหมาะสม แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมหรือได้รับข้อมูลมา
3) กรณีการใช้ข้อมูลเป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งอย่างช้าที่สุดข้าเมื่อมีการติดต่อสื่อสารครั้งแรก
4) กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม ต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก
5) เมื่อมีการเปลี่ยนแปลงของข้อมูล (Information) ที่มีผลกระทบอย่างมีนัยสำคัญ ต่อการประมวลผลที่เคยแจ้งให้เจ้าข้องข้อมูลทราบ อาทิ การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญแม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยตามที่เคยแจ้งไว้ก็ตาม หรือ เป็นการเพิ่มขั้นตอนการประมวลผลข้อมูลอย่างมาก ควรแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้นหรือโดยเร็วที่สุด

[วิธีการแจ้ง] การแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล ไม่ได้กำหนดวิธีการแจ้งไว้อย่างชัดเจน สามารถแจ้งโดยวาจา หนังสือ วิธีการทางอิเล็กทรอนิกส์ หรือช่องทางอื่นได้ แต่การแจ้งนั้นต้องมีลักษณะที่เข้าถึงได้ง่าย มีความพร้อมใช้งาน สามารถเข้าดูการแจ้งรายละเอียดได้ทุกเมื่อ และไม่มีค่าใช้จ่าย โดยทั่วไปองค์กรมักแจ้งผ่านเว็บไซต์ทางการหลักขององค์กร โดยต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูล

ในกรณีที่องค์กรไม่มีเว็บไซต์ทางการหลัก สามารถแจ้งสามารถกระทำได้โดยวิธีอื่น เช่น การแจ้งเป็นหนังสือ การยื่นสำเนาเอกสารต่อหน้าบุคคล การแจ้งผ่านอีเมล การแนบไฟล์แปลงลิงก์ URL หรือ QR code โดยจัดวางบนช่องทางโซเชียลมีเดียหลัก หรือ จัดวางในข้อความต้อนรับอัตโนมัติ การแจ้งผ่านช่องทางอื่น ๆ ซึ่งเป็นช่องทางหลักในการติดต่อ และสังเกตเห็นได้ง่าย

3.3 การขอความยินยอม

[กรณีที่ต้องขอความยินยอม] หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามสถานการณ์ ดังต่อไปนี้

1) เมื่อไม่มีฐานทางกฎหมายอื่นรองรับ: หากการใช้ข้อมูลนั้นไม่สามารถอ้างอิงฐานทางกฎหมายอื่นได้ เช่น ไม่ใช่การปฏิบัติตามสัญญา หรือไม่ใช่การปฏิบัติตามกฎหมาย จึงจำเป็นต้องใช้ฐานความยินยอมตามมาตรา 24
2) กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว: ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลศาสนา ข้อมูลประวัติอาชญากรรม และไม่เข้าข้อยกเว้นตามที่กฎหมายกำหนดในมาตรา 26

[การขอความยินยอมของผู้เยาว์] ในกรณีที่ผู้เยาว์ยังไม่บรรลุนิติภาวะโดยการสมรสหรือโดยคำสั่งศาล ตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์ (กรณีได้รับความยินยอมจากผู้แทนโดยชอบธรรมให้ประกอบธุรกิจหรือทำสัญญาจ้างแรงงาน) ให้ดำเนินการขอความยินยอม ดังนี้

1) กรณีผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์เท่านั้น
2) กรณีผู้เยาว์อายุมากกว่า 10 ปีแต่ยังไม่บรรลุนิติภาวะนั้น ผู้เยาว์สามารถให้ความยินยอมด้วยตนเองได้โดยไม่ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง หากเป็นนิติกรรมที่ผู้เยาว์ทำเองเฉพาะตัว หรือเป็นการสมแก่ฐานานุรูปและจำเป็นในการดำรงชีพตามสมควร หรือเพื่อให้ได้มาซึ่งสิทธิอันใดอันหนึ่ง หรือเพื่อหลุดพ้นจากหน้าที่อันใดอันหนึ่งตามที่บัญญัติไว้ในมาตรา 22 – 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์

ฐานความยินยอมไม่ใช่ทางเลือกบังคับสำหรับข้อมูลส่วนบุคคลของผู้เยาว์ หากแต่ยังคงสามารถใช้ฐานทางกฎหมายอื่นตามมาตรา 24 แทนได้ทุกช่วงอายุของผู้เยาว์ และเมื่อใช้ฐานอื่นก็ไม่ต้องนำเกณฑ์อายุตามมาตรา 20 มาใช้ ทั้งนี้ต้องเป็นฐานที่เข้ากับวัตถุประสงค์จริง ทั้งนี้ สำหรับกรณีอาศัยฐานประโยชน์โดยชอบด้วยกฎหมายต้องระวังเป็นพิเศษเนื่องจากผู้เยาว์เป็นกลุ่มเปราะบาง

อย่างไรก็ดี หากมีการประมวลผลข้อมูลส่วนบุคคลออนไหว ยังคงต้องใช้ความยินยอมโดยชัดแจ้ง เว้นแต่เข้าข้อยกเว้นตามมาตรา 26

ตัวอย่างที่ 1

บริษัท ก ผู้ให้บริการแอปพลิเคชั่น ต้องจัดให้มีมาตรการทางเทคนิคเพื่อให้ผู้เยาว์สามารถระบุและยืนยันอายุตนเองได้ เพื่อขอความยินยอมโดยชัดแจ้งต่อผู้เยาว์ซึ่งมีอายุ 10 ปีขึ้นไป

ตัวอย่างที่ 2

บริษัท ข ผู้ให้บริการจัดค่ายกิจกรรม ซึ่งมีกลุ่มลูกค้าเป้าหมายคือผู้เยาว์อายุไม่เกิน 10 ปี ต้องจัดให้มีแบบฟอร์มให้ผู้ใช้อำนาจปกครองลงนามให้ความยินยอมโดยชัดแจ้ง พร้อมตรวจสอบหลักฐานแสดงความเป็นผู้ใช้อำนาจปกครองประกอบกับตรวจสอบบัตรประจำตัวประชาชน เพื่อยืนยันว่ามีอำนาจกระทำการแทนผู้เยาว์จริง

[รายละเอียดในการขอความยินยอม] ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดเตรียมข้อมูลดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถทำความเข้าใจและตัดสินใจเกี่ยวกับการให้ความยินยอมของตน

1) ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ชื่อและที่อยู่หน่วยงาน เป็นต้น

2) ข้อมูลส่วนบุคคลที่ประมวลผล เช่น ข้อมูลสุขภาพ เป็นต้น
3) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
4) ช่องทางเพิกถอนความยินยอม
5) การยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
6) แจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลหรือนโยบายคุ้มครองข้อมูลส่วนบุคคล

หากเจ้าของข้อมูลส่วนบุคคล “ไม่ยินยอม” ให้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องจัดทำเอกสาร หลักฐาน เพื่อยืนยันความไม่ยินยอมนั้น เช่น กรณีลูกค้าไม่ยินยอมให้โรงแรมส่งข้อมูลทางการตลาดในภายหลัง โรงแรมไม่จำเป็นต้องดำเนินการใดทางเอกสารเพื่อยืนยันความไม่ยินยอมนั้น

[Cookie] คุกกี้ (Cookie) คือ ไฟล์ข้อมูลขนาดเล็กที่เว็บไซต์สร้างขึ้น ซึ่งแสดงประวัติการเยี่ยมชมเว็บไซต์และการดาวน์โหลด โดยคุกกี้จะจดจำข้อมูลหลายรูปแบบ เช่น ตำแหน่งผู้ใช้งาน ภาษาบนเว็บไซต์ หรือ ข้อมูลของผู้ใช้งาน และเมื่อกลับเข้าไปใช้งานเว็บไซต์อีกครั้ง อุปกรณ์ที่ใช้งานจะสามารถจดจำเว็บไซต์นั้นได้ ไฟล์คุกกี้จึงถือเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ผู้ดูแลเว็บไซต์จึงมีหน้าที่ต้องมีขอความยินยอมของผู้ใช้งานเพื่อจัดเก็บไฟล์คุกกี้ด้วย ซึ่งเรียกว่า Cookie Consent

ประเภทของคุกกี้

1.1) คุกกี้ที่จำเป็น (Necessary cookies)

คุกกี้ประเภทนี้ไม่จำเป็นต้องขอความยินยอมจากผู้ใช้งานเนื่องจากเป็นการเก็บไฟล์คุกกี้เพื่อให้เว็บไซต์สามารถใช้งานฟังก์ชันพื้นฐานต่างๆได้และมีความจำเป็นเพื่อให้เว็บไซต์ทำงานได้อย่างถูกต้อง เช่น การนำทางเว็บไซต์ การเข้าถึงพื้นที่ปลอดภัยบนเว็บไซต์

1.2) คุกกี้ที่ไม่จำเป็น (Non-necessary Cookies)

คุกกี้เหล่านี้จำเป็นต้องขอความยินยอมโดยชัดแจ้งจากผู้ใช้งานเนื่องจากไม่มีความสำคัญต่อการใช้งานเว็บไซต์โดยตรง และ อาจก่อให้เกิดความรำคาญแก่ผู้ใช้งานได้ โดยคุกกี้ประเภทนี้แบ่งออกเป็น

- คุกกี้โฆษณา (Marketing Cookies) เป็นคุกกี้ที่มีการส่งข้อมูลไปยังเว็บไซต์ Third Party เพื่อติดตามผู้เยี่ยมชมเว็บไซต์ โดยมีวัตถุประสงค์คือ การแสดงโฆษณาที่เกี่ยวข้องสำหรับผู้ใช้งานแต่ละราย
- คุกกี้เก็บข้อมูลการใช้งาน (Statistics Cookies) เป็นคุกกี้ทางสถิติที่รวบรวมและรายงานข้อมูลทางสถิติการเยี่ยมชมเว็บไซต์ของผู้ใช้งาน โดยไม่ระบุชื่อ

- คุกกี้ฟังก์ชันการทำงาน (Preference Cookies) เป็นคุกกี้ซึ่งบันทึกข้อมูลการเปลี่ยนแปลงลักษณะการทำงาน หรือ รูปลักษณ์เว็บไซต์ ของผู้ใช้งาน เช่น การจดจำการ log in ภาษาที่ใช้งาน และ ภูมิภาคของผู้ใช้งาน

[KYC] KYC หรือ Know Your Customer คือกระบวนการพิสูจน์ยืนยันตัวตนในการทำความรู้จักกับลูกค้า เพื่อป้องกันการทุจริตและปลอมแปลงข้อมูลในธุรกรรมทางการเงิน ฟอกเงิน และสร้างความปลอดภัยแก่เจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นหลักเกณฑ์ที่กำหนดใน พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 โดยผู้ที่มีหน้าที่ตรวจสอบข้อเท็จจริงของลูกค้า ได้แก่ สถาบันทางการเงินตามคำนิยามของพระราชบัญญัติดังกล่าว เช่น ธนาคารพาณิชย์ บริษัทเงินทุน บริษัทหลักทรัพย์ บริษัทประกันชีวิต บริษัทประกันวินาศภัย และผู้ประกอบอาชีพตามมาตรา 16

[E-KYC] (Electronic Know Your Customer) คือกระบวนการตรวจสอบพิสูจน์และยืนยันตัวตนผ่านช่องทางดิจิทัล โดยอาจมีการใช้ภาพสแกนใบหน้า ที่เป็นข้อมูลชีวภาพ (Biometric Data) อันเป็นข้อมูลส่วนบุคคลอ่อนไหว ตามมาตรา 26 จึงต้องมีการขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อนดำเนินการประมวลผลดังกล่าว

3.4 การส่งต่อหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ส่งที่อยู่ในประเทศไทยไปยังผู้รับที่อยู่ในต่างประเทศ ไม่ว่าจะเป็นการส่งในรูปแบบเอกสาร (ทางกายภาพ) หรือการส่งผ่านระบบคอมพิวเตอร์และระบบเครือข่ายออนไลน์ หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามหลักเกณฑ์ในมาตรา 28 และมาตรา 29 เพื่อความสะดวกในการพิจารณา หน่วยงานสามารถดำเนินการตามลำดับขั้นตอน ดังนี้

ขั้นที่ 1 พิจารณาว่า "เป็นการส่งหรือโอนไปต่างประเทศ" หรือไม่

หน่วยงานต้องพิจารณาก่อนว่ากิจกรรมของตนเข้าข่ายเป็น "การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ" หรือไม่ เพราะหากไม่เข้าข่าย ก็ไม่ต้องพิจารณาหลักเกณฑ์ตามมาตรา 28 และมาตรา 29 กรณีที่ ไม่ถือว่าเป็น การส่งหรือโอนไปต่างประเทศ ได้แก่

- การส่งผ่านข้อมูล (Data Transit): การส่งข้อมูลที่มีการผ่านเครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือระบบเครือข่ายในต่างประเทศเพียงเพื่อเป็นสื่อกลาง (Intermediary) ในการรับส่งข้อมูลเท่านั้น
- การเก็บพักข้อมูล (Data Storage): การนำข้อมูลไปจัดเก็บไว้ในระบบคลาวด์ (Cloud) หรือ Server ในต่างประเทศ

ทั้งนี้ ต้องไม่มีบุคคลใดนอกจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือ ลูกจ้าง เข้าถึงข้อมูลส่วนบุคคล เนื่องจากมีมาตรการทางเทคนิคหรือเงื่อนไขทางกฎหมายรองรับ

ตัวอย่างกรณีที่ไม่เป็นการส่งต่อหรือโอนข้อมูลส่วนบุคคล

- บริษัท A ประเทศไทย ส่งข้อมูลส่วนบุคคลไปยังบริษัท B ซึ่งตั้งอยู่ในประเทศไทย ผ่านทางอีเมล ซึ่งมีเครื่องคอมพิวเตอร์แม่ข่าย (Server) อยู่ในประเทศอินเดีย ในกรณีนี้ถือว่าเป็นการส่งผ่านข้อมูล (Data Transit) โดยที่มี Server เป็นเพียงสื่อกลางในการรับส่ง (Intermediary) เท่านั้น
- บริษัท A ประเทศไทย ส่งข้อมูลส่วนบุคคลไปยังระบบคลาวด์ ซึ่งมี Server อยู่ในประเทศสหรัฐอเมริกา เพื่อทำการสำรองข้อมูล (Back Up) โดยมีเพียงบริษัท A เท่านั้นที่สามารถเข้าถึงข้อมูลที่ถูกกักเก็บไว้ในระบบคลาวด์ได้ ในกรณีนี้ถือว่าเป็นการเก็บพักข้อมูล (Data Storage) ที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลดังกล่าว นอกเหนือจากบริษัท A ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นผู้ส่งหรือโอนข้อมูลส่วนบุคคลนั้นเอง

ตัวอย่างกรณีที่เป็นการส่งต่อหรือโอนข้อมูลส่วนบุคคล

- บริษัท A ประเทศไทย ส่งข้อมูลส่วนบุคคลไปยังระบบคลาวด์ ซึ่งมี Service อยู่สหรัฐอเมริกา เพื่อเก็บข้อมูลให้กับบริษัท B ประเทศญี่ปุ่น โดยบริษัท B สามารถเข้าถึงข้อมูลได้ในกรณีนี้ถือว่าเป็นการส่งต่อหรือโอนข้อมูลที่มีบุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลดังกล่าว
- บริษัท A ประเทศไทยส่งข้อมูลพนักงานให้บริษัทประกันที่สิงคโปร์ เพื่อทำกรมธรรม์ประกันสุขภาพกลุ่ม บริษัทประกันรับข้อมูลไปแล้วตัดสินใจในการประเมินความเสี่ยง คิดเบี้ย และบริหารกรมธรรม์ในกรณีนี้ถือว่าเป็นการส่งต่อหรือโอนข้อมูลที่ข้อมูลเดินทางไปยังต่างประเทศ ไม่ว่าจะเป็นการส่งหรือโอนข้อมูลโดยทางกายภาพ หรือผ่านระบบคอมพิวเตอร์ หรือระบบเครือข่ายไปยังผู้รับข้อมูลส่วนบุคคลที่ตั้งอยู่ในต่างประเทศ

ขั้นที่ 2 พิจารณา "ฐานทางกฎหมาย/ข้อยกเว้น" ตามมาตรา 28

โดยหลักแล้ว การส่งหรือโอนไปต่างประเทศจะกระทำได้ก็ต่อเมื่อประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ดี กฎหมายกำหนดข้อยกเว้นไว้ ซึ่งหากการส่งหรือโอนของหน่วยงานเข้าข้อยกเว้นข้อใดข้อหนึ่งดังต่อไปนี้ หน่วยงานก็สามารถส่งหรือโอนข้อมูลไปยังประเทศปลายทาง

นั้นได้ โดยไม่ต้องพิจารณาความเพียงพอของมาตรฐานการคุ้มครองของประเทศปลายทาง หน่วยงานจึงควรตรวจสอบข้อยกเว้นเหล่านี้เป็นลำดับแรกเพื่อลดภาระในการพิจารณา ได้แก่

1) **การปฏิบัติตามกฎหมาย** โดยเป็นกรณีที่จำเป็นต้องปฏิบัติตามกฎหมาย ทั้งนี้ไม่จำกัดเฉพาะกระบวนพิจารณาตามกฎหมายเท่านั้น แต่ยังรวมถึงการดำเนินการทางแพ่งหรือทางอาญา (รวมถึงการดำเนินการนอกศาลและขั้นตอนก่อนฟ้องคดี) และการดำเนินการทางปกครอง เช่น การให้ข้อมูลแก่หน่วยงานกำกับดูแลในขั้นตอนการค้นหาข้อเท็จจริงและพยานหลักฐาน
2) **ความยินยอมของเจ้าของข้อมูลส่วนบุคคล** โดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลแล้ว
3) **ความจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา** หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
4) **การกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล**
5) **การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ** ของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6) **ความจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ**

ขั้นที่ 3 หากไม่เข้าข้อยกเว้น ให้พิจารณา "ความเพียงพอ" ของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง

เมื่อการส่งหรือโอนไม่เข้าข้อยกเว้นตามขั้นที่ 2 หน่วยงานต้องพิจารณาว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่จะรับข้อมูลนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ หากเพียงพอจึงจะส่งหรือโอนได้ โดยการพิจารณาความเพียงพอให้พิจารณาปัจจัย ดังนี้

- **กรอบกฎหมาย (Legal Framework)** มีมาตรการหรือกลไกทางกฎหมายที่สอดคล้องกับประเทศไทย โดยเฉพาะในเรื่อง
  - มาตรการรักษาความปลอดภัยและมาตรการคุ้มครองข้อมูลที่เหมาะสม
  - การบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้
  - มาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ ทั้งนี้ ไม่จำเป็นต้องเป็นกฎหมายเฉพาะแบบพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่พิจารณาจากองค์ประกอบของกลไก ไม่ว่าจะปรากฏอยู่ในกฎหมายฉบับใด
- **หน่วยงานผู้บังคับใช้กฎหมาย (Regulator)** มีหน่วยงานที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่มีปัญหาว่าประเทศปลายทางมีมาตรฐานที่เพียงพอหรือไม่ ให้เสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อวินิจฉัย โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เป็นผู้เสนอ ไม่ว่าจะเป็นการรับเรื่องจากผู้ควบคุมข้อมูลส่วนบุคคลหรือ สคส. เสนอเอง คณะกรรมการอาจวินิจฉัยเป็นรายกรณีหรือกำหนดเป็นรายชื่อประเทศ/ภูมิภาค (whitelist) ก็ได้ และเมื่อมีหลักฐานใหม่หรือกรณีอื่นอันสมควร เช่น ประเทศที่เคยได้รับการรับรองหย่อนมาตรฐานลง สคส. อาจขอให้คณะกรรมการทบทวนคำวินิจฉัยใหม่ได้

ขั้นที่ 4 กรณีส่งภายในเครือกิจการ/เครือธุรกิจเดียวกัน: นโยบายคุ้มครองข้อมูล (BCR) ตามมาตรา 29

หากหน่วยงานจำเป็นต้องส่งข้อมูลไปยังหน่วยงานอื่นที่ตั้งอยู่ในต่างประเทศแต่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน หน่วยงานสามารถใช้กลไกตามมาตรา 29 ได้ กล่าวคือ หากผู้ส่งและผู้รับข้อมูลได้จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding Corporate Rules: BCR) ที่ได้รับการตรวจสอบและรับรองจาก สคส. แล้ว จึงสามารถส่งหรือโอนข้อมูลได้ โดยไม่ต้องพิจารณาความเพียงพอของมาตรฐานการคุ้มครองของประเทศปลายทางตามมาตรา 28

[เครือกิจการหรือเครือธุรกิจเดียวกัน] "เครือกิจการหรือเครือธุรกิจเดียวกัน" หมายถึง กิจการที่ผู้ประกอบกิจการมีอำนาจควบคุมหรือบริหารจัดการเหนือกิจการอื่น หรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือกิจการอื่น ในรูปแบบบริษัทใหญ่ บริษัทย่อย หรือบริษัทร่วม รวมทั้งบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันทางกฎหมายหรือเกี่ยวข้องกันเนื่องจากประกอบธุรกิจหรือกิจการร่วมกัน โดยใช้หลักเกณฑ์การพิจารณาตามกฎหมายที่เกี่ยวข้องและมาตรฐานทางบัญชีอันเป็นที่ยอมรับโดยทั่วไป

[BCR] นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding Corporate Rules: BCR) หมายถึง นโยบายหรือข้อตกลงในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ส่งหรือโอนข้อมูลและผู้รับข้อมูลตกลงร่วมกันและมีผลผูกพัน เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมระหว่างเครือกิจการหรือเครือธุรกิจเดียวกัน โดยต้องได้รับการตรวจสอบและรับรองจาก สคส. ทั้งนี้ การยื่น BCR ให้ สคส. ตรวจสอบและรับรอง สามารถกระทำได้โดยการยื่นโดยตรง ทางไปรษณีย์ หรือช่องทางอิเล็กทรอนิกส์อื่นตามที่ประกาศกำหนด

[สาระสำคัญของ BCR] สาระสำคัญที่ BCR ต้องมี ได้แก่

(1) มีผลและสภาพบังคับในทางกฎหมาย สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และผูกพันผู้เกี่ยวข้อง เช่น บุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องของผู้ส่งและผู้รับ

(2) มีการรับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และการร้องเรียน

(3) มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมาย

ขั้นที่ 5 กรณีไม่มี BCR หรือยังไม่มีคำวินิจฉัย: มาตรการคุ้มครองที่เหมาะสม (Appropriate Safeguards)

ในกรณีที่ยังไม่มีคำวินิจฉัยเกี่ยวกับความเพียงพอของมาตรฐานประเทศปลายทางตามมาตรา 28 หรือยังไม่มี BCR ตามมาตรา 29 ผู้ส่งหรือโอนข้อมูลยังสามารถส่งหรือโอนข้อมูลไปยังประเทศปลายทางได้ โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28 หากได้จัดให้มี มาตรการคุ้มครองที่เหมาะสม (Appropriate Safeguards) ซึ่งอาจอยู่ในรูปแบบใดรูปแบบหนึ่ง ดังนี้

- ข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคล ที่เป็นข้อสัญญาในการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับการโอนข้อมูลข้ามพรมแดน ทั้งนี้ ข้อสัญญาที่คู่สัญญาจัดทำขึ้นตามกฎหมายของต่างประเทศหรือจัดทำโดยองค์การระหว่างประเทศที่นำมาใช้ได้ เช่น ASEAN Model Contractual Clauses for Cross Border Data Flows และ Standard Contractual Clauses (SCCs) สำหรับการโอนข้อมูลไปยังประเทศที่สาม รวมถึงข้อสัญญาอื่นตามที่คณะกรรมการฯ ประกาศกำหนด
- การรับรอง (Certification) ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการโอนข้อมูลข้ามพรมแดนว่ามีมาตรการคุ้มครองข้อมูลที่เหมาะสมตามมาตรฐานที่เป็นที่ยอมรับ
- ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสารหรือข้อตกลงที่มีผลผูกพันทางกฎหมายและใช้บังคับได้ระหว่างหน่วยงานรัฐของไทยกับหน่วยงานรัฐของประเทศอื่น ในกรณีการโอนข้อมูลระหว่างหน่วยงานรัฐไทยกับหน่วยงานรัฐอื่น

สำหรับ ข้อสัญญาการส่งหรือโอนข้อมูล ที่จัดทำขึ้นเอง ต้องมีเนื้อหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยในเรื่อง

(1) การประมวลผลต้องเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
(2) มาตรการรักษาความปลอดภัยขั้นต่ำ
(3) เงื่อนไขการรับข้อมูลของผู้ประมวลผลข้อมูลส่วนบุคคล
(4) การแจ้งเหตุละเมิดข้อมูล และ
(5) มาตรการเยียวยา

ส่วนข้อสัญญาซึ่งจัดขึ้นตามกฎหมายต่างประเทศ ต้องมีเนื้อหาครอบคลุมเรื่องการแจ้งการโอน การจำกัดการส่งเท่าที่จำเป็น ทางเลือกในการยกเลิกการโอนให้บุคคลภายนอกหรือนอกวัตถุประสงค์ การ

กำหนดความรับผิดชอบในการโอนไว้ในสัญญา การรักษาความมั่นคงปลอดภัย การกำหนดสิทธิการเข้าถึงข้อมูล และมาตรการเยียวยาทางกฎหมาย ทั้งนี้ โดยปกติข้อสัญญาตามกฎหมายต่างประเทศจะแก้ไขไม่ได้ เว้นแต่การแก้ไขนั้นไม่ขัดกับเนื้อหาข้างต้นและไม่กระทบสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เช่น การอ้างอิงกฎหมายที่ใช้บังคับ การเพิ่มเติมมาตรการคุ้มครองที่เหมาะสม หรือการแก้ไขเนื้อหาที่ไม่ใช่สาระสำคัญ เป็นต้น

3.5 การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) คือ สัญญาหรือเอกสารทางกฎหมายที่มีผลผูกพันระหว่างผู้ควบคุมข้อมูลส่วนบุคคลรายหนึ่งและผู้ประมวลผลข้อมูลส่วนบุคคลอีกรายหนึ่ง ซึ่งกำหนดขึ้นเพื่อควบคุมการประมวลผลข้อมูลส่วนบุคคลในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของตน ข้อตกลงนี้เป็นเครื่องมือสำคัญในการจัดสรรหน้าที่และความรับผิด และสร้างความมั่นใจว่าการประมวลผลจะเป็นไปตามมาตรฐานที่กฎหมายกำหนด

[ความเป็นสัญญาอุปกรณ์] ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) เป็นสัญญาอุปกรณ์ กล่าวคือ ไม่ได้เป็นสัญญาที่ดำรงอยู่ได้โดยอิสระ แต่เป็นสัญญาแนบท้ายไปกับสัญญาประธาน ซึ่งเป็นสัญญาหลักที่กำหนดความสัมพันธ์ทางธุรกิจหรือการว่าจ้างระหว่างคู่สัญญา เมื่อเมื่อสัญญาประธานสิ้นสุดลง ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลจะกำหนดหน้าที่สุดท้ายของผู้ประมวลผลข้อมูลส่วนบุคคล คือการลบหรือส่งคืนข้อมูลทั้งหมดตามที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้

ตัวอย่างกิจกรรม “การว่าจ้างบริการบริหารจัดการเงินเดือนพนักงาน (Payroll Administration)”

สัญญาประธาน คือ สัญญาจ้างบริการบริหารจัดการเงินเดือนพนักงาน

- คู่สัญญา: บริษัท A ผู้ว่าจ้าง และ บริษัท B ผู้รับจ้าง
- เนื้อหาหลัก: กำหนดขอบเขตงานว่า บริษัท B ต้องคำนวณเงินเดือน, หักภาษี ณ ที่จ่าย, และดำเนินการโอนเงินเข้าบัญชีพนักงานของบริษัท A ภายในวันที่กำหนด รวมถึงอัตราค่าจ้างบริการที่บริษัท A ต้องจ่ายให้บริษัท B

สัญญาอุปกรณ์ คือ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

- เนื้อหา: เนื่องจากบริษัท B ต้องเข้าถึงข้อมูล ชื่อ-นามสกุล, เลขบัญชีธนาคาร, และเงินเงินเดือนของพนักงาน ข้อตกลงจึงถูกทำขึ้นเพื่อกำหนดวิธีการจัดการข้อมูลเหล่านี้ให้ปลอดภัย:
    - คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล: บริษัท B ต้องใช้ข้อมูลพนักงานเพื่อวัตถุประสงค์ในการจ่ายเงินเดือนตามสัญญาจ้างเท่านั้น ห้ามนำไปใช้เพื่อประโยชน์อื่น

- มาตรการความปลอดภัย: บริษัท B ต้องใช้ระบบจัดเก็บข้อมูลที่มีการเข้ารหัสและจำกัดสิทธิการเข้าถึง
- สิทธิการตรวจสอบ (Audit): บริษัท A มีสิทธิเข้าตรวจสอบระบบของบริษัท B เพื่อให้มั่นใจว่าข้อมูลพนักงานมีความมั่นคงปลอดภัยตามที่ตกลงกันไว้ในข้อตกลง

[องค์ประกอบ] เพื่อให้ข้อตกลงมีความสมบูรณ์และคุ้มครองทั้งสองฝ่าย จึงควรมีองค์ประกอบที่สำคัญของข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

1) สาระสำคัญของการประมวลผลข้อมูลส่วนบุคคล
2) ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล
3) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
4) ประเภทของข้อมูลส่วนบุคคลที่นำมาประมวลผล
5) ประเภทของเจ้าของข้อมูลส่วนบุคคล
6) สิทธิ หน้าที่ และความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

3.6 การจัดให้มีช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (DSAR)

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องกำหนดจัดเตรียมให้มีช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่สะดวกและเข้าถึงง่าย เพื่อให้สามารถเข้ามาใช้สิทธิต่าง ๆ

[ระยะเวลาดำเนินการ] ผู้ควบคุมข้อมูลส่วนบุคคลมีหนาที่จะต่องดำเนินการตามสิทธิเมื่อเจ้าของข้อมูลส่วนบุคคลร่องขอโดยไม่ชักช้า ภายใน 30 วันนับแต่วันที่ได้รับคำขอ เว้นแต่ สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed) ซึ่งเป็นสิทธิที่แม้เจ้าของข้อมูลส่วนบุคคลไม่ได้ร้องขอ แต่ผู้ควบคุมข้อมูลส่วนบุคคลก็ต้องดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบตามที่กฎหมายกำหนดตามมาตรา 23

[ขั้นตอนการดำเนินการ] เมื่อองค์กรได้รับคำร้องขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล องค์กรมีหน้าที่ต้องดำเนินการพิจารณาและตอบสนองต่อคำร้องดังกล่าวให้เสร็จสิ้นภายในระยะเวลา 30 วันนับแต่วันที่ได้รับคำร้อง โดยมีขั้นตอนที่เป็นข้อแนะนำดังต่อไปนี้

1) การตรวจสอบและพิสูจน์ตัวตนผู้ยื่นคำร้อง (Data Subject Authentication)

ก่อนเริ่มกระบวนการค้นหาหรือเปิดเผยข้อมูล องค์กรต้องจัดให้มีกระบวนการตรวจสอบเพื่อยืนยันตัวตน ของผู้ยื่นคำร้องอย่างเคร่งครัด เพื่อป้องกันความเสี่ยงด้านความปลอดภัยของข้อมูล และป้องกันการเข้าถึงข้อมูลโดยมิชอบจากการสวมรอย โดยมีแนวทางปฏิบัติดังนี้

- กรณีผู้ยื่นคำร้องเป็นเจ้าของข้อมูลส่วนบุคคลโดยตรง: ต้องตรวจสอบเอกสารหลักฐานที่ออกโดยราชการซึ่งยังไม่หมดอายุ เช่น บัตรประจำตัวประชาชน หรือหนังสือเดินทาง หรือตรวจสอบผ่านระบบการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์ที่องค์กรกำหนด
- กรณีการมอบอำนาจ: ต้องตรวจสอบหนังสือมอบอำนาจที่ถูกต้องตามกฎหมาย พร้อมสำเนาเอกสารแสดงตนที่มีการลงนามรับรองสำเนาถูกต้องของทั้งผู้มอบอำนาจและผู้รับมอบอำนาจอย่างครบถ้วน

2) การสืบค้นและรวบรวมชุดข้อมูลส่วนบุคคล (Data Retrieval and Verification)

เมื่อกระบวนการพิสูจน์ตัวตนเสร็จสิ้นและถูกต้อง ให้ดำเนินการสืบค้น รวบรวม และตรวจสอบชุดข้อมูลส่วนบุคคลตามขอบเขตที่ระบุในคำร้อง

- ตรวจสอบฐานข้อมูลระบุตัวตน ประวัติการทำธุรกรรม ประวัติการซื้อสินค้าหรือบริการ รวมถึงข้อมูลการติดต่อสื่อสาร เช่น บันทึกการสนทนากับศูนย์บริการลูกค้า หรือประวัติการแชท ที่อยู่ในความครอบคลุมดูแลขององค์กร
- จัดเตรียมชุดข้อมูลดังกล่าวให้อยู่ในรูปแบบสำเนาเอกสาร หรือรูปแบบอิเล็กทรอนิกส์ที่สามารถอ่านหรือใช้งานได้โดยทั่วไป เพื่อเตรียมส่งมอบให้แก่เจ้าของข้อมูลส่วนบุคคล

3) การคัดกรองและปกปิดข้อมูลของบุคคลอื่น (Data Redaction)

เพื่อป้องกันการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลภายนอก องค์กรต้องทำการตรวจทานอย่างละเอียดก่อนส่งมอบสำเนาข้อมูล โดยกำหนดมาตรการปกปิดข้อมูล (Redaction) ดังนี้

- การปิดทึบหรือบดบังข้อมูล (Masking/Blurring): ในกรณีที่ชุดข้อมูลมีลักษณะเป็นภาพถ่าย ภาพเคลื่อนไหว หรือเอกสารที่มีข้อมูลของบุคคลที่สามปรากฏอยู่ เช่น รายงานการประชุม หรือภาพบันทึกจากระบบสารสนเทศ ต้องดำเนินการเบลอใบหน้า เซนเซอร์ หรือปิดทับชื่อ-นามสกุล และข้อมูลติดต่อของบุคคลอื่นทั้งหมด
- การตัดทอนข้อมูล: หากชุดข้อมูลอยู่ในรูปแบบประวัติการสนทนาหรือข้อความแชท ต้องลบข้อมูลหรือความเห็นส่วนบุคคลของพนักงานหรือบุคคลอื่นที่ไม่มีความเกี่ยวข้องกับสิทธิของตัวผู้ยื่นคำร้องออกให้หมดสิ้น เพื่อคงไว้เฉพาะข้อมูลที่เป็นสิทธิโดยชอบธรรมของเจ้าของข้อมูลส่วนบุคคลรายนั้น ๆ เท่านั้น

3.7 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach)

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดให้มีช่องทางรับแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแผนการรับมือ เพื่อให้สามารถแก้ไขสถานการณ์ได้ทันท่วงที และดำเนินการตามประกาศ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

[นิยามและประเภทของการละเมิด] "การละเมิดข้อมูลส่วนบุคคล" หมายถึง การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ตามหลัก CIA ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ ข้อผิดพลาดบกพร่อง อุบัติเหตุ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ หรือเหตุอื่นใด และไม่ขึ้นอยู่กับว่าผู้กระทำละเมิดจะเป็นใคร ซึ่งอาจเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล พนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลภายนอก โดยแบ่งได้เป็น 3 ประเภท

1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality) การเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity) การเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability) การทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลจนไม่อยู่ในสภาพพร้อมใช้งานตามปกติ ไม่ว่าจะถาวรหรือชั่วคราว

หน่วยงานควรดำเนินการตามลำดับ ดังนี้

ขั้นที่ 1 ทราบเหตุและตรวจสอบยืนยันเหตุการละเมิด

เมื่อหน่วยงานทราบหรือได้รับแจ้งเหตุ ให้ประเมินความน่าเชื่อถือและตรวจสอบข้อเท็จจริงว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดหรือไม่ โดยพึงตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยทั้งมาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการทางกายภาพ เพื่อยืนยันว่ามีการละเมิดเกิดขึ้นจริงหรือไม่

หากระหว่างตรวจสอบพบว่าเหตุการละเมิดมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล ให้หน่วยงานดำเนินการเอง หรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดสิ้นสุดหรือไม่ส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะกระทำได้ โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

ขั้นที่ 2 ประเมินความเสี่ยงของเหตุการละเมิด

[ปัจจัยการประเมินความเสี่ยงของเหตุการละเมิด] หน่วยงานต้องประเมินความเสี่ยงโดยพิจารณาปัจจัยประกอบกัน ได้แก่

1) ลักษณะและประเภทของการละเมิด
2) ลักษณะหรือประเภทของข้อมูลส่วนบุคคล
3) ปริมาณของข้อมูลส่วนบุคคล ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ที่เกี่ยวข้อง
4) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อจำกัดในการปกป้องสิทธิของตนเอง
5) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของหน่วยงานหรือต่อสาธารณะ
6) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (บุคคลธรรมดา/นิติบุคคล ตลอดจนขนาดและลักษณะของกิจการ)
7) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ใช้หรือจะใช้
8) ลักษณะของระบบจัดเก็บข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ขั้นที่ 3 พิจารณาว่าก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของบุคคลหรือไม่

หากประเมินแล้ว พบว่าไม่มีความเสี่ยง อาจจะพิจารณาไม่ต้องแจ้งต่อ สคส. แต่หากประเมินแล้วพบว่ามีความเสี่ยง ต้องดำเนินการแจ้งเหตุการละเมิดนั้นต่อ สคส.

ในกรณีที่ประเมินแล้ว ไม่มีความเสี่ยง เช่น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หรือข้อมูลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ เช่น ทำ Anonymization, Pseudonymization หรือ Encryption ไว้ หน่วยงานยังควรบันทึกเหตุการณ์ หลักฐาน และข้อมูล/เอกสาร/มาตรฐานการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องไว้ เพื่ออธิบายการประเมินความเสี่ยง และใช้เป็นหลักฐานกรณีตรวจสอบย้อนหลัง

ขั้นที่ 4 พิจารณาว่าเป็นความเสี่ยงที่ร้ายแรงต่อสิทธิเสรีภาพหรือไม่

หากเป็นความเสี่ยงร้ายแรงหน่วยงานต้องแจ้งเหตุการละเมิดต่อเจ้าของข้อมูลส่วนบุคคลด้วย เพื่อให้เจ้าของข้อมูลส่วนบุคคลทราบและป้องกันตนเองได้ หากพิจารณาแล้วเห็นว่าไม่ร้ายแรงสามารถแจ้งเพียง สคส. โดยไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลได้

ขั้นที่ 5 แจ้งต่อ สคส. และ/หรือเจ้าของข้อมูลส่วนบุคคล

[การแจ้งเหตุการละเมิดต่อ สคส.]

- **[รูปแบบ]** แจ้งเป็นลายลักษณ์อักษรส่งไปที่สำนักงาน หรือแจ้งผ่านวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นตามที่ สคส. กำหนด เช่น ทางไปรษณีย์อิเล็กทรอนิกส์ saraban@pdpc.or.th
- **[เนื้อหา]** แจ้งเท่าที่จะสามารถกระทำได้ โดยเนื้อหาในการแจ้งมีความคล้ายกับข้อมูลที่ใช้ประเมินความเสี่ยง ได้แก่
  (1) ลักษณะและประเภทของเหตุการละเมิด โดยอาจบรรยายลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ที่เกี่ยวข้อง
  (2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือบุคคลที่ได้รับมอบหมายให้ประสานงานและให้ข้อมูลเพิ่มเติม
  (3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้น
  (4) ข้อมูลเกี่ยวกับมาตรการที่หน่วยงานใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิด หรือเยียวยาความเสียหาย
- **[ระยะเวลา]** ต้องแจ้งโดยไม่ชักช้า (without undue delay) ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ (aware) หรือมีเหตุอันควรเชื่อได้ว่ามีการละเมิดเกิดขึ้นจริง

[การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคล] เฉพาะกรณีที่ความเสี่ยงร้ายแรงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หน่วยงานต้องแจ้งเจ้าของข้อมูลส่วนบุคคลด้วย

- **[รูปแบบ]** แจ้งเป็นรายบุคคลเป็นหนังสือหรือทางช่องทางอิเล็กทรอนิกส์ หากโดยสภาพไม่สามารถแจ้งรายบุคคลได้ ให้แจ้งเป็นกลุ่มหรือผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่น โดยไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล
- **[เนื้อหา]** จะมีความคล้ายคลึงกับที่แจ้ง สคส. แต่จะมีรายละเอียดเพิ่มอีก 2 ประการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลเตรียมรับมือและใช้สิทธิได้ คือ (1) แนวทางการเยียวยาความเสียหายและมาตรการที่หน่วยงานใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิด และ (2) ข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิด หรือเยียวยาความเสียหาย รวมถึงลักษณะของการละเมิด ผลกระทบที่อาจเกิดขึ้น และชื่อ/สถานที่ติดต่อของ DPO หรือผู้ประสานงาน
- **[ระยะเวลา]** แจ้งโดยไม่ชักช้า (without undue delay) เพื่อให้เจ้าของข้อมูลส่วนบุคคลเตรียมป้องกัน ระงับ แก้ไข หรือเยียวยาความเสียหายได้ทันท่วงที

[กรณีมีสัญญาการประมวลผลข้อมูล (DPA)] เมื่อหน่วยงานจัดให้มีข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับผู้ประมวลผลข้อมูลส่วนบุคคล หน่วยงานต้องระบุ

ไว้ใน DPA ให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่หน่วยงาน (ผู้ควบคุมข้อมูลส่วนบุคคล) โดยไม่ชักช้า (without undue delay) ภายใน 72 ชั่วโมง นับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุ เท่าที่จะสามารถกระทำได้ (where feasible) ทั้งนี้ อาจตกลงให้ระยะเวลาสั้นกว่านี้ได้ เพื่ออำนวยความสะดวกให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถมีระยะเวลาในการประเมินความเสี่ยงและดำเนินการอื่น ๆ ได้ทันท่วงที

[มาตรการรับมือและฟื้นฟูภายหลังเกิดเหตุ] ภายหลังเกิดเหตุ หน่วยงานต้องใช้มาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิด รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยให้มีประสิทธิภาพเหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

3.8 การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเข้าลักษณะตามมาตรา 41 ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) โดยหน่วยงานที่ต้องจัดให้มี DPO ได้แก่

1) **[มาตรา 41 (1)]** ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
2) **[มาตรา 41 (2)]** ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
3) **[มาตรา 41 (3)]** ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งมีกิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 เช่น ข้อมูลสุขภาพ ศาสนาพันธุกรรม หรือประวัติอาชญากรรม เป็นต้น

[หลักเกณฑ์พิจารณากรณีตามมาตรา 41 (2)] หน่วยงานต้องพิจารณาองค์ประกอบ 3 ส่วนประกอบกัน ได้แก่

1) **เป็นกิจกรรมหลัก (Core activities)** กิจกรรมหลัก หมายถึง กิจกรรมที่จำเป็นและมีความสำคัญเพื่อบรรลุวัตถุประสงค์หรือเป้าหมายหลักในการดำเนินงานในกิจการหรือภารกิจของหน่วยงาน ซึ่งต่างจากกิจกรรมเสริม (Ancillary activities) ที่เป็นเพียงการ

สนับสนุน เช่น การจ่ายเงินเดือนพนักงาน หรือการสนับสนุนงานด้าน IT ตัวอย่างเช่น บริษัทรับจ้างรักษาความปลอดภัย: การเก็บข้อมูลส่วนบุคคลจากกล้องวงจรปิดถือเป็น "กิจกรรมหลัก" ขณะที่การซ่อมแซมกล้องวงจรปิดถือเป็น "กิจกรรมเสริม"

2) **จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ** การประมวลผลนั้นต้องมีลักษณะที่ต้องติดตามหรือตรวจสอบข้อมูลหรือระบบเป็นประจำและเป็นระบบ (regular and systematic monitoring)
3) **มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (Large scale)** โดยพิจารณาปริมาณข้อมูล จำนวนเจ้าของข้อมูลส่วนบุคคล และขอบเขตของการประมวลผลประกอบกัน

ทั้งนี้ ในการพิจารณาว่าเข้าเงื่อนไขข้างต้นหรือไม่ หน่วยงานต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลประกอบด้วย เพื่อให้การจัดให้มี DPO เป็นไปอย่างเหมาะสมกับลักษณะและระดับความเสี่ยงของการประมวลผล

[บทบาทและหน้าที่ของ DPO] เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลภายในหน่วยงานเป็นไปอย่างมีประสิทธิภาพ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีบทบาทและหน้าที่ ดังนี้

1) ให้คำแนะนำและตรวจสอบการดำเนินงานภายในของหน่วยงานเพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
3) รักษาความลับที่ได้มาจากการปฏิบัติหน้าที่
4) ได้รับความคุ้มครองในการปฏิบัติงาน เพื่อให้สามารถมีอิสระในการปฏิบัติหน้าที่ให้ความเห็นหรือตรวจสอบได้อย่างเป็นกลางและเป็นอิสระ

[แนวทางการปฏิบัติงานของ DPO] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรทำงานด้วยวิธีการที่คำนึงถึงความเสี่ยง (Risk-based Approach) โดยให้ความสำคัญกับกิจกรรม ปัญหา หรือข้อมูลที่มีความเสี่ยงสูงเป็นลำดับต้น แต่ต้องไม่ละเลยการดูแลการประมวลผลที่มีความเสี่ยงต่ำ และต้องดูแลตรวจสอบข้อมูลให้เหมาะสมกับประเภทของเจ้าของข้อมูลส่วนบุคคล

[บทบาทของ DPO ในการแจ้งเหตุการละเมิด] ในกรณีที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพบเหตุการละเมิดข้อมูลส่วนบุคคล DPO ต้องรีบดำเนินการเพื่อให้หน่วยงานแจ้งเหตุการละเมิดต่อ สคส. โดยไม่ชักช้า ภายในระยะเวลาไม่เกิน 72 ชั่วโมง เว้นแต่กรณีที่ไม่มีแนวโน้มก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และหากไม่สามารถแจ้งภายใน 72 ชั่วโมงได้ ต้องชี้แจงถึงสาเหตุที่ดำเนินการล่าช้า ทั้งนี้ เฉพาะเหตุการละเมิดที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล DPO และหน่วยงานจึงมีหน้าที่แจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลด้วย

3.9 การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate Security Measures) ตามมาตรา 37 (1) แม้หน่วยงานจะได้รับยกเว้นไม่ต้องนำ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯมาใช้บังคับไม่ว่าทั้งหมดหรือบางส่วน หน่วยงานก็ยังต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย

[นิยามความมั่นคงปลอดภัย] หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

[หน้าที่ตามมาตรา 37 (1)] ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล และต้องทบทวน/ตรวจสอบมาตรการดังกล่าวเมื่อ (1) มีความจำเป็น หรือ (2) เมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้ยังคงมีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

[มาตรการขั้นต่ำ] มาตรการรักษาความมั่นคงปลอดภัยของหน่วยงานอย่างน้อยต้องประกอบด้วย

- การควบคุมการเข้าถึง (Access control)
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
- การกำหนดความรับผิดชอบของผู้ใช้งาน (User responsibility)
- การตรวจสอบย้อนหลัง (Audit trails)

[หลักการทั่วไปของการรักษาความมั่นคงปลอดภัย] นอกจากมาตรการขั้นต่ำแล้ว มาตรการของหน่วยงานต้องเป็นไปตามหลักการทั่วไป ดังนี้

- ครอบคลุมข้อมูลทุกรูปแบบและทุกมิติ ต้องครอบคลุมข้อมูลในรูปแบบต่าง ๆ (เอกสาร อิเล็กทรอนิกส์ และอื่น ๆ) และประกอบด้วยมาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการทางกายภาพ โดยคำนึงถึงความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย ตลอดจนโอกาสและผลกระทบจากการละเมิดข้อมูลส่วนบุคคล
- ครอบคลุมวงจรการดำเนินการด้านความมั่นคงปลอดภัย อย่างน้อยต้องมีการระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจสอบและเฝ้าระวัง การเผชิญเหตุละเมิดข้อมูลส่วนบุคคล และการรักษา/ฟื้นฟูความเสียหาย
- รักษาความมั่นคงปลอดภัยอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึง (1) ปัจจัยทางเทคโนโลยี (2) บริบทสภาพแวดล้อม (3) มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงาน

หรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน (4) ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผย (5) ทรัพยากรที่ต้องใช้ และ (6) ความเป็นไปได้ในการดำเนินการประกอบกัน

- การป้องกันเชิงลึก (Defense in depth) สำหรับการประมวลผลในรูปแบบอิเล็กทรอนิกส์ มาตรการต้องครอบคลุมระบบสารสนเทศที่เกี่ยวข้อง โดยพิจารณาใช้มาตรการป้องกันหลายชั้น (multiple layers of security controls) อย่างเหมาะสมตามระดับความเสี่ยง เพื่อลดความเสี่ยงในกรณีที่มาตรการบางอย่างมีข้อจำกัดในบางสถานการณ์
- การเสริมสร้างความตระหนักรู้ ต้องมีการเสริมสร้างความตระหนักรู้และแจ้งนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูลให้แก่ทุกคนที่เกี่ยวข้อง

[เหตุและปัจจัยในการทบทวนมาตรการ] หน่วยงานต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยเมื่อ (1) มีความจำเป็น (2) เทคโนโลยีเปลี่ยนแปลงไป หรือ (3) มีเหตุละเมิดข้อมูลส่วนบุคคล (เว้นแต่การละเมิดนั้นไม่มีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล) โดยการทบทวนให้คำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการประมวลผล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

[มาตรการของผู้ประมวลผลข้อมูลส่วนบุคคล] ในการจัดให้มีข้อตกลงระหว่างหน่วยงานกับผู้ประมวลผลข้อมูลส่วนบุคคล (DPA) หน่วยงานควรกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี (1) มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และ (2) การแจ้งเหตุละเมิดให้หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลทราบ ซึ่งสอดคล้องกับหน้าที่ตามมาตรา 40 (2)

[มาตรการตามกฎหมายอื่น] เมื่อมีกฎหมายอื่นกำหนดให้หน่วยงานจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย มาตรการดังกล่าวก็ต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดด้วย

[กรณีหน่วยงานที่ได้รับยกเว้น] สำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องนำพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯมาใช้บังคับตามมาตรา 4 เช่น การเก็บข้อมูลเพื่อประโยชน์ส่วนตัว/ครอบครัว หน่วยงานของรัฐด้านความมั่นคง กิจการสื่อมวลชน สภาผู้แทนราษฎร/วุฒิสภา การพิจารณาพิพากษาคดีของศาล และข้อมูลของบริษัทข้อมูลเครดิต ตลอดจนกิจการที่ได้รับยกเว้นบางส่วนตามพระราชกฤษฎีกาที่เกี่ยวข้อง หน่วยงานเหล่านี้ยังคงต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามมาตรฐานที่กำหนด

4. หน้าที่ของหน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

ก่อนจะพิจารณาหน้าที่ของหน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล พึงต้องพิจารณาบทบาทของหน่วยงานว่ามีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเสียก่อน

[พิจารณาบทบาทตามความเป็นจริง] สถานะของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลถือเป็นแนวคิดเชิงหน้าที่ (Functional Concept) ซึ่งมุ่งเน้นการจัดสรรความรับผิดชอบตามบทบาทที่เกิดขึ้นจริง ในทางปฏิบัติ การพิจารณาสถานะทางกฎหมายจึงต้องยึดตามข้อเท็จจริงในแต่ละกิจกรรม (Case-by-case Basis) มากกว่าข้อความที่ระบุไว้ในข้อตกลงหรือสัญญา ทั้งนี้ บทบาทดังกล่าวถูกกำหนดโดยพฤติการณ์จริงของการดำเนินงาน จึงไม่สามารถเจรจาต่อรองเพื่อเปลี่ยนแปลงสถานะให้ขัดต่อความเป็นจริงได้

[ผู้ประมวลผลข้อมูลส่วนบุคคล] ความเป็นผู้ประมวลผลข้อมูลส่วนบุคคลประกอบด้วย 2 องค์ประกอบหลัก ดังนี้

1) บุคคลธรรมดาหรือนิติบุคคล (Natural or Legal Person)
2) ดำเนินการในนามของผู้ควบคุมข้อมูล (On behalf of the Controller)

ผู้ประมวลผลข้อมูลส่วนบุคคลให้บริการเพื่อตอบสนองวัตถุประสงค์และประโยชน์ของผู้ควบคุมข้อมูลโดยเปรียบเสมือนการได้รับมอบหมายงานมาทำ โดยผู้ประมวลผลข้อมูลส่วนบุคคลต้องประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น และไม่สามารถนำข้อมูลไปใช้เพื่อวัตถุประสงค์ของตนเองได้

[อำนาจการตัดสินใจในวิธีการที่ไม่เป็นสาระสำคัญ] ผู้ประมวลผลข้อมูลสามารถตัดสินใจในรายละเอียดทางเทคนิคหรือการปฏิบัติงานได้ เช่น การเลือกใช้ซอฟต์แวร์ ฮาร์ดแวร์ หรือมาตรการความปลอดภัยในรายละเอียด

หน้าที่สำคัญที่หน่วยงานต้องปฏิบัติเมื่อมีบทบาทผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

หน้าที่ของหน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล		
ลำดับ	**หน้าที่**	**มาตราที่เกี่ยวข้อง**
1	การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	40 (3)
2	การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ	40 (2)
3	การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	41
4	การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	40 (2)
5	ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)	40

ตาราง 2 หน้าที่ของหน่วยงาน ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

4.1 การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 โดยมีรายละเอียดสำคัญที่แตกต่างจากกรณีของผู้ควบคุมข้อมูลส่วนบุคคล คือ การระบุข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล โดยจะต้องระบุชื่อ และรายละเอียดติดต่อของผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคล ได้ดำเนินการจัดการข้อมูลให้ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น

4.2 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลหน่วยงาน ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคล[29] โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน หรือมีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลเกิดขึ้นจริง เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการตามกฎหมายต่อไปได้อย่างทันท่วงทีโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน หรือนับแต่มีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลเกิดขึ้นจริง[30]

ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้พบเหตุละเมิดของข้อมูลส่วนบุคคล ต้องแจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลโดยทันทีหลังทราบว่ามีการละเมิดข้อมูลส่วนบุคคลเมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งการละเมิดของข้อมูลส่วนบุคคลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุละเมิดต่อ สคส. เว้นแต่เหตุดังกล่าวมิได้ก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลอาจสามารถดำเนินการแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลได้ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบอำนาจในการดำเนินการตามความเหมาะสมแก่ผู้ ประมวลผลข้อมูลส่วนบุคคลโดยระบุไว้ในข้อสัญญาพึงระลึกไว้เสมอว่าหน้าที่รับผิดชอบในการแจ้งเตือนตามกฎหมายเป็นของผู้ควบคุม ข้อมูลส่วนบุคคลมิใช่หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

[29] มาตรา 40 (2) แห่งพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

[30] ข้อ 8 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

4.3 การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องพิจารณาแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยใช้หลักเกณฑ์เดียวกับกรณีของผู้ควบคุมข้อมูลส่วนบุคคลที่ได้กล่าวมาแล้วข้างต้น

หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์เหมือนกรณีผู้ควบคุมข้อมูลส่วนบุคคลที่ได้กล่าวมาแล้ว

4.4 การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

4.5 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล มีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล โดยมาตรา 40 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย ทั้งนี้ ข้อตกลงดังกล่าวอาจจัดทำเป็นสัญญาแยกต่างหากหรือผนวกเป็นส่วนหนึ่งของสัญญาให้บริการหลักก็ได้ หน่วยงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลจึงมีหน้าที่ต้องประมวลผลข้อมูลส่วนบุคคลทั้งตามหน้าที่ที่กฎหมายบัญญัติและตามที่ระบุในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล โดยหน้าที่ประการสำคัญได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเฉพาะตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในส่วนนั้น และต้องปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด นอกจากนี้ แม้ข้อตกลงจะกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลไว้แล้ว คู่สัญญาแต่ละฝ่ายก็ไม่สามารถอ้างข้อกำหนดในข้อตกลงดังกล่าวเพื่อให้ตนหลุดพ้นจากความรับผิดตามกฎหมายได้

[Data Processing Addendum] กรณีที่หน่วยงานพัฒนาหรือให้บริการแพลตฟอร์ม หรือแอปพลิเคชัน ส่วนใหญ่แล้วหน่วยงานจะทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลในลักษณะแนบท้ายสัญญาการให้บริการ (Data Processing Addendum) ที่เป็นข้อตกลงระหว่างผู้ให้บริการฝ่ายหนึ่ง และ

ผู้ใช้บริการอีกฝ่ายหนึ่ง ทั้งนี้ แม้หน่วยงานจะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ที่ต้องมีหน้าที่ ตามมาตรา 40 วรรคสาม การจัดทำ Data Processing Addendum เปรียบเสมือนการประกาศให้ผู้ใช้บริการได้ทราบรายละเอียดของการประมวลผลและเป็นการสร้างความน่าเชื่อถือ และที่สำคัญคือ ก่อให้เกิดความสะดวก เนื่องจากไม่ต้องทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลเป็นรายคู่สัญญา

5. โทษและความรับผิดของหน่วยงาน

[ลักษณะบทลงโทษ] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดความรับผิดทางแพ่ง โทษทางอาญา และโทษทางปกครองบทลงโทษไว้ 3 ประเภท เพื่อเอาผิดกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และบุคคลที่เกี่ยวข้อง ที่ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เพื่อให้เกิดความเคร่งครัดในการกำกับดูแล (Regulate) โดยทั่วไปองค์กรจะเป็นผู้รับผิดในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทางแพ่ง ไม่ว่าจงใจหรือประมาท แต่หากกรรมการหรือผู้บริหารที่รู้เห็นเป็นใจหรือละเลยไม่สั่งการป้องกัน จะต้องรับโทษอาญาส่วนตัวด้วย และหากเจ้าหน้าที่ควบคุมข้อมูลส่วนบุคคลได้รู้ข้อมูลจากการปฏิบัติหน้าที่แล้วนำไปเปิดเผยโดยไม่มีอำนาจ ย่อมต้องรับโทษอาญาเป็นการส่วนตัวเช่นกัน ซึ่งความรับผิดและโทษดังกล่าวแบ่งออกเป็น 3 ประเภท ได้แก่ ความรับผิดทางแพ่ง โทษทางอาญา และโทษทางปกครอง

5.1 ความรับผิดทางแพ่ง

ตามมาตรา 77 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดความรับผิดทางแพ่ง โดยหากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ และทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น ไม่ว่าการกระทำนั้นจะเกิดโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม

ความรับผิดทางแพ่งดังกล่าวมีลักษณะเป็นการกำหนด “ความรับผิดโดยเคร่งครัด (Strict Liability)”[31] กล่าวคือ ผู้เสียหายเพียงพิสูจน์ว่าเกิดความเสียหายจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล โดยไม่จำเป็นต้องพิสูจน์เจตนาหรือความประมาทของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล และภาระการพิสูจน์จะตกอยู่กับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่ต้องพิสูจน์ตามข้อยกเว้นที่จะทำให้ไม่ต้องรับผิดตามที่ปรากฏในมาตรา 77 วรรคหนึ่ง (1) และ (2) ได้แก่

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือ

[31] การกำหนด “ความรับผิดโดยเคร่งครัด (Strict Liability)” มีลักษณะเหมือนกับกฎหมายอื่น ๆ ได้แก่ พ.ร.บ. ความรับผิดต่อความเสียหายที่เกิดขึ้นจากสินค้าที่ไม่ปลอดภัย พ.ศ. 2551

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ทั้งนี้ในการชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดค่าสินไหมทดแทนทั้งหมด 2 ประเภท ได้แก่

- ค่าสินไหมทดแทนที่แท้จริง เมื่อการฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าจะจงใจหรือประมาทเลินเล่อหรือไม่ก็ตามมาตรา 77 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กล่าวคือ หน่วยงาน ต้องชดเชยค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคลตามความเสียหายจริงที่เกิดขึ้น
- ค่าสินไหมทดแทนเพื่อการลงโทษ (Punitive Damages) ซึ่งศาลอาจสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงตามที่เห็นสมควรแต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง ตามมาตรา 78 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

อย่างไรก็ตาม การเรียกค่าสินไหมทดแทนทั้งสองประเภทนั้น มีอายุความ 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิดหรือผู้รับผิด หรือ 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

<table>
<tr><th colspan="4">ตารางสรุปความรับผิดทางแพ่ง</th></tr>
<tr><th>บทกำหนดความรับผิด</th><th>ผู้กระทำความผิด</th><th>องค์ประกอบความรับผิด</th><th>ความรับผิด</th></tr>
<tr><td rowspan="3">ม. 77</td><td>ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล</td><td><u>Strict Liability</u>
- ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติ พ.ร.บ. นี้ (ไม่ว่าจะจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม) และ
- ทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล</td><td>- ค่าสินไหมทดแทนที่แท้จริง
- ค่าสินไหมทดแทนเพื่อการลงโทษ (ม. 78)</td></tr>
<tr><td colspan="2">ข้อยกเว้น</td></tr>
<tr><td colspan="2">- ความเสียหายเกิดจากเหตุสุดวิสัย
- ความเสียหายเกิดจากเจ้าของข้อมูลส่วนบุคคล
- ปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย</td></tr>
</table>

ตาราง 3 สรุปความรับผิดทางแพ่ง

5.2 โทษทางอาญา

ตามมาตรา 79 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดลักษณะของโทษทางอาญาไว้ 2 ลักษณะ ได้แก่ โทษปรับ และโทษจำคุก นอกจากนี้ยังซึ่งอาจสามารถลงโทษทั้งโทษปรับและโทษจำคุกไปพร้อมกันได้ โดยภายใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดโทษทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคล โดยแบ่งระดับโทษตามเจตนาและผลกระทบ ดังต่อไปนี้

- กรณีที่ 1
  (1) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือ
  (2) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ
  (3) โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย **โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย** ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- กรณีที่ 2
  (1) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือ
  (2) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ
  (3) โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย **เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย สำหรับตนเองหรือผู้อื่น** ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

นอกเหนือจากโทษทางอาญาที่บังคับลงโทษแก่ผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 79 แล้ว ในมาตรา 80 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ยังกำหนดโทษทางอาญาบังคับลงโทษแก่ **ผู้ที่ได้ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ** โดยไม่ว่าจะเป็นบุคคลจากฝั่งของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล และรวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลที่เจ้าหน้าที่ฯ มีหน้าที่ต้องเก็บรักษาความลับ โดย**หากผู้นั้นนำข้อมูลไปเปิดเผยแก่ผู้อื่น** ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ โดยมีข้อยกเว้นเฉพาะในกรณีที่เปิดเผยข้อมูลด้วยเหตุผล ดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

ตัวอย่างกรณีโทษทางอาญา

จำเลยมีข้อมูลเกี่ยวกับ ชื่อ-นามสกุล หมายเลขโทรศัพท์ บัญชีธนาคารและหมายเลขบัญชีธนาคาร อันเป็นข้อมูลส่วนบุคคลของผู้อื่นจำนวนหลายราย จำเลยกับพวกจึงเป็นผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล อันเป็นการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แล้วบังอาจนำข้อมูลส่วนบุคคลนั้นไปขายให้แก่สายลับ[32]

นอกเหนือจากสองกรณีที่กล่าวมาข้างต้น หากผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจาก (1) การสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใด ซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือ (2) ในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือ กระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษ ตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย[33] ซึ่งเป็นบทกำหนดโทษผู้แทนนิติบุคคล แม้โดยหลักแล้วผู้แทนนิติบุคคลนั้นจะไม่ได้เจตนากระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่ก็ต้องรับโทษอาญาไปด้วย[34]

---

[32] คดีหมายเลขแดงที่ อ 1087/2566

[33] มาตรา 81 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

[34] สาเหตุที่มีการบัญญัติเช่นนี้อันเนื่องมาจาก ศาลรัฐธรรมนูญได้มีคำวินิจฉัยเกี่ยวกับความรับผิดของผู้แทนนิติบุคคลว่า พระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ. 2545 มาตรา 54 เฉพาะในส่วนที่สันนิษฐานให้กรรมการผู้จัดการ ผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ต้องรับโทษทางอาญาร่วมกับการกระทำความผิดของนิติบุคคล โดยไม่ปรากฏว่ามีการกระทำหรือเจตนาประการใดอันเกี่ยวกับการกระทำความผิดของนิติบุคคลนั้น ขัดหรือแย้งต่อรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 39 วรรคสอง เป็นอันใช้บังคับไม่ได้ และต่อมาศาลรัฐธรรมนูญได้มีคำวินิจฉัยในลักษณะดังกล่าวทำนองเดียวกัน คือ พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 มาตรา 74 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 78 พระราชบัญญัติสถานบริการ พ.ศ. 2509 มาตรา 28/4 และพระราชบัญญัติปุ๋ย พ.ศ. 2518 มาตรา 72/5 ขัดหรือแย้งต่อรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 39 วรรคสอง เป็นอันใช้บังคับไม่ได้ ดังนั้น นับตั้งแต่ พ.ศ. 2560 จึงได้มีการแก้ไขบทบัญญัติที่เกี่ยวข้องกับความรับผิดทางอาญาของผู้แทนนิติบุคคลที่ปรากฏในกฎหมายกว่า 76 ฉบับ และกฎหมายฉบับอื่น ๆ ต่อมา ให้มีลักษณะที่ไม่ให้ขัดหรือแย้งต่อรัฐธรรมนูญ ตามพระราชบัญญัติแก้ไขเพิ่มเติมบทบัญญัติแห่งกฎหมายที่เกี่ยวกับความรับผิดในทางอาญาของผู้แทนนิติบุคคล พ.ศ. 2560

ตารางสรุปโทษทางอาญา				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
ม. 79 วรรคหนึ่ง	ม. 27 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลอ่อนไหวโดยปราศจากฐานทางกฎหมาย โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย	จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
ม. 79 วรรคหนึ่ง	ม. 27 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย	
ม. 79 วรรคหนึ่ง	ม. 28	ผู้ควบคุมข้อมูลส่วนบุคคล	การโอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย	
ม. 79 วรรคสอง	ม. 27 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลอ่อนไหวโดยปราศจากฐานทางกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย	จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ
ม. 79 วรรคสอง	ม. 27 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย	
ม. 79 วรรคสอง	ม. 28	ผู้ควบคุมข้อมูลส่วนบุคคล	การโอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย	
ม. 80 วรรคหนึ่ง	-	ผู้ใด	ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ และนำข้อมูลไปเปิดเผยแก่ผู้อื่น	จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
ม. 81	-	นิติบุคคล (โดย ผู้แทนนิติบุคคล)	ในกรณีที่นิติบุคคลกระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ โดยความผิดนั้นเกิดจากการที่ผู้แทนนิติบุคคล	ผู้แทนนิติบุคคลต้องรับโทษตามที่บัญญัติ

ตารางสรุปโทษทางอาญา				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
			(1) สั่งการ (2) กระทำการ หรือ (3) ละเว้นไม่สั่งการ หรือ (4) ไม่กระทำการ	ไว้สำหรับความผิดนั้นๆ

ตาราง 4 สรุปโทษทางอาญา

5.3 โทษทางปกครอง

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดโทษทางปกครองในรูปแบบโทษปรับทางปกครอง โดยมุ่งลงโทษแก่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งบุคคลที่เกี่ยวข้อง ซึ่งมีหน้าที่ต้องปฏิบัติตามข้อกำหนดของพระราชบัญญัตินี้ หากบุคคลดังกล่าวได้กระทำการละเลยเ หรือฝ่าฝืนข้อกำหนดที่พระราชบัญญัตินี้กำหนดไว้ โดยการละเลยหรือฝ่าฝืนข้อกำหนดหมายถึงการไม่ปฏิบัติตามหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมาย ไม่ดำเนินการให้สอดคล้องกับมาตรการที่กำหนด หรือไม่ปฏิบัติตามข้อกำหนดในเชิงปฏิบัติการที่เกี่ยวข้องกับการประมวลผลข้อมูลบุคคล การกำหนดโทษทางปกครองนี้ มีวัตถุประสงค์เพื่อให้ผู้ที่มีหน้าที่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายอย่างเคร่งครัด เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลและป้องกันการละเมิดหรือการใช้ข้อมูลส่วนบุคคลในทางที่ผิด โดยมีการกำหนดโทษทางปกครองไว้ในมาตรา ดังต่อไปนี้

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
ม. 82	ม. 19 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่ขอความยินยอมตามรูปแบบที่กฎหมายกำหนด	
ม. 82	ม. 19 วรรคหก	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่แจ้งผลกระทบของการถอนความยินยอม	
ม. 82	ม. 23	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่มีการแจ้งรายละเอียดการประมวลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ (รวมถึงกรณีตามมาตรา 25 วรรคสอง)	

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
ม. 82	ม. 30 วรรคสี่	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิขอเข้าถึงหรือรับสำเนา ภายในระยะเวลาที่กำหนด	ปรับไม่เกิน 1 ล้านบาท
ม. 82	ม. 39 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่มีการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ROP เพื่อให้สามารถตรวจสอบได้	
ม. 82	ม. 41 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) DPO	
ม. 82	ม. 42 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่จัดให้มีการสนับสนุนการทำงานของเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล (DPO)DPO	
ม. 82	ม. 42 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	ให้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)DPO ออกจากงานโดยเหตุที่ DPO ปฏิบัติหน้าที่ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ	
ม. 82	ม. 42 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	เจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล (DPO)DPO ไม่สามารถรายงานไปยังผู้บริหารสูงสุดได้โดยตรง	
ม. 83	ม. 19 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	การขอความยินยอมโดยการหลอกหลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์	
ม. 83	ม. 21	ผู้ควบคุมข้อมูลส่วนบุคคล	การประมวลผลข้อมูลไม่สอดคล้องกับวัตถุประสงค์ หรือการไม่แจ้งวัตถุประสงค์ใหม่ (รวมถึงกรณีตามมาตรา 25 วรรคสอง)	
ม. 83	ม. 22	ผู้ควบคุมข้อมูลส่วนบุคคล	การเก็บรวบรวมข้อมูลเกินความจำเป็นสำหรับวัตถุประสงค์	

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
ม. 83	ม. 24	ผู้ควบคุมข้อมูลส่วนบุคคล	การเก็บรวบรวมข้อมูลโดยไม่มีฐานทางกฎหมาย	ปรับไม่เกิน 3 ล้านบาท
ม. 83	ม. 25 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคล โดยไม่มีฐานทางกฎหมาย	
ม. 83	ม. 27 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลโดยไม่มีฐานทางกฎหมาย	
ม. 83	ม. 27 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคล อีกฝ่ายในการขอรับข้อมูล	
ม. 83	ม. 28	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ	
ม. 83	ม. 29 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยไม่ได้จัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด	
ม. 83	ม. 29 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลไปต่างประเทศโดยไม่ได้จัดให้มีมาตรการที่เหมาะสม	
ม. 83	ม. 32 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	การประมวลผลข้อมูลส่วนบุคคลต่อไป แม้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้าน	
ม. 83	ม. 37	ผู้ควบคุมข้อมูลส่วนบุคคล	การไม่ปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล 1) ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม 2) ไม่ได้จัดให้มีการป้องกันไม่ให้ผู้อื่นใช้/เปิดเผยข้อมูลโดยปราศจากอำนาจหรือมิชอบ	ปรับไม่เกิน 3 ล้านบาท

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
			3) ไม่มีกระบวนการลบหรือทำลายข้อมูลเมื่อพ้นกำหนด 4) ไม่จัดให้มีการแจ้งเหตุละเมิดแก่ สคส. ภายใน 72 ชม. หรือในกรณีที่มีความเสี่ยงสูงไม่แจ้งแก่เจ้าของข้อมูลส่วนบุคคล 5) ไม่ได้จัดให้มีการแต่งตั้งตัวแทนเมื่อเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร	
ม. 84	ม. 26 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การประมวลผลข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ขอความยินยอม และไม่เป็นไปตามข้อยกเว้น	ปรับไม่เกิน 5 ล้านบาท
ม. 84	ม. 26 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	ไม่ปฏิบัติให้เป็นไปตามที่กฎหมายกำหนดในการเก็บรวบรวมข้อมูลประวัติอาชญากรรม	
ม. 84	ม. 27 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวโดยไม่มีฐานทางกฎหมาย	
ม. 84	ม. 27 วรรคสอง	ผู้ควบคุมข้อมูลส่วนบุคคล	การใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคล อีกฝ่ายในการขอรับข้อมูล	
ม. 84	ม. 28	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปยังประเทศที่ไม่มีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ	
ม. 84	ม. 29 วรรคหนึ่ง	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปต่างประเทศโดยไม่ได้จัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด	ปรับไม่เกิน 5 ล้านบาท

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
ม. 84	ม. 29 วรรคสาม	ผู้ควบคุมข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปต่างประเทศโดยไม่ได้จัดให้มีมาตรการที่เหมาะสม	
ม. 85	ม. 41 วรรคหนึ่ง	ผู้ประมวลผลข้อมูลส่วนบุคคล	ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) DPO	ปรับไม่เกิน 1 ล้านบาท
ม. 85	ม. 42 วรรคสอง	ผู้ประมวลผลข้อมูลส่วนบุคคล	ไม่จัดให้มีการสนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) DPO	
ม. 85	ม. 42 วรรคสาม	ผู้ประมวลผลข้อมูลส่วนบุคคล	ให้ DPเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)O ออกจากงานโดยเหตุที่ DPO ปฏิบัติหน้าที่ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ	
ม. 85	ม. 42 วรรคสาม	ผู้ประมวลผลข้อมูลส่วนบุคคล	DPOเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ไม่สามารถรายงานไปยังผู้บริหารสูงสุดได้โดยตรง	
ม. 86	ม. 29 วรรคหนึ่ง	ผู้ประมวลผลข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยไม่ได้จัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด	ปรับไม่เกิน 3 ล้านบาท
ม. 86	ม. 29 วรรคสาม	ผู้ประมวลผลข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยไม่ได้จัดให้มีมาตรการที่เหมาะสม	
ม. 86	ม. 37 (5)	ผู้ประมวลผลข้อมูลส่วนบุคคล	ไม่ได้จัดให้มีการแต่งตั้งตัวแทนเมื่อเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร	
ม. 86	ม. 40 วรรคหนึ่ง	ผู้ประมวลผลข้อมูลส่วนบุคคล	การไม่ปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล โดยไม่มีเหตุอันควร	

ตารางสรุปโทษทางปกครอง				
บทกำหนดโทษ	**บทกำหนดหน้าที่**	**ผู้กระทำความผิด**	**ฐานความผิด**	**ระวางโทษ**
			1) ดำเนินการนอกคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล 2) ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม 3) ไม่มีการจัดทำ ROP เพื่อให้สามารถตรวจสอบได้	
ม. 87	ม. 29 วรรคหนึ่ง	ผู้ประมวลผลข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปต่างประเทศโดยไม่ได้จัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด	ปรับไม่เกิน 5 ล้านบาท
ม. 87	ม. 29 วรรคสาม	ผู้ประมวลผลข้อมูลส่วนบุคคล	การส่งหรือโอนข้อมูลส่วนบุคคลอ่อนไหวไปต่างประเทศโดยไม่ได้จัดให้มีมาตรการที่เหมาะสม	
ม. 88	ม. 39 วรรคหนึ่ง	ตัวแทน	ไม่มีการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล ROP เพื่อให้สามารถตรวจสอบได้	ปรับไม่เกิน 1 ล้านบาท
ม. 88	ม. 41 วรรคหนึ่ง	ตัวแทน	ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) DPO	
ม. 89	ม. 75	ผู้ใด	ไม่ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน	ปรับไม่เกิน 5 แสนบาท
ม. 89	ม. 76 (1)	ผู้ใด	ไม่มาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการกระทำความผิดตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ	
ม. 89	ม. 76 วรรค 4	ผู้ใด	ไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามสมควร	

ตาราง 5 สรุปโทษทางปกครอง