พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

(ประกาศลงในราชกิจจานุเบกษา วันที่ 27 พฤษภาคม 2562)

- หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ยกเว้น หมวด 2 (การคุ้มครองข้อมูลส่วนบุคคล) หมวด 3 (สิทธิของเจ้าของข้อมูลส่วนบุคคล) หมวด 5 (การร้องเรียน) หมวด 6 (ความรับผิดทางแพ่ง) หมวด 7 (บทกำหนดโทษ) และความในมาตรา 95 (การดำเนินการกับข้อมูลเดิม) และมาตรา 96 (การตรากฎหมายลำดับรอง) ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปี นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

คำนิยาม

ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ฯลฯ

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา รสนิยมทางเพศ ข้อมูลทางชีวภาพ ทั้งนี้กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

บทบาทของผู้เกี่ยวข้อง และการบังคับใช้

ผู้ควบคุมข้อมูลส่วนบุคคล - บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
(ม 6 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

ผู้ประมวลผลข้อมูลส่วนบุคคล - บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
(ม 6 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

ผู้ควบคุมข้อมูล (Controllers)

ผู้ประมวลผล (Processors)

เจ้าของข้อมูล – บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุถึง

(บุคคลหมายถึงคนธรรมดาที่มีชีวิตอยู่ ไม่รวมถึงนิติบุคคล)

เจ้าของข้อมูล (Data Subjects)

บุคคลภายนอก (Third Parties)

*ความยินยอม
*ต้องเก็บบจากเจ้าของข้อมูล
*ห้ามเก็บ Sensitive Data
*ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเจ้าของข้อมูล เช่น วัตถุประสงค์ , อำนาจตามกฎหมายหรือสัญญา , ข้อมูลฯ ที่จะเก็บ , ระยะเวลาที่เก็บ , อาจจะเปิดเผยข้อมูลให้ใคร , สถานที่ วิธีการติดต่อ สิทธิของเจ้าของข้อมูล
(ม 22,23 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

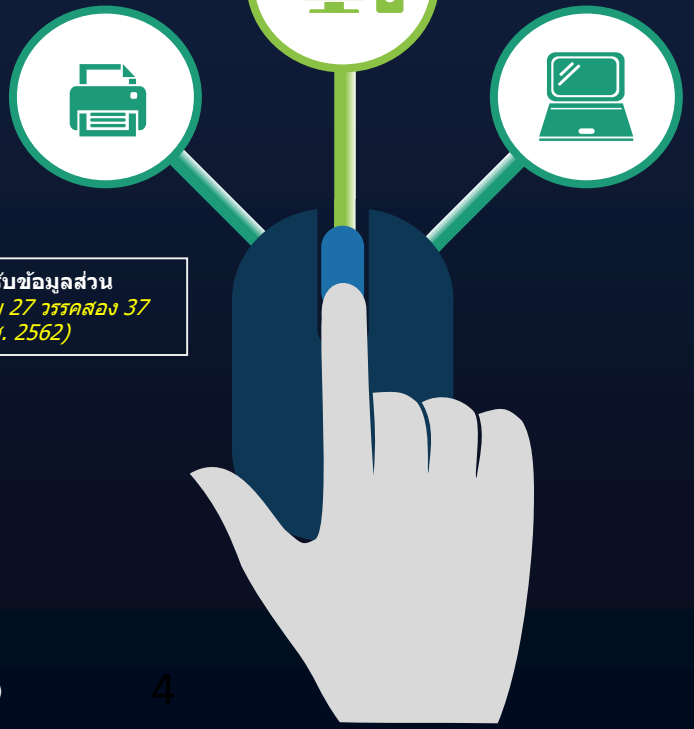
*เช่น บุคคล นิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผย *(ม 27 วรรคสอง 37 (2) พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)*

*ความยินยอม
*การโอนข้อมูลไปต่างประเทศ ปลายทางต้องมีมาตรฐานที่เพียงพอ
(ม 28,29 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

การใช้

การเก็บรวบรวม

การเปิดเผย



การบังคับใช้กฎหมาย

การเก็บรวบรวบข้อมูลส่วนบุคคล

มาตรา 24

1. ได้รับความยินยอมจากเจ้าของข้อมูล (Consent)
2. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
3. เพื่อป้องกันหรือระงับอัตราต่อชีวิต (Vital Interest)
4. มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
5. มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public Task)
6. มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมินสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
7. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

การบังคับใช้กฎหมาย

การเก็บรวบรวบข้อมูลส่วนบุคคลที่เป็น Sensitive Data

มาตรา 26

1. ได้รับความยินยอมโดยชัดแจ้ง (Consent)
2. ป้องกันหรือระงับอันตรายต่อชีวิต (Vital interest)
3. การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน
4. ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
5. การก่อตั้งสิทธิเรียบร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
6. จำเป็นในการปฏิบัติตามกฎหมายที่เกี่ยวข้องตามที่กำหนด

การบังคับใช้กฎหมาย

การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล สำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศที่รับข้อมูลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่**เพียงพอ**

เว้นแต่

1. การปฏิบัติตามกฎหมาย
2. ได้รับความยินยอมจากเจ้าของข้อมูล
3. การปฏิบัติตามสัญญา
4. การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
6. เพื่อประโยชน์สาธารณะที่สำคัญ

การบังคับใช้กฎหมาย

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
3. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
4. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
5. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure)

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
2. ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
4. แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
5. แต่งตั้งตัวแทนภายในราชอาณาจักร
6. จัดทำบันทึกรายการ

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และ ผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล

1. ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
3. จัดทำและเก็บรักษารายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
4. แต่งตั้งตัวแทนภายในราชอาณาจักร
5. ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล ให้ถือว่า ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

1. ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูล
2. ส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย
3. การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

การดำเนินการของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาฯ

ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563 ประกาศในราชกิจจานุเบกษาแล้วเมื่อวันวันที่ 20 กุมภาพันธ์ 2563 ใช้บังคับตั้งแต่วันที่ 21 กุมภาพันธ์ 2563 มีสาระสำคัญ ดังนี้

- **ประธานกรรมการ** : รับสมัครจากบุคคลไม่น้อยกว่า **3** รายชื่อ
- **กรรมการผู้ทรงคุณวุฒิ** : รับสมัครจากบุคคลไม่น้อยกว่า **18** รายชื่อ
- ดำเนินการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิให้แล้วเสร็จภายใน **60** วันนับแต่วันที่ระเบียบฯ ใช้บังคับ (**21 เมษายน 2563**) ด้วยวิธีการรับสมัคร โดยกำหนดให้เปิดรับสมัครเป็นระยะเวลา **21** วัน
- คณะกรรมการสรรหาคัดเลือกบุคคลผู้มีคุณสมบัติและไม่มีลักษณะต้องห้าม และยินยอมให้เสนอชื่อเข้ารับคัดเลือกโดยให้คำนึงถึงความโปร่งใสและความเป็นธรรมในการสรรหา แล้วแจ้งรายชื่อประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ พร้อมหลักฐานแสดงคุณสมบัติและการไม่มีลักษณะต้องห้าม รวมทั้งความยินยอมของบุคคลดังกล่าวต่อคณะรัฐมนตรีเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ

รับสมัร

เข้ารับการคัดเลือกเพื่อเป็น

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิใน
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

รวม 10 คน

คุณสมบัติ

1. มีความเชี่ยวชาญในด้านที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล
   - ด้านการคุ้มครองข้อมูลส่วนบุคคล
   - ด้านการคุ้มครองผู้บริโภค
   - ด้าน ICT
   - ด้านสังคมศาสตร์
   - ด้านกฎหมาย
   - ด้านสุขภาพ
   - ด้านการเงิน
   - ด้านอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
2. มีสัญชาติไทย
3. ไม่เป็น หรือ เคยเป็น บุคคลล้มละลาย
4. ไม่เคยต้องคำพิพากษาถึงที่สุดให้จำคุก
5. ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากงาน
6. ไม่เคยถูกถอดถอนออกจากตำแหน่ง
7. ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง

http://bit.ly/2019pdpa

ดูรายละเอียดเพิ่มเติมในประกาศฯ

การยื่นใบสมัคร

ตั้งแต่วันที่ 4 - 24 มีนาคม 2563 ในเวลาราชการ

- ยื่นใบสมัครด้วยตนเองพร้อมเอกสารและหลักฐานประกอบการรับสมัคร

ณ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
ชั้น 7 อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

- ส่งไปรษณีย์ลงทะเบียน ไปรษณีย์ไทย THAILAND POST ตอบรับถึง
  “หน่วยธุรการของคณะกรรมการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ตามที่อยู่ข้างต้น

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

pdpc@mdes.go.th | 021421033 | ติดต่อสอบถามเพิ่มเติม

การเตรียมความพร้อมระดับองค์กร

1. การตั้งคณะทำงาน (Working Group) ภายในองค์กร

การตั้งคณะทำงานภายในองค์กรควรประกอบไปด้วยกลุ่มคนต่อไปนี้

- ฝ่ายกำหนดนโยบายและยุทธศาสตร์ขององค์กร
- ฝ่ายกฎหมาย
- ฝ่ายเทคโนโลยีสารสนเทศ
- ฝ่ายบุคคล หรือฝ่ายที่เกี่ยวข้องกับขบวนการทางธุรกิจขององค์กร

เพื่อศึกษาและทำความเข้าใจบริบทของกฎหมาย และเตรียมความพร้อมในการตรวจสอบ และปรับปรุงการดำเนินขององคกร์ให้สอดคล้องตามข้อกำหนดของกฎหมาย

2. การจับคู่ข้อมูล (Data Map)

ตรวจสอบกระบวนการที่เกี่ยวข้องกับการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กร

หน่วยงานต้องตรวจสอบข้อมูลส่วนบุคคลที่มีอยู่ในองค์กร ตามกระบวนการไหลของข้อมูล (Data flows) เพื่อให้ทราบว่าข้อมูลส่วนบุคคลที่องค์กรนำมาใช้ในการประมวลผลมีที่มาจากแหล่งใด ข้อมูลที่จัดเป็นข้อมูลในลักษณะใด (แบบทั่วไป หรือ ข้อมูลอ่อนไหว) ถูกจัดเก็บไว้ที่ใด จัดเก็บด้วยเหตุผลใด และถูกควบคุมโดยใคร โดยใช้วิธีการทำ Data Map เป็นต้น

3. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPOs) ในองค์กร

กรณีที่หน่วยงานเข้าข่ายตามข้อกำหนดของกฎหมาย จะต้องดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office)

เพื่อทำหน้าที่

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลฯ ผู้ประมวลผลข้อมูลฯ ลูกจ้าง ผู้รับจ้างของผู้ควบคุมข้อมูลฯ หรือที่เกี่ยวข้องกับพ.ร.บ. นี้

ตรวจสอบการการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูล่วนบุคคล

ประสานงานและให้ความร่วมมือกับสำนักงานฯ กรณีเกิดปัญหา

รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่ตามกฎหมายนี้

4. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

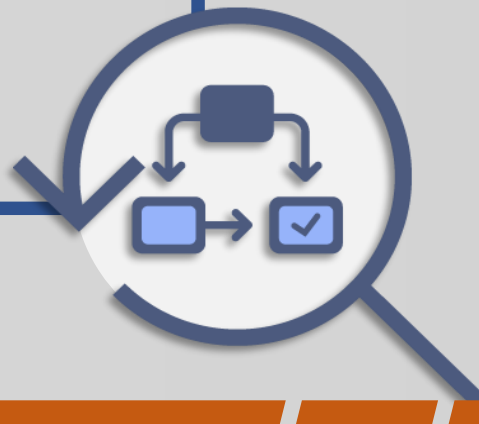
- เพื่ออธิบายขอบเขตและวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล (จัดเก็บ ใช้ เปิดเผย)
- เพื่อประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล
- เพื่อจัดความเสี่ยงที่จะมีผลกระทบต่อเสรีภาพของบุคคล และ
- เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานที่มีความเหมาะสม

5. ระบุและบันทึกแหล่งที่มาของข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ

หน่วยงานต้องให้ความสำคัญกับแหล่งที่มาของข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ รวมทั้งต้องบันทึกกิจกรรมที่เกิดขึ้นตลอดวงจรชีวิตของข้อมูล (รวบรวมจัดเก็บ ใช้ เปิดเผย และการทำลาย) เพื่อการบริการจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับข้อกำหนดของกฎหมาย

6. กำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล

หน่วยงานต้องจำแนกหรือแยกแยะข้อมูลให้เป็นหมวดหมู่ข้อมูลส่วนบุคคล เพื่อระบุและจัดการข้อมูลบนพื้นฐานความเสี่ยง รวมถึงกำหนดฐานการประมวลผลข้อมูลผลข้อมูลส่วนบุคคลที่เหมาะสม



7. ระบุ/กำหนดฐานการประมวลผลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน่วยงานจะต้องประมวลผลข้อมูลส่วนบุคคลบนฐานการประมวลผลที่ชอบกฎหมาย (Lawfulness of processing) ทั้งในส่วนของข้อมูลส่วนบุคคลแบบทั่วไป (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 24 และมาตรา 26 โดยลำดับ

8. กำหนดหลักเกณฑ์และวิธีการขอความยินยอมสอดคล้องกับสิทธิของเจ้าของข้อมูล

1. การพัฒนากระบวนงาน และระบบงานที่เกี่ยวข้องเพื่อรองรับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย เช่น การขอความยินยอมที่ชัดแจ้ง ข้อความเข้าใจง่าย
2. การใช้สิทธิขอถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล
3. การขอเข้าถึง และปรับปรุงข้อมูลให้เป็นปัจจุบัน เป็นต้น

9. จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน

หน่วยงานควรพิจารณาจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่มีเนื้อหาครอบคลุมตามหลักการอย่างน้อย ดังนี้

1. หลักการการรวบรวม จัดเก็บ ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Collection Limitation)
2. หลักการใช้ และเปิดเผยข้อมูลอย่างจำกัด (Use Limitation)
3. หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards)
4. หลักการการกำหนดวัตถุประสงค์ที่ชัดเจน (Purpose Specification)
5. หลักการคุณภาพของข้อมูลส่วนบุคคล (Data Quality)
6. หลักการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล (Individual Participation)
7. หลักการเปิดเผยข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย (Openness)
8. หลักความรับผิดชอบของบุคคลที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคล/ประมวลผลข้อมูลส่วนบุคคล (Accountability)

10. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงานต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ถูกจัดเก็บ ใช้ และเปิดเผย โดยต้องกำหนดให้มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่สอดคล้องกับมาตรฐานสากล เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย

11. กำกับดูแลและตรวจสอบและประเมินความเสี่ยง

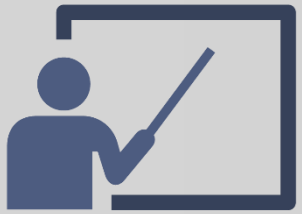
หน่วยงานจะต้องมีการกำกับดูแล และตรวจสอบการดำเนินงานบุคคลากร และผู้เกี่ยวเกี่ยวเพื่อให้เกิดการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่หน่วยงานทำการรวบรวม จัดเก็บ และเผยแพร่ถูกควบคุมภายใต้มาตรการที่กำหนดไว้ รวมถึงต้องมีการตรวจสอบและประเมินความเสี่ยงเป็นประจำอย่างสม่ำเสมอ

12. ทบทวนหรือปรับปรุงกระบวนงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล

หน่วยงานต้องทบทวนหรือปรับปรุงกระบวนงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เมื่อพบว่ามีความเสี่ยง หรือพบว่ามีกระบวนงานที่ไม่สอดคล้องกับข้อกำหนดของกฎหมาย โดยทบทวนตามวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้ เปิดเผย ลบหรือทำลายข้อมูล

13. สร้างความตระหนักรู้ และฝึกอบรม

หน่วยงานต้องสร้างความตระหนักรู้ สำนึกรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล และหน้าที่ความรับผิดชอบของหน่วยงาน รวมถึงการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และผลกระทบที่เกิดขึ้นจากการละเมิดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ให้แก่บุคลากรของหน่วยงาน โดยการเผยแพร่ข้อมูลข่าวสาร และการฝึกอบรมให้ความรู้ที่เกี่ยวข้องเป็นประจำสม่ำเสมอ



14. กำหนดมาตรการที่เหมาะสมด้านการรั่วไหลของข้อมูล (Data Breaches)

หน่วยงานต้องกำหนดมาตรการที่เหมาะสมเพื่อป้องกันการละเมิด และตรวจสอบ รวมถึงการรายงานผลการละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้น และต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

15. การออกแบบและพัฒนาระบบโดยคำนึงถึงความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล (Security and Privacy by Design)

หน่วยงานต้องให้ความสำคัญในการพัฒนาระบบงานที่คำนึงถึงการสร้างความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบระบบงาน กล่าวคือหน่วยงานต้องใช้มาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอ ตั้งแต่ขั้นตอนการออกแบบไปจนถึงขั้นตอนพัฒนาระบบงาน ตลอดจนบริการ ผลิตภัณฑ์ หรือการดำเนินการ ในลักษณะที่คุ้มครองสิทธิ์ส่วนบุคคลและข้อมูลส่วนบุคคล ตัวอย่าง Data protection by design เช่น การใช้นามแฝง และ การเข้ารหัส (Encoding)

การเตรียมความพร้อมระดับองค์กร

16. กำหนดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลทางด้านกายภาพ (Physical Security)

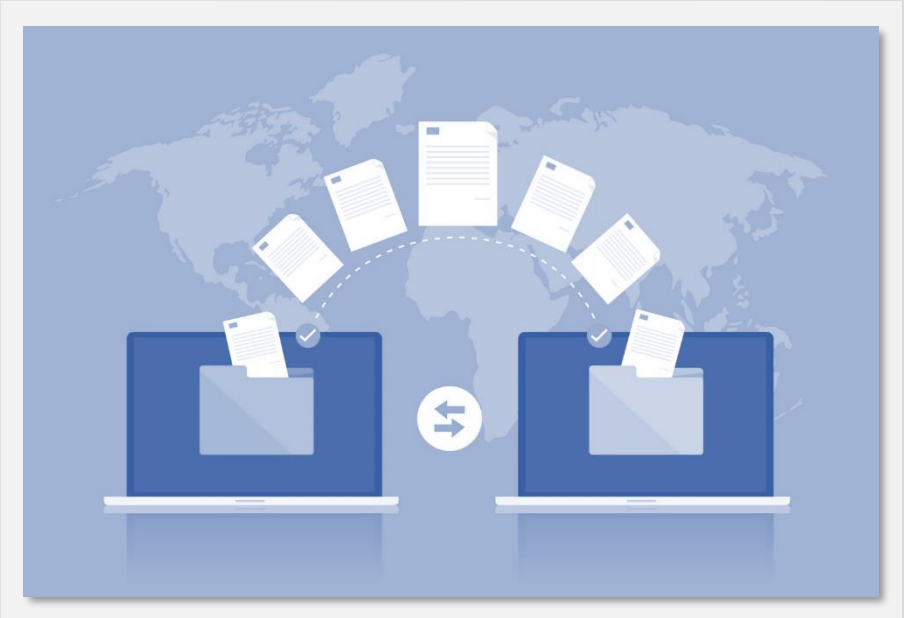
หน่วยงานต้องกำหนดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพของอุปกรณ์ประมวลผลและอุปกรณ์ที่เกี่ยวข้องที่ถูกนำมาใช้ในองค์ทั้งจากบุคคลภายนอกและภายในองค์กร เช่น กำหนดนโยบายของศูนย์ข้อมูล เครือข่ายและระบบสื่อสาร รวมถึงการจัดสารสื่อบันทึกข้อมูล เป็นต้น

17. กำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน

หน่วยงานต้องกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคลไว้อย่างชัดเจน และสิทธิการเข้าถึงได้เฉพาะผู้ที่มีสิทธิและมีหน้าที่รับผิดชอบเกี่ยวกับการดำเนินการขององค์กร

18. กำหนดมาตรการหรือแนวปฏิบัติที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เพียงพอ (Cross-Border Data Transfer)

หากหน่วยงานมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางหรือองค์การระหว่างประเทศ จะต้องคำนึงถึงว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ เว้นแต่ดำเนินการเป็นตามข้อยกเว้นตามที่กฎหมายกำหนดในมาตรา 28



Thank you