การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
MASS RAPID TRANSIT AUTHORITY OF THAILAND
รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม
A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2566

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 มาตรา 37 ประกอบกับข้อ 4 และข้อ 5 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ตระหนักและให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของ รฟม. จึงเห็นสมควรปรับปรุงประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ลงวันที่ 31 พฤษภาคม 2565 โดยอาศัยอำนาจตามความในมาตรา 24 วรรคหนึ่ง แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศไว้ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ให้ยกเลิกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ลงวันที่ 31 พฤษภาคม 2565

ข้อ 4 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล

รฟม. จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยอยู่บนพื้นฐานหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

/(1) เก็บรวบรวม ...

(1) เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมาย เป็นธรรม และมีความโปร่งใส ต่อเจ้าของข้อมูลส่วนบุคคล (Lawfulness, Fairness and Transparency)

(2) เก็บรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการที่ชอบด้วยกฎหมาย และจัดเก็บข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ในการดำเนินงาน และตามที่กฎหมายกำหนดเท่านั้น (Purpose Limitation) โดยจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เป็นกรณีที่กฎหมายกำหนดให้สามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

(3) เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย (Data Minimization)

(4) ข้อมูลส่วนบุคคลมีความถูกต้องและเป็นปัจจุบัน พร้อมใช้งาน รวมถึงต้องมีการดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะได้รับการปรับปรุงแก้ไข (Accuracy)

(5) ประมวลผลข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็นต่อการประมวลผลข้อมูลส่วนบุคคล (Storage Limitation) เว้นแต่กรณีมีกฎหมายกำหนดไว้ต้องจัดเก็บข้อมูลส่วนบุคคลไว้นานกว่าระยะเวลาเท่าที่จำเป็นดังกล่าว

(6) การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงมีการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย และป้องกันการสูญหายโดยอุบัติเหตุ การถูกทำลาย หรือถูกทำให้เสียหาย (Integrity and Confidentiality)

ข้อ 5 ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มีขอบเขตการบังคับใช้ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของ รฟม.

สำหรับข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับ รฟม. จะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปตามวัตถุประสงค์เดิม

ข้อ 6 หลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล

รฟม. จะประมวลผลข้อมูลส่วนบุคคลโดยปฏิบัติตามหลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล ดังนี้

(1) ต้องแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล

(2) ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนการประมวลผลข้อมูลส่วนบุคคล เว้นแต่กรณีดังต่อไปนี้ สามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

(ก) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวข้องกับการศึกษาวิจัย หรือสถิติ

/(ข) เพื่อป้องกัน ...

(ข) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(ค) เพื่อปฏิบัติตามกฎหมาย

(ง) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

(จ) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(ฉ) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(3) ไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว รวมถึงการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือผู้มีอำนาจกระทำแทนเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้ง หรือได้รับยกเว้นตามที่กฎหมายกำหนด

(4) ไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ให้กับบุคคลอื่น เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลโดยทำหนังสือให้ความยินยอมเปิดเผยข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือกรณีตามมาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามมาตรา 24 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ข้อ 7 ช่องทางการติดต่อ

หากเจ้าของข้อมูลส่วนบุคคลมีข้อสงสัย ข้อเสนอแนะ หรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ รฟม. หรือเกี่ยวกับนโยบายนี้ หรือต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลสามารถติดต่อสอบถามได้ที่

(1) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.)
175 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์ 0 2716 4044
ช่องทางการติดต่อ saraban@mrta.co.th

(2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)
คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
175 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์ 0 2716 4044
ช่องทางการติดต่อ saraban@mrta.co.th

/ข้อ 8 แนวปฏิบัติ ...

ข้อ 8 แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม.

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม. มีรายละเอียดตามเอกสารแนบท้ายประกาศ ประกอบด้วย

หมวด 1 แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

หมวด 2 แนวปฏิบัติสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ประกาศ ณ วันที่ 25 ธันวาคม พ.ศ. 2566

(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

สารบัญ

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2566

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ผู้ว่าการ หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
3. คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หมายถึง กลุ่มของบุคคลซึ่งได้รับมอบหมายจากผู้ว่าการให้ปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะเป็นทางตรงหรือทางอ้อม ซึ่งไม่รวมข้อมูลผู้ถึงแก่กรรมหรือข้อมูลของนิติบุคคล
5. ข้อมูลนิรนาม หมายถึง ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวตนของบุคคลได้
6. การปกปิดข้อมูล (Data Marking) หมายถึง การปกปิดข้อมูลจริงเพื่อให้ข้อมูลนั้นแสดงเป็นข้อมูลหลอกหรือนามแฝง
7. เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลที่ข้อมูลส่วนบุคคลสามารถระบุถึงตัวบุคคลนั้น ไม่รวมผู้ถึงแก่กรรมและนิติบุคคล
8. การประมวลผลข้อมูลส่วนบุคคล หมายถึง การเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
9. ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง ผู้ปฏิบัติงานให้ รฟม. ซึ่งมีอำนาจหน้าที่ในการออกนโยบาย มาตรการ แนวทางปฏิบัติให้เป็นไปตามที่กฎหมายกำหนด รวมถึงตัดสินใจเกี่ยวกับการจัดเก็บ ใช้ เปิดเผย และกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
10. ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” โดยที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
    - ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายใน) หมายถึง บุคลากร รฟม.
    - ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายนอก) หมายถึง บุคคลหรือนิติบุคคล รวมถึงผู้รับจ้างของ รฟม. ซึ่งต้องปฏิบัติตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ที่ รฟม. กำหนด
11. ผู้พบเห็นเหตุการณ์ หมายถึง ผู้พบเห็นเหตุการละเมิดข้อมูลส่วนบุคคล

12. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) หมายถึง สัญญาหรือข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เพื่อให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามวัตถุประสงค์ และขอบเขตที่ รฟม. กำหนดเท่านั้น โดยสามารถจัดทำเป็นหนังสือปกติหรือหนังสืออิเล็กทรอนิกส์ก็ได้
13. ความมั่นคงปลอดภัย หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
14. การละเมิดข้อมูลส่วนบุคคล หมายถึง การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้
    (1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
    (2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
    (3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ
15. ฝทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
16. ผู้ดูแลระบบ หมายถึง บุคลากร รฟม. ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ และพนักงานของผู้รับจ้างที่รับผิดชอบติดตั้งหรือบำรุงรักษาระบบสารสนเทศให้ รฟม.

หมวด 1
แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 1
การประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อกำหนดแนวทางในการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 21 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

มาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 37 วรรคหนึ่ง

มาตรา 39 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม

(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง โดยอนุโลม

ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 7.2 และ 7.4

ผู้รับผิดชอบ

- ผู้ควบคุมข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล และทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
2. นโยบายการบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคล
   2.1 คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ ฝทท. จัดให้มีการทำและทบทวนหรือปรับปรุงนโยบายการคุ้มครองข้อมูลส่วนบุคคล และแนวปฏิบัติที่สนับสนุนการทำงานต่าง ๆ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
   2.2 ผู้บริหาร รฟม. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคลในแต่ละปีงบประมาณ
   2.3 ผู้บริหาร รฟม. จัดให้มีบุคลากรดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
   2.4 ผู้บริหาร รฟม. แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอ เพื่อให้พนักงานเจ้าหน้าที่ทุกคนได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
3. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดวิธีการประเมินความเสี่ยงกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล
4. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายและอยู่ภายใต้การดำเนินงานของ รฟม. เท่านั้น
5. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA) เพื่อควบคุมการประมวลผลข้อมูลส่วนบุคคล และให้เจ้าของข้อมูลส่วนบุคคลตรวจสอบได้ โดยอย่างน้อยต้องประกอบไปด้วยรายละเอียดตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรายละเอียดดังต่อไปนี้
   (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
   (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
   (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
   (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
   (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
   (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
   (7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
   (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)
   (9) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย
   (10) วิธีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
   (11) วิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (หากมี)

6. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องทบทวน/ปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ให้ถูกต้องทันสมัย พร้อมใช้งานตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลของ รฟม. อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
7. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดตามวิธีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล โดยอย่างน้อยต้องประกอบไปด้วยรายละเอียดตามมาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรายละเอียดดังต่อไปนี้
   (1) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
   (2) การแจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
   (3) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
   (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเป็นเวลา 10 ปี
   (5) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
   (6) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ประกอบด้วย สถานที่ติดต่อ และวิธีการติดต่อ
   (7) ข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย สถานที่ติดต่อ และวิธีการติดต่อ
   (8) สิทธิของเจ้าของข้อมูลส่วนบุคคล
   (9) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย
8. ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
9. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดแนวปฏิบัติประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) และแนวปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)
10. ผู้ควบคุมข้อมูลส่วนบุคคลต้องประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) และกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่เหมาะสม
11. ผู้ควบคุมข้อมูลส่วนบุคคลต้องรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
12. ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) เมื่อมีการส่งมอบข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายนอก) ประมวลผล
13. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องตรวจสอบการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงของลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคล และลูกจ้างหรือผู้รับจ้างของผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 2
มาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

  มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

  (1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 6

ผู้รับผิดชอบ

- ผู้บริหาร รฟม.
- คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล
- ฝทท.
- ผู้ดูแลระบบ

แนวปฏิบัติ

1. ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล ครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ในรูปแบบเอกสาร หรือรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. การสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคล
   2.1 ผู้บริหาร รฟม. ทุกระดับชั้น มีหน้าที่สนับสนุนและส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานเจ้าหน้าที่ ต่อไปนี้
      (1) ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
      (2) จูงใจให้พนักงานเจ้าหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล
      (3) สร้างความตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
   2.2 การสร้างความตระหนักแก่พนักงานเจ้าหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
      (1) ฝทท. ต้องดำเนินการฝึกอบรมหรือประชาสัมพันธ์ เพื่อสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ใช้งานเป็นประจำทุกปี
      (2) ฝทท. ต้องแจ้งพนักงานเจ้าหน้าที่ให้รับทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
3. การบริหารจัดการข้อมูลส่วนบุคคล
   3.1 ฝทท. และผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดรายการข้อมูลส่วนบุคคล และระบุผู้รับผิดชอบดูแลข้อมูลส่วนบุคคล พร้อมทั้งกำหนดลำดับชั้นความลับ เพื่อรับผิดชอบดูแลข้อมูลส่วนบุคคลตลอดวงจรชีวิตข้อมูล
   3.2 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ต้องใช้ข้อมูลส่วนบุคคลอย่างระมัดระวังและใช้เพื่อปฏิบัติงานของ รฟม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รฟม.
   3.3 เจ้าของข้อมูลส่วนบุคคลและผู้ดูแลระบบ ต้องจัดประเภทข้อมูลส่วนบุคคลตามที่ รฟม. กำหนด และทบทวนอย่างสม่ำเสมอ
   3.4 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ดูแลระบบ ต้องจัดทำป้ายกำกับข้อมูลส่วนบุคคล (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่สอดคล้องกับประเภทข้อมูลส่วนบุคคลตามระดับชั้นความลับที่ รฟม. กำหนด
4. การควบคุมการเข้าถึงข้อมูลส่วนบุคคล
   4.1 ฝทท. และผู้ควบคุมข้อมูลส่วนบุคคล ร่วมกันกำหนดสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล พร้อมทั้งทบทวนเมื่อมีการเปลี่ยนแปลง

4.2 ขั้นตอนปฏิบัติในการจัดเก็บข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ดูแลระบบ ต้องปฏิบัติ ดังนี้

4.2.1 จัดประเภทข้อมูลส่วนบุคคล ดังนี้

(1) ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น

(2) ข้อมูลส่วนบุคคลอ่อนไหว เช่น

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม
- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

4.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

(1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร

(2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร

(3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รฟม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

4.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รฟม. กำหนด

4.2.4 จัดแบ่งระดับชั้นการเข้าถึง

(1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย

(2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

(3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

4.3 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย ซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และข้อกำหนดทางด้านการคุ้มครองข้อมูลส่วนบุคคลอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

4.4 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูล และผู้ดูแลระบบ ต้องดำเนินการปกปิดข้อมูล (Data Marking) ให้สอดคล้องกับประเภทข้อมูลส่วนบุคคลตามระดับชั้นความลับที่ รฟม. กำหนด

ส่วนที่ 3
การส่งมอบข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น

วัตถุประสงค์

- เพื่อป้องกันมิให้บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ รฟม. ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

กฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

  มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

  บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

  ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39

  มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

  (2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 7.3

ผู้รับผิดชอบ

- ผู้ควบคุมข้อมูลส่วนบุคคล
- คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องไม่เปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องบันทึกการเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล
3. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดให้มีช่องทางการขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
4. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดวิธีการการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
5. คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นผู้ตัดสินใจว่าจะรับคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลหรือไม่
6. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดทำข้อตกลงในการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) เพื่อควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายนอก) ดำเนินการตามที่ รฟม. กำหนด
7. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องบันทึกข้อมูลของผู้ร้องขอก่อนส่งมอบข้อมูลส่วนบุคคล ดังนี้
   (1) ชื่อ-นามสกุล
   (2) ข้อมูลสำหรับการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล
   (3) วัน เดือน ปี ที่ให้ข้อมูล
   (4) ฐานทางกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล
   (5) วัตถุประสงค์การนำไปใช้งาน และ/หรือ เปิดเผย

ส่วนที่ 4
การควบคุมการลบหรือทำลายข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อควบคุมการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้น อยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา 33 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2) (4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้ ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคห้ามาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 7.4

ผู้รับผิดชอบ

- ผู้ควบคุมข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องทบทวนข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนอย่างสม่ำเสมอ และดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม เมื่อครบกำหนดระยะเวลาการเก็บรักษาตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล หรือตามที่ขอความยินยอมไว้
2. ผู้ควบคุมข้อมูลส่วนบุคคล สามารถยกเว้นไม่กระทำการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนามได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย เช่น
   - เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
   - เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
   - เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์
   - เพื่อการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ส่วนที่ 5
การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

  มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

  (4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

ผู้รับผิดชอบ

- ผู้ว่าการ
- ผู้ควบคุมข้อมูลส่วนบุคคล
- คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

1. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดแนวปฏิบัติกรณีเกิดข้อร้องเรียนหรือกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล
2. ผู้ควบคุมข้อมูลส่วนบุคคล ต้องกำหนดหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
3. ผู้พบเห็นเหตุการณ์ต้องแจ้งให้ ฝทท. ทราบ เมื่อพบเห็นเหตุการละเมิดข้อมูลส่วนบุคคลตามแนวปฏิบัติกรณีเกิดข้อร้องเรียนหรือกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคลที่กำหนด

4. เมื่อ ฝทท. ได้รับแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ให้ตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล หากพบว่าเป็นการละเมิดข้อมูลส่วนบุคคลจะต้องประเมินความเสี่ยงที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลตามแนวปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment) และดำเนินการ ดังนี้
   4.1 กรณีไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ ฝทท. จัดทำบันทึกเหตุการละเมิดข้อมูลส่วนบุคคล และนำเสนอให้คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรับทราบ
   4.2 กรณีมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ ฝทท. จัดทำบันทึกเหตุการละเมิดข้อมูลส่วนบุคคล และดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
   4.3 กรณีมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ ฝทท. จัดทำบันทึกเหตุการละเมิดข้อมูลส่วนบุคคล และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบด้วย
5. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
   5.1 ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดก็ตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้
   5.2 ผู้ว่าการ เป็นผู้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบลายลักษณ์อักษร
6. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
   6.1 คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องกำหนดวิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ และแนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติม
   6.2 ผู้ว่าการ เป็นผู้อนุมัติวิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล และแนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล
7. ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ต้องให้ความร่วมมือกับเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เมื่อถูกร้องขอให้ส่งเอกสารหรือข้อมูลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการชี้แจงข้อเท็จจริงเพื่อสนับสนุนการตรวจสอบและการปฏิบัติงานของเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 2
แนวปฏิบัติสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อเป็นแนวปฏิบัติให้ผู้ประมวลผลข้อมูลส่วนบุคคลนำไปปฏิบัติให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

  มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

  (1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

  (2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

  (3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

  ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

  การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

  ความใน (3) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 8

ผู้รับผิดชอบ

- ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเก็บรวบรวมข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็นตามวัตถุประสงค์การดำเนินงานของ รฟม. เท่านั้น
2. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด
3. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล โดยอย่างน้อยต้องประกอบด้วยรายละเอียดดังต่อไปนี้
   (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
   (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
   (3) ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล
   (4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
   (5) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
   (6) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
   (7) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
   (8) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
   (9) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)
   (10) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย
   (11) วิธีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
   (12) วิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (หากมี)
4. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องทบทวนบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
5. เมื่อผู้พบเห็นเหตุการณ์พบเหตุการละเมิดข้อมูลส่วนบุคคล ต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลและ ฝทท. ทราบ ตามแนวปฏิบัติที่กำหนด
6. ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายใน) ต้องประมวลผลข้อมูลส่วนบุคคลตามเงื่อนไขที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้ และผู้ประมวลผลข้อมูลส่วนบุคคล (ภายนอก) ต้องประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ที่ตกลงไว้กับผู้ควบคุมข้อมูลส่วนบุคคล