ระเบียบปฏิบัติการแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล[1] หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

บริษัทได้กำหนดข้อกำหนดการแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล เพื่อใช้เป็นแนวทางในการปฏิบัติที่เหมาะสมในการแก้ไขและลดผลกระทบต่อเจ้าของข้อมูลที่เกิดการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าเจ้าของข้อมูลจะได้รับผลกระทบจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลน้อยที่สุด

1. วัตถุประสงค์

1.1 เพื่อใช้เป็นแนวทางปฏิบัติที่เหมาะสมในการแก้ไขปัญหาจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

1.2 เพื่อลดผลกระทบจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

1.3 เพื่อใช้เป็นแนวทางในการปรับปรุง และพัฒนาระบบการคุ้มครองป้องกันข้อมูลส่วนบุคคลให้มีประสิทธิภาพ และเหมาะสม เพียงพอมากขึ้น

2. ขั้นตอนการแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

บริษัทได้กำหนดขั้นตอนการแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล ดังนี้

2.1 การยับยั้งการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

1) เมื่อฝ่ายเทคโนโลยีสารสนเทศ พบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนที่อาจทำให้ข้อมูลรั่วไหลจากการตรวจสอบ หรือทดสอบให้รีบแจ้งผู้แทนฝ่ายบริหารระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Management Representative : DPMR) เพื่อแจ้งเจ้าหน้าที่คุ้มครองข้อมูลของบริษัท (Data Protection Officer : DPO) ทราบโดยทันที

[1] มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) ให้ DPMR พิจารณา หากเป็นพนักงานภายในบริษัท ให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทางวินัยตามระเบียบที่เกี่ยวข้อง แต่หากเป็นบุคคลภายนอก หรือเกิดจุดอ่อนของระบบให้นำเสนอประธานเจ้าหน้าที่บริหารทราบ และดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

2.2 การแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

กรณีที่พบเหตุการละเมิดข้อมูลส่วนบุคคลผู้พบเหตุการละเมิดจะต้องพิจารณาถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลก่อนเป็นลำดับแรก หากพบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลให้ดำเนินการตามข้อ 2.2.3

2.2.1 กรณีที่มีการรั่วไหล หรือละเมิดข้อมูลที่เป็นเอกสาร

1) เมื่อผู้ควบคุมข้อมูลพบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล ให้แจ้ง DPMR เพื่อแจ้ง DPO ทราบโดยทันที

2) ให้ DPMR แจ้งให้ประธานเจ้าหน้าที่บริหารทราบ

3) ให้ดำเนินการแก้ไขยับยั้งการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยเร็ว เช่น หากพบการทำลายกุญแจตู้เก็บเอกสารให้ดำเนินการเปลี่ยนกุญแจภายใน 1 วัน หรือพบมีการเปิดเผยข้อมูลส่วนบุคคลให้ดำเนินการทำลายเอกสารที่เปิดเผยนั้นทันที เป็นต้น

4) ให้ดำเนินการสืบสวน และสอบสวนเพื่อหาผู้กระทำละเมิดมาลงโทษตามระเบียบของบริษัท

5) กรณีการละเมิดที่พบจะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ให้ประธานเจ้าหน้าที่บริหาร หรือมอบหมายให้ DPO แจ้งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบเหตุการละเมิดภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

2.2.2 กรณีที่มีการรั่วไหล หรือละเมิดข้อมูลที่เป็นข้อมูลอิเล็กทรอนิกส์

1) เมื่อฝ่ายเทคโนโลยีสารสนเทศ พบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ จากการตรวจสอบ หรือทดสอบระบบให้รีบแจ้ง DPMR เพื่อแจ้ง DPO ทราบโดยทันที

2) ให้ DPMR แจ้งประธานเจ้าหน้าที่บริหารทราบ

3) ให้ DPMR ร่วมกับฝ่ายเทคโนโลยีสารสนเทศดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้าจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

4) ให้ดำเนินการสืบสวน และสอบสวนเพื่อหาผู้กระทำละเมิดมาลงโทษตามระเบียบของบริษัท หรือกฎหมาย

5) กรณีการละเมิดที่พบมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ให้ประธานเจ้าหน้าที่บริหาร หรือ DPO แจ้งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบเหตุการละเมิดภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

2.2.3 กรณีที่มีการรั่วไหล หรือละเมิดข้อมูลที่มีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

1) เมื่อฝ่ายเทคโนโลยีสารสนเทศ พบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ จากการตรวจสอบ หรือทดสอบให้รีบแจ้ง DPMR เพื่อแจ้ง DPO ทราบโดยทันที

2) ให้ DPMR แจ้งประธานเจ้าหน้าที่บริหารทราบ และกำหนดแนวทางเยียวยา

3) ให้ประธานเจ้าหน้าที่บริหาร หรือมอบหมายให้ DPO แจ้งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบเหตุการละเมิดภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

4) ให้ DPO แจ้งให้เจ้าของข้อมูลทราบถึงการรั่วไหล หรือละเมิดข้อมูลพร้อมแนวทางเยียวยา แต่หากไม่สามารถแจ้งให้เจ้าของข้อมูลทราบเป็นรายบุคคลได้ ให้พิจารณาออกเป็นประกาศแจ้งการรั่วไหล หรือละเมิดข้อมูลแทนได้

5) ให้ DPMR ร่วมกับฝ่ายเทคโนโลยีสารสนเทศดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้าจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

6) ให้ดำเนินการสืบสวน และสอบสวนเพื่อหาผู้กระทำละเมิดมาลงโทษตามระเบียบของบริษัท หรือกฎหมาย

2.3 การบันทึก และรายงานการละเมิดและการแก้ไขการละเมิด

1) ให้ผู้พบการละเมิดแจ้งให้ DPMR ทราบ

2) ให้ DPMR ทำการบันทึกรายละเอียดการละเมิด ซึ่งต้องประกอบด้วย ข้อมูลที่ถูกละเมิด สถานที่พบการละเมิด ประเภทและจำนวนของเจ้าของข้อมูลที่ต้องระมัดระวังว่าจะถูกละเมิด ประเภทและจำนวนของข้อมูลส่วนบุคคลที่ต้องระมัดระวังว่าจะถูกละเมิด คำอธิบายสาเหตุการละเมิด เช่น ความผิดพลาดของบุคคล ความผิดพลาดของระบบ หรือการถูกโจมตีหรือโจรกรรมข้อมูล เป็นต้น และโอกาสที่ข้อมูลส่วนบุคคลถูกละเมิดซ้ำ คำอธิบายมาตรการที่ดำเนินการแก้ไขหรือเสนอว่าจะแก้ไข มาตรการที่จะแจ้งและเยียวยาต่อเจ้าของข้อมูล รวมถึงมาตรการที่เหมาะสมที่จะลดความเสี่ยง

3) กรณีที่ต้องมีการรายงานการละเมิดให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ ให้ใช้แบบฟอร์มตามที่สำนักงานคุ้มครองข้อมูลส่วนบุคคลกำหนด หากสำนักงานคุ้มครองข้อมูลส่วนบุคคลยังไม่ได้กำหนดแบบฟอร์มให้ใช้บันทึกเหตุการละเมิดที่บริษัทจัดทำ พร้อมชื่อ และที่ติดต่อของ DPO แจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

กรณีที่ไม่สามารถระบุข้อมูลและแจ้งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบทันภายในเวลาที่กำหนด ให้ระบุเท่าที่จะดำเนินการได้จัดส่งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลไปก่อน และเมื่อดำเนินการตรวจสอบข้อมูลแล้วเสร็จให้จัดส่งข้อมูลให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบโดยทันที

4) ให้ DPMR สรุปรายงานการละเมิดให้ DPO และผู้บริหารทราบในการประชุมทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล