

แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification)

- ❖ แนวปฏิบัตินี้ใช้บังคับเป็นการทั่วไปกับส่วนงานและบุคลากรของสำนักบริหารการทะเบียน กรมการปกครอง (“สน.บพ.”) ทุกระดับ
- ❖ แนวปฏิบัตินี้ไม่ถือเป็นส่วนหนึ่งของสัญญาจ้าง แต่เป็นการกำหนดแนวทางการทำงานที่บุคลากรของ สน.บพ. ต้องปฏิบัติตาม โดยการไม่ดำเนินการตามแนวปฏิบัตินี้จะมีผลทางวินัยบุคลากร
- ❖ แนวปฏิบัตินี้จะได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมอ ซึ่งจะได้แจ้งให้บุคลากรของ สน.บพ. ทุกคนทราบทุกครั้ง

๑. **[ขอบเขตการบังคับใช้]** แนวปฏิบัตินี้วางกรอบแนวทางการดำเนินการที่สำคัญสำหรับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล โดยสอดคล้องและเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ”)
๒. **[ขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล]** ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (มาตรา ๓๗ (๔)) เมื่อ สน.บพ. ทราบถึงการละเมิดข้อมูลส่วนบุคคลแล้ว สน.บพ. จะต้องแจ้งเหตุดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (“สำนักงาน”) ทราบภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ ในกรณีที่การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (high risk) สน.บพ. จะต้องแจ้งเหตุละเมิดนั้นให้เจ้าของข้อมูลทราบ พร้อมแนวทางการเยียวยาโดยไม่ชักช้า โดยการแจ้งดังกล่าวและชื่อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
๓. **[การละเมิดข้อมูลส่วนบุคคล]** การละเมิดข้อมูลส่วนบุคคล ได้แก่ การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด
ทั้งนี้ เหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้
 - ๑) การละเมิดความลับของข้อมูลส่วนบุคคล (confidentiality breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

- ๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (integrity breach) ซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
- ๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (availability breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ตัวอย่างของการเหตุละเมิดข้อมูลส่วนบุคคล ได้แก่

- การอนุมัติสิทธิการเข้าถึงข้อมูลส่วนบุคคลแก่บุคคลที่สามที่ไม่สมควรได้รับอนุญาต
- การส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลที่ไม่มีหน้าที่หรือไม่มีความรับผิดชอบในเรื่องนั้น ๆ
- กรณีอุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลสูญหายหรือถูกขโมย
- การแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- เหตุการณ์ใด ๆ ข้างต้นเกิดขึ้นกับบุคคลที่สามซึ่งประมวลผลข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของ สน.บพ.

๔. [กระบวนการดำเนินการเมื่อทราบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล] เมื่อทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

๔.๑. ผู้ปฏิบัติงานซึ่งเป็นผู้รับทราบข้อเท็จจริงเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจะต้องรายงานเหตุดังกล่าวต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สน.บพ. **ทันที** เพื่อร่วมกันพิจารณากำหนดแนวทางการระงับหรือบรรเทาผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้น ทั้งนี้ โดยกรอกรายละเอียดของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลตามแบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และดำเนินการส่งแบบฟอร์มดังกล่าวผ่านช่องทาง ดังต่อไปนี้

- ช่องทางที่ ๑ ผ่านอีเมล โดยส่งไปที่อีเมล [.]
- ช่องทางที่ ๒ ผ่าน [.] โดย [.]
- ช่องทางที่ ๓ ผ่าน [.] โดย [.]

๔.๒. หลังจากได้รับแจ้งตาม ๔.๑ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวน และควบคุมการละเมิดข้อมูลส่วนบุคคล รวมถึงกู้คืนข้อมูลส่วนบุคคลที่ถูกละเมิด และ/หรือกระบวนการที่ได้รับผลกระทบ

๔.๓. หลังจากได้รับแจ้งตาม ๔.๑ และปฏิบัติตาม ๔.๒ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแจ้งให้ผู้บริหารทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลดังกล่าว และร่วมกับฝ่ายเทคโนโลยีสารสนเทศหรือส่วนงานที่เกี่ยวข้องอื่น ๆ ในการประเมินความเสี่ยงของผลกระทบที่จะเกิดขึ้นต่อสิทธิและเสรีภาพของบุคคล โดยใช้หลักเกณฑ์การประเมินความเสี่ยงตามที่ระบุไว้ในคู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เวอร์ชัน ๑.๐ โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ในแต่ละระดับความเสี่ยงจะต้องดำเนินการดังนี้

๔.๓.๑. ในกรณีที่ผลประเมินชี้ว่าไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารชี้แจงและส่งเอกสารหรือหลักฐานอันแสดงให้เห็นว่าเหตุการณ์ละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใดให้สำนักงานตรวจสอบ

๔.๓.๒. ในกรณีที่ผลประเมินชี้ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้นต่อสำนักงาน

๔.๓.๓. ในกรณีที่ผลประเมินชี้ว่ามีความเสี่ยงสูง (high risk) ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ทั้งสำนักงานและเจ้าของข้อมูลทราบ

๔.๔. การดำเนินงานในข้อ ๔.๑ ข้อ ๔.๒ และข้อ ๔.๓ ต้องดำเนินการภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ

๔.๕. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลตาม ๔.๓ ต้องแจ้งไปยังสำนักงานและเจ้าของข้อมูลที่ได้รับผลกระทบ โดยในแต่ละกรณีต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

การแจ้งสำนักงาน

๑) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูล หรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ สน.บพ. มอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

๔) ข้อมูลเกี่ยวกับมาตรการที่ สน.บพ. ใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

หมายเหตุ : การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงาน ให้ดำเนินการโดยกรอกรายละเอียดตามแบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และส่งแบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าวผ่านช่องทางอิเล็กทรอนิกส์ โดยยื่นไปที่อีเมล saraban@pdpc.or.th โดยระบุชื่อเรื่อง “[แจ้งเหตุละเมิด]...(สำนักทะเบียน กรมการปกครอง)...”

การแจ้งเจ้าของข้อมูล

- ๑) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
 - ๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ สน.บพ. มอบหมายให้ทำหน้าที่ประสานงาน
 - ๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
 - ๔) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ สน.บพ. ใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อเสนอแนะเกี่ยวกับมาตรการที่เจ้าของข้อมูลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย
- ๔.๖. เมื่อปัญหาการละเมิดข้อมูลส่วนบุคคลได้รับการแก้ไขเรียบร้อยแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น รวมทั้งสรุปผลวิเคราะห์เหตุการณ์ละเมิด สิ่งที่ได้เรียนรู้ และแนวทางการแก้ไขเหตุการณ์ดังกล่าว เพื่อทำแนวทางป้องกันไม่ให้เกิดความเสียหายที่เพิ่มมากขึ้น รวมไปถึงการระบุหรือส่งมอบหน้าที่ต่าง ๆ ให้กับผู้รับผิดชอบเพื่อดำเนินการตามแผนต่าง ๆ ตามที่กำหนดไว้