แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลและรายงาน
ของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

สารบัญ

บทนำ

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) หรือ "พอช." ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลที่สถาบันฯ จัดเก็บ รวบรวม ใช้ หรือเปิดเผย โดยมุ่งเน้นการปฏิบัติให้เป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด แม้การปฏิบัติตามกฎหมายจะมีรายละเอียดที่ซับซ้อน แต่การยกระดับการคุ้มครองสิทธิของประชาชนถือเป็นภารกิจสำคัญในการขับเคลื่อนองค์กรอย่างโปร่งใส

หน้าที่ของ พอช. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 37 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พอช. มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) รวมถึงเจ้าของข้อมูลโดยไม่ชักช้า เพื่อระงับความเสียหายและสร้างความเชื่อมั่นในการประมวลผลข้อมูล

วัตถุประสงค์

1. เพื่อกำหนดขั้นตอนมาตรฐานในการจัดการและระงับเหตุเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล
2. เพื่อแก้ไขและบรรเทาผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลให้ได้รับความเสียน้อยที่สุด
3. เพื่อให้การรายงานเหตุต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลเป็นไปอย่างถูกต้องตามกรอบเวลาที่กฎหมายกำหนด

ขอบเขต

กระบวนการปฏิบัติงานที่กำหนดไว้ในแนวปฏิบัติฉบับนี้ใช้กับการจัดการและการรายงานเหตุละเมิดข้อมูลส่วน บุคคลประกอบไปด้วย ช่องทางการเฝ้าระวังและตรวจสอบ กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคลการ รายงานเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุละเมิดข้อมูลส่วนบุคลลต่อสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ภายใน 24 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้หากเป็นกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบ ต่อสิทธิและเสรีภาพของบุคคล พร้อมแนวทางการเยียวยาเจ้าของข้อมูลส่วนบุคคลในการแจ้งเหตุละเมิดให้เจ้าของ ข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าด้วย ทั้งนี้ พอช. จะดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบ ต่อสิทธิและเสรีภาพของบุคคล พอช. อาจแก้ไขเพิ่มเติมแนวทางนี้เป็นครั้งคราว โดย พอช. จะแจ้งให้ผู้ปฏิบัติงาน ให้ พอช. ทราบตามความเหมาะสม

ประเภทการแจ้ง	ระยะเวลา	เงื่อนไข/หมายเหตุ
การแจ้งภายใน พอช.	ภายใน 24 ชั่วโมง	เจ้าหน้าที่ผู้พบเหตุหรือผู้ประสานงาน DPO ต้องแจ้งต่อ ผู้อำนวยการ พอช. ทันทีที่ทราบเหตุ
การแจ้งต่อ สคส. (ภายนอก)	ภายใน 72 ชั่วโมง	ผู้อำนวยการ พอช. ดำเนินการแจ้งต่อ สคส. นับแต่ทราบเหตุ (ยกเว้นกรณีไม่มีความเสี่ยง)
การแจ้งเจ้าของข้อมูล	โดยไม่ชักช้า	ต้องแจ้งพร้อมแนวทางเยียวยา หากประเมินแล้วพบว่ามี ความเสี่ยงสูง ต่อสิทธิและเสรีภาพ

คำนิยาม

คำศัพท์	ความหมาย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะเช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เลข บัตรประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับ ขี่ เลขประจำตัวผู้เสียภาษีเลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) ทะเบียนรถยนต์ IP Address, Cookies, Log File เป็นต้น
การประมวลผลข้อมูลส่วน บุคคล (Processing of Personal Data)	การดำเนินการใดๆ กับข้อมูลส่วนบุคคล (อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วน บุคคลในลักษณะใดลักษณะหนึ่งได้) เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบ จัดโครงสร้างการปรับปรุงหรือการแก้ไขข้อมูล การดึงข้อมูล การให้คำปรึกษาที่ต้องใช้ ข้อมูลในการให้คำปรึกษา การใช้ข้อมูล การเปิดเผยด้วยการส่งต่อ การเผยแพร่ หรือ การกระทำใด ๆ เพื่อให้ข้อมูลสามารถเข้าถึงหรือใช้งานได้ การรวมข้อมูลเข้าด้วยกัน การดำเนินการเพื่อให้ข้อมูลสอดคล้องกัน การจำกัดการใช้งาน การลบ หรือการทำลาย ข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่สามารถระบุตัวตนได้จากข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้ อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทน คนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำ การแทนคนเสมือนไร้ความสามารถ รวมตลอดทั้งผู้ที่ถือว่าเป็น

คำศัพท์	ความหมาย
	เจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ผู้อำนวยการ (บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล)
ผู้ประมวลผลข้อมูลส่วน บุคคล (Data Processor)	บุคคลหรือองค์กรใดที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลส่วนบุคคล
เหตุละเมิดข้อมูลส่วนบุคคล	การละเมิดความปลอดภัยของข้อมูลส่วนบุคคลที่ที่มีการเก็บรวบรวมใช้หรือเผยแพร่ ซึ่งนำไปสู่ผลกระทบของเจ้าของข้อมูลส่วนบุคคล ความเสียหายและความไม่ชอบด้วยกฎหมาย เช่น • การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • การแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • การลบข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต • ข้อมูลส่วนบุคคลสูญหาย หรือถูกโจรกรรม • การประมวลผลข้อมูลส่วนบุคคลผิดพลาด/ไม่ถูกต้อง • การประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ที่กำหนดไว้
เจ้าหน้าที่คุ้มครองข้อมูลส่วน บุคคล (Data Protection Officer) หรือ DPO	เป็นเจ้าหน้าที่จะเข้ามาดูแลและให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลทั้งในองค์กร ไม่ว่าจะเป็นข้อมูลภายในขององค์กร หรือจะเป็นข้อมูลภายนอก โดย DPO ให้ คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล และตรวจสอบการใช้ข้อมูลส่วนบุคคล
เจ้าหน้าที่ประสานงาน คุ้มครองข้อมูลส่วนบุคคล	เป็นเจ้าหน้าที่สนับสนุนและประสานงานภายในหน่วยงาน หน้าที่ ดังนี้ (1) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) (2) ในกรณีพบเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล ถูกละเมิด ให้แจ้งไปยังเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคลของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) โดยไม่ชักช้า ภายใน 24 ชั่วโมง นับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เนื่องจากต้องแจ้งต่อไปยัง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง (3) รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาในการปฏิบัติหน้าที่

คำศัพท์	ความหมาย
	(4) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ในการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของ เจ้าข้อมูลส่วนบุคคลหรือข้อร้องเรียนใด ๆ ตามกฎหมายว่าด้วยคุ้มครองข้อมูลส่วน บุคคลในกรณีที่หน่วยงานเป็นผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (5) ติดต่อประสานงานภายในหน่วยงาน ให้มีการดำเนินงานที่ถูกต้องตามกฎหมาย ว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล รวมทั้งให้คำแนะนำแก่หน่วยงาน ลูกจ้างหรือผู้รับจ้างเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ (6) ทบทวนกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของหน่วยงาน ให้ถูกต้องและเป็นปัจจุบัน (7) ศึกษาและทำความเข้าใจกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน บุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
พอช.	สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)
แผน BCP	แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan : BCP)
แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ICT	แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ICT สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

แผนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

เมื่อหน่วยงานได้รับแจ้งข้อมูลเบื้องต้นว่าเกิดเหตุการณ์ไม่ปกติ เข้าข่ายเป็นเหตุการละเมิดข้อมูลส่วนบุคคล จำต้องดำเนินการตาม 5 ขั้นตอน ดังต่อไปนี้

1) ประเมินความน่าเชื่อถือของข้อมูลการละเมิดที่ได้รับแจ้ง และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถทำได้ หน่วยงานจะต้องดำเนินการประเมินว่าข้อมูลการละเมิดที่ได้รับแจ้งเบื้องต้นนั้น มีเหตุอันควรเชื่อได้ว่ามีการ ละเมิดข้อมูลส่วนบุคคลจริงหรือไม่ โดยหน่วยงานควรดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของ ข้อมูลส่วนบุคคล

- มาตรการเชิงองค์กร (organizational measures) เช่น นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การประเมินความเสี่ยง การสร้างความตระหนักและการอบรมความรู้แก่บุคลากรภายในองค์กร เป็นต้น

- มาตรการเชิงเทคนิค (technical measures) เช่น ระบบการเข้ารหัสข้อมูล (encryption) การทำข้อมูลแฝง (pseudonymisation) เป็นต้น

- มาตรการทางกายภาพ (physical measures) เช่น การมีระบบความปลอดภัยกล้องวงจรปิดสอดส่อง ดูแลบริเวณที่มีการเก็บเซิร์ฟเวอร์ของหน่วยงาน เป็นต้น ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้ หน่วยงานจะต้องดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับ หน่วยงานเอง เพื่อยืนยันว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วน บุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เพื่อประกอบพิจารณาในการดำเนินการขั้นตอนต่อไป

2) ป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคล ส่งผลกระทบเพิ่มเติมโดยทันที หน่วยงานได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด รวมทั้งประเมินความเสี่ยงของเหตุการละเมิด ข้อมูลส่วนบุคคลแล้วพบว่าเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้หน่วยงานดำเนินการใช้มาตรการในการป้องกัน ระงับ หรือแก้ไขให้เหตุการณ์ละเมิดนั้นสิ้นสุดลง หรือทุเลาลงเท่าที่สามารถกระทำได้โดยทันที

3) แจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่ามีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง

- ให้หน่วยงานจะต้องแจ้งในผู้อำนวยการทราบภายใน 24 นับแต่ทราบเหตุเท่าที่จะ สามารถกระทำได้

- หากเหตุการละเมิดดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานไม่สามารถแจ้งเหตุละเมิดดังกล่าวได้ จะต้องดำเนินการชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องกับการแจ้ง เหตุล่าช้าแก่สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) เพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้ง เหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่ พอช.โดยเร็วไม่เกินสิบวันนับแต่ทราบเหตุ

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) จะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน คณะกรรมการข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้กรณีมี เหตุจำเป็นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถแจ้งเหตุละเมิดที่ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของ บุคคลต้องโดยรายงานโดยไม่ชักช้าแต่ไม่เกินสิบห้าวันนับแต่ทราบเหตุ โดย สคส. จะพิจารณายกเว้นความผิดจากการ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าตามที่เห็นสมควร

4) แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงนั้นให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดดังกล่าวโดยไม่ชักช้า พร้อมกับแจ้งแนวทางในการเยียวยาผลกระทบที่เกิดจากเหตุ ละเมิดดังกล่าวไปด้วยให้ พอช. พร้อมรายงานตาม (3) เพื่อพิจารณาด้วย

วิธีการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล หนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หากโดยสภาพหน่วยงานไม่สามารถดำเนินการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล เนื่องจากไม่มีวิธีการติดต่อหรือโดยเหตุจำเป็นอื่นใด หน่วยงานอาจแจ้งเหตุการละเมิดเป็นกลุ่ม หรือแจ้งเป็นการทั่วไป ผ่านสื่อสาธารณะ สื่อสังคม ออนไลน์หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ ได้รับผลกระทบ หรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ เช่น เว็บไซต์ที่ให้บริการแก่ผู้รับบริการ เป็นต้น ทั้งนี้ การแจ้งในลักษณะดังกล่าวจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

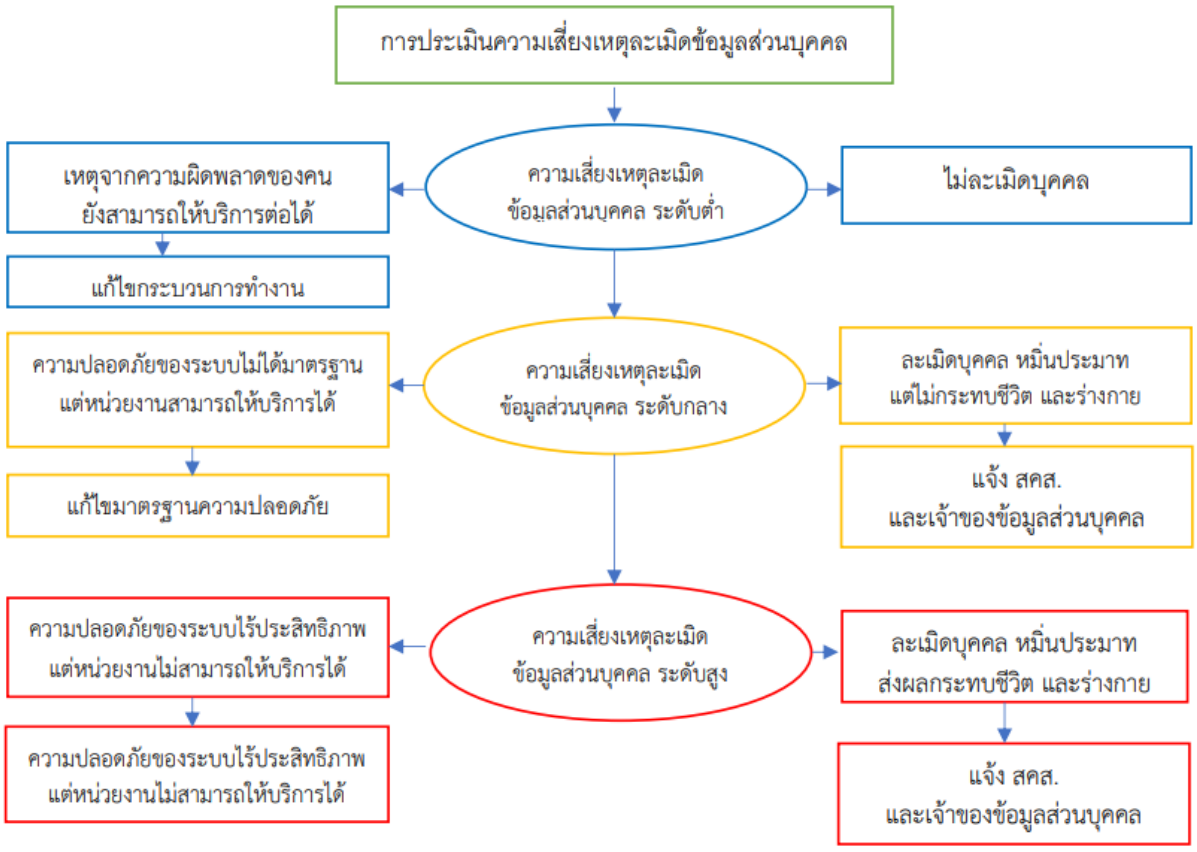
5) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการ ละเมิดข้อมูลส่วนบุคคลดังกล่าว หน่วยงานจะต้องดำเนินการป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็น ที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

การประเมินความเสี่ยงเหตุละเมิดบุคคล

ดังนั้น การประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล จึงแยกประเมินเป็นเหตุละเมิด และเหตุจากระบบการรักษาความมั่นคงปลอดภัยของข้อมูล ดังนี้

1. การประเมินความเสี่ยงเหตุละเมิดบุคคล ต้องประเมินจากผลกระทบที่อาจเกิดความร้ายแรงละเมิดต่อเจ้าของข้อมูลส่วนบุคคล เช่น ถูกนำไปประจาน ดูถูก ดูหมิ่นเกลียดชัง ถูกหมิ่นประมาท ถูกเลือกปฏิบัติ ถูกสะกดรอย ตาม ถูกทำร้ายร่างกาย การแบล็คเมล์เรียกค่าไถ่ ถูกสวมรอยบุคคล ขโมยรหัสผ่านหรือเข้าถึงข้อมูลอื่น ๆ ต่อไป
2. การประเมินความเสี่ยงหตุการรักษาความมั่นคงปลอดภัย ต้องประเมินจากความร้ายแรงของผลกระทบ (Impact Levels) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคาม ทางไซเบอร์มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ประกอบกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิด ข้อมูลส่วนบุคคล พ.ศ. 2565

ทั้งนี้ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ได้จัดทำปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับ ความเสี่ยง รายละเอียดตามภาคผนวก



การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนจากการตรวจสอบ หรือ ทดสอบ หรือเกิดจุดอ่อนของระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

1) ให้ผู้รับผิดชอบเทคโนโลยีสารสนเทศ

1.1 ดำเนินการตรวจสอบยับยั้งการโจมตีหรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

1.2 เสนอผู้บริหารของหน่วยงาน

1.3 กรณีที่มีการรั่วไหลหรือคาดว่าจะเกิดเหตุละเมิดข้อมูลส่วนบุคคลให้รีบแจ้งเจ้าหน้าที่ประสานงาน DPO หรือเจ้าหน้าที่คุ้มครองข้อมูล (DPO) ให้จัดทำรายงานฯ สรุปในเบื้องต้นนำเสนอให้ ปลัดกระทรวง ภายใน 24 ชั่วโมงนับตั้งแต่เมื่อทราบเหตุละเมิด เพื่อ พอช. จัดสรุปผลเสนอ สคส. ภายใน 72 ชั่วโมง

1.4 เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอ พอช. เพื่อ พอช. ส่งสรุปการดำเนินงานให้ สกมช. และ สคส. ต่อไป

2) ให้หัวหน้าหน่วยงาน

2.1 หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทาง วินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง

2.2 หากเป็นบุคคลภายนอก ให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่ เกี่ยวข้อง

2.3 ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค) 2.4 สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 วรรค 1 และ วรรค 4 ผู้ควบคุมข้อมูล ส่วนบุคคลมีหน้าที่จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า สำหนังานปลัดกระทรวงสาธารณสุขจึงได้กำหนด กระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล ดั้งนี้

1.การยับยั้งการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนที่อาจทำให้ข้อมูลรั่วไหล จากการตรวจสอบ หรือทดสอบหรือเกิดจุดอ่อนของระบบ

1) ให้ผู้รับผิดชอบของหน่วยงาน

1.1 ดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่า จะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

1.2 ให้แจ้งเจ้าหน้าที่ประสานงาน DPO ของหน่วยงาน เสนอหัวหน้าหน่วยงาน เพื่อหน่วยงานเตรียมร่าง

1.2.1 จัดทำรายงานในเบื้องต้นเสนอปลัดกระทรวง ให้ภายใน 24 ชั่วโมงนับตั้งแต่เมื่อทราบเหตุ ละเมิด เพื่อ พอช. จัดสรุปผลเสนอ สคส. ภายใน 72 ชั่วโมง

1.2.2 แจ้งเจ้าข้อมูลข้อมูลส่วนบุคคล

1.2.3 ทำการสื่อสารเกี่ยวกับเหตุการณ์ทั้งภายในและภายนอก

1.3 เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอ พอช. เพื่อ พอช. ส่งสรุปการดำเนินงานให้ สกมช. และ สคส. ต่อไป

2) ให้หัวหน้าหน่วยงาน

2.1 หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทาง วินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง

2.2 หากเป็นบุคคลภายนอก ให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่ เกี่ยวข้อง

2.3 ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

2.4 สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

2. การแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

ข้อ 1 รับแจ้งเหตุรายงานเหตุการณ์ การควบคุมความเสียหายและการแก้ไขสถานการณ์

1) ผู้พบเหตุรายงานเหตุการณ์ พบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจให้รีบแจ้งเจ้าหน้าที่ประสานงาน DPO ทราบโดยทันที

2) เจ้าหน้าที่ประสานงาน DPO รับแจ้งเหตุและตรวจสอบข้อมูลเบื้องต้นพร้อมบันทึกเหตุการณ์

3) เจ้าหน้าที่ประสานงาน DPO ประชุมและหรือยืนยันเหตุการณ์ (ภายใน 24 ชม.) เจ้าหน้าที่ประสานงาน DPO จะต้องประเมินเหตุการณ์ ดังนี้

(ก)กรณีที่ไม่พบต้นเหตุการณ์การละเมิด

(1) เจ้าหน้าที่ประสานงาน DPO จัดทำบันทึกเอกสาร

(2) เจ้าหน้าที่ประสานงาน DPO จะรายงานข้อมูลให้ผู้บริหารและสำเนา DPO รับทราบ

(ข)กรณีที่มีพบต้นเหตุการณ์การละเมิด

เจ้าหน้าที่ประสานงาน DPO จะต้องพิจารณาว่าเหตุการณ์ดังนี้

(1) กรณีที่เกี่ยวข้องระบบ IT ทีม IT / เจ้าหน้าที่ประสานงาน DPO ทำการหาสาเหตุ แก้ไข และควบคุม สถานการณ์ พร้อมทั้งวิเคราะห์ว่าเหตุการณ์นั้นว่าจำเป็นต้องปิดระบบ IT หรือไม่

1.1 กรณีที่ปิดระบบแล้ว

1.1.1 ทีม IT / เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

1) ดำเนินการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ICT / แผน BCP

2) กระบวนการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ICT / แผน BCP

3) กู้คืนระบบ (DR-Site)

4) กู้คืนกระบวนการสำคัญ

5) ติดตามสถานการณ์

6) ประกาศยกเลิกแผน BCP/DRP

1.1.2 กลับสู่ภาวะปกติ

1.1.3 ดำเนินการตามข้อ 2 ต่อไป

1.2 กรณีที่ไม่ปิดระบบแล้ว

1.2.1 ทีม IT / เจ้าหน้าที่ประสานงาน DPO ตรวจสอบขอบเขตของการ ละเมิดหรือการรั่วไหลข้อมูล

1.2.2 ทีม IT / เจ้าหน้าที่ประสานงาน DPO พิจารณาว่าความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อ สิทธิเสรีภาพของเจ้าของข้อมูล

1.2.3 ดำเนินการตามข้อ 2 ต่อไป

(2) กรณีที่ไม่เกี่ยวข้องกับระบบ IT

2.1 เจ้าหน้าที่ประสานงาน DPO รับทราบเหตุต้องดำเนินการ

1) ตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล

2) พิจารณาว่าระดับความเสี่ยงที่มีผลต่อสิทธิเสรีภาพของเจ้าของข้อมูล

2.2 ดำเนินการตามข้อ 2 ต่อไป

ข้อ 2 การวิเคราะห์ประเมินความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล

ทีม IT / เจ้าหน้าที่ประสานงาน DPO ตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล

ก. กรณีการละเมิดหรือรั่วไหลข้อมูลไม่ใช่ข้อมูลส่วนบุคคล

1) เจ้าหน้าที่ประสานงาน DPO จะรายงานข้อมูลให้ผู้บริหารและสำเนา DPO รับทราบ

2) ไม่ต้องแจ้งสคส. และหรือเจ้าขอข้อมูลส่วนบุคคล

3) ทีม IT ต้องจัดทำรายงานแจ้งคณะทำงานพัฒนาระบบเทคโนโลยีดิจิทัลและธรรมาภิบาลข้อมูลภาครัฐ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

ข. กรณีการละเมิดหรือรั่วไหลข้อมูลเป็นข้อมูลส่วนบุคคล

1) ทีม IT ต้องจัดทำรายงานแจ้งคณะทำงานพัฒนาระบบเทคโนโลยีดิจิทัลและธรรมาภิบาลข้อมูลภาครัฐ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

2) ทีม IT / เจ้าหน้าที่ประสานงาน DPO จัดเตรียมร่างการแจ้งเตือน (อนุมัติโดยผู้บริหาร)

3) ทีม IT / เจ้าหน้าที่ประสานงาน DPO ดำเนินการวิเคราะห์ระดับความเสี่ยง

3.1 กรณีมีระดับความเสี่ยงสูงต่อสิทธิของเจ้าของข้อมูล (ระดับความเสี่ยงสูง)

3.1.1 เจ้าหน้าที่ประสานงาน DPO จัดทำรายงานและแนวทางเยี่ยวยา แจ้งให้ผู้บริหาร หน่วยงานและ DPOเพื่อเสนอให้ผู้อำนวยการและส่ง สคส.รับทราบ (ภายใน 72 ชม.) ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลาให้หน่วยงานอาจพิจารณานำเสนอรายงาน เบื้องต้นต่อ สคส.และปลัดกระทรวงพร้อมกันได้

3.1.2 พอช. แจ้งสาเหตุและแนวทางเยี่ยวยาต่อเจ้าของข้อมูลส่วนบุคคล

3.1.3 พอช. ดำเนินการสื่อสารภายในและภายนอก

3.1.4 ทีม IT / เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินงาน

1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

3.2 กรณีมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล(ระดับความเสี่ยงน้อย หรือปานกลาง)

3.2.1 เจ้าหน้าที่ประสานงาน DPO แจ้งให้ผู้บริหารและ DPO เพื่อเสนอผู้อำนวยการ และส่ง สคส.รับทราบ (ภายใน 72 ชม.) ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลา หน่วยงานนำเสนอรายงานต่อ สคส.กับ CDC พร้อมกันได้

3.2.2 หน่วยงานดำเนินการสื่อสารภายในและภายนอก

3.2.3 ทีม IT / เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

3.3 กรณีไม่มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล

3.3.1 เจ้าหน้าที่ประสานงาน DPO แจ้งให้ ผู้บริหารและ DPO เพื่อเสนอ CDO รับทราบ

3.3.2 หน่วยงานดำเนินการสื่อสารภายใน

3.3.3 ทีม IT / เจ้าหน้าที่ประสานงาน DPO ต้องดำเนินการ

1) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

2) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

3) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

การรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลและคณะทำงานข้อมูลส่วนบุคคลประเมินผลกระทบของเหตุการณ์การ ละเมิดข้อมูลส่วนบุคคล ผลการพิจารณาระดับความรุนแรงมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลระดับ ต่ำ, ปานกลาง, สูง ให้ดำเนินการรายงานเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล