SACIT

ประกาศสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

เรื่อง แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

---

๑. วัตถุประสงค์

เพื่อใช้สำหรับเป็นแนวทางปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำของสถาบัน (DPO) ตลอดจนเป็นแนวทางในการปฏิบัติให้กับบุคลากร สถาบัน หรือบุคคลอื่นใดที่พบเจอเหตุละเมิดข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสถาบัน และเป็นไปตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) กำหนดตามกฎหมาย

๒. ขอบเขต

แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลนี้ ใช้ดำเนินการงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ในกรณีที่อาจเกิดหรือเกิดเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งอยู่ในความควบคุมดูแลของสถาบัน โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ต้องประเมินความเสี่ยงและแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล ว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลผู้เป็นเจ้าของข้อมูลเพียงใด

๓. คำจำกัดความ

“สถาบัน” หมายความว่า สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า สถาบัน ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า ผู้ได้รับคำสั่งแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำสถาบัน

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคล ซึ่งมีหน้าที่ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในนามของสถาบัน

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดย มิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ กระทำโดยปราศจากอำนาจหรือโดยมิชอบ หรือกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรือเหตุอื่นใด ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลผู้เป็นเจ้าของข้อมูลเพียงใด

๔. ประโยชน์ที่คาดว่าจะได้รับ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำสถาบัน (DPO) ตลอดจนบุคลากรสถาบัน หรือบุคคลอื่นใดที่พบเจอเหตุละเมิดข้อมูลส่วนบุคคลซึ่งเกี่ยวข้องกับสถาบัน ทราบแนวทางในการปฏิบัติเมื่อพบเจอเหตุละเมิดข้อมูลส่วนบุคคล และสามารถแจ้งเหตุดังกล่าว ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลตามระยะเวลาที่กฎหมายกำหนด

๕. ช่องทางการรับเรื่องหรือการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) มีช่องทางการรับเรื่องหรือการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลรวม ๖ ช่องทาง ดังนี้

๕.๑ ที่อยู่ : สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ๕๙ หมู่ ๔ ตำบลช้างใหญ่ อำเภอบางไทร จังหวัดพระนครศรีอยุธยา ๑๓๒๙๐

๕.๒ เว็บไซต์ : www.sacit.or.th

๕.๓ โทรศัพท์ : ๐๓๕-๓๖๗๐๕๔ - ต่อ ๑๙๔๑ - ๑๙๔๓

๕.๔ โทรสารโทร : ๐ ๓๕๓๖ ๗๐๕๑ สายด่วน ๑๒๘๙

๕.๕ ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (อีเมล) : info@sacit.or.th, saraban@sacit.or.th

๕.๖ Line https : //line.ee/zi9fpm6

หมายเหตุ : แบบฟอร์มการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล สามารถดาวน์โหลดได้ที่ เว็บไซต์ https://www.sacit.or.th ไปที่ หัวข้อ“ข้อมูลส่วนบุคคล หรือ PDPA” เลือกหัวข้อ “แบบฟอร์ม” และเลือกหัวข้อ “แบบฟอร์มการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล” พร้อมหลักฐานประกอบการพิจารณา

๖. แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

เมื่อได้รับเรื่อง แจ้งหรือพบเจอเหตุละเมิดข้อมูลส่วนบุคคลให้ดำเนินการโดยอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ช่องทางอิเล็กทรอนิกส์ในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลสำหรับผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๘ โดยมีขั้นตอน ดังนี้

๖.๑ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลขึ้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องตรวจสอบความน่าเชื่อถือและข้อเท็จจริงการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งต้องมีการประเมินความเสี่ยงว่าเหตุละเมิดที่เกิดขึ้นนั้นมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลมากน้อยเพียงใด โดยเหตุละเมิดข้อมูลส่วนบุคคลมีวิธีการได้มา ๓ กรณี ดังนี้

(๑) บุคลากรสถาบัน หรือบุคคลภายนอกแจ้งเหตุละเมิดข้อมูลส่วนบุคคลด้วยตนเอง

(๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพบเจอเหตุละเมิดด้วยตนเอง

(๓) ผู้ประมวลผลข้อมูลส่วนบุคคลพบเจอเหตุละเมิดข้อมูลส่วนบุคคล จะต้องดำเนินการแจ้งให้สถาบันทราบโดยเร็ว

๖.๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ดำเนินการพิจารณาความน่าเชื่อถือและข้อเท็จจริงว่าเหตุละเมิดดังกล่าวเป็นความจริง รวมทั้งได้ประเมินความเสี่ยงเสร็จสิ้นแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องดำเนินการแจ้งผลสรุปดังกล่าวแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมง หรือระยะเวลาท่าที่จะสามารถกระทำได้ หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) พิจารณาแล้วเห็นว่าเหตุละเมิดไม่เป็นความจริงและไม่มีความเสี่ยงใดๆ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องแจ้งเหตุยกเว้นดังกล่าว พร้อมหลักฐานแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) พิจารณา อนึ่ง ข้อมูลสาระสำคัญที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตามวรรคแรก ได้แก่ บทสรุปเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผลกระทบที่อาจเกิดขึ้น และมาตรการเยียวยา

๖.๓ เมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ประเมินความเสี่ยงแล้วพบว่ามีความเสี่ยงสูงต่อสิทธิและเสรีภาพ หรือมีความจำเป็น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ โดยมีข้อมูลสาระสำคัญ ได้แก่ บทสรุปเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ผลกระทบที่อาจเกิดขึ้น และมาตรการเยียวยา

๗. ตัวอย่างเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

๗.๑ เหตุการณ์ที่ไม่ถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

หน่วยงานแห่งหนึ่ง ขอเบอร์ติดต่อเจ้าหน้าที่ทุกคน เพื่อจัดทำหนังสือโทรศัพท์ในที่ทำงาน เจ้าหน้าที่ ก ไม่ให้เบอร์ติดต่อกับผู้ประมวลผลข้อมูลในการจัดทำหนังสือโทรศัพท์ และอ้างว่าผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งในความจริงผู้ประมวลผลสามารถกระทำได้ เนื่องจากเป็นการใช้ในการดำเนินงานภายในหน่วยงาน เพื่อให้การปฏิบัติงานมีความสะดวกและมีประสิทธิภาพยิ่งขึ้น แต่ทั้งนี้ผู้ควบคุมข้อมูลยังคงมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่นำมาใช้ในการดำเนินงานภายในหน่วยงาน

๗.๒ เหตุการณ์ที่ถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

เจ้าหน้าที่ในหน่วยงานแห่งหนึ่ง ได้ใช้กระดาษพิมพ์งานของตน ซึ่งด้านหลังเป็นสำเนาบัตรประจำตัวประชาชน ซึ่งเจ้าหน้าที่ดังกล่าวใช้กระดาษรียูสในการพิมพ์งานโดยที่ด้านหลังเป็นสำเนาบัตรประจำตัวประชาชน หากแต่กรณีดังกล่าวพบเจอโดยบุคคลภายนอกอาจถือได้ว่าเป็นการละเมิดข้อมูลส่วนบุคคล ทำให้ข้อมูลรั่วไหลไปยังภายนอกอาทำให้เจ้าของบัตรเสียหายได้

๘. การประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

๘.๑ ปัจจัยที่อาจจะนำมาพิจารณาในการประเมินความเสี่ยงโดยที่ข้อ ๑๒ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ได้กำหนดปัจจัยในการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งอาจพิจารณาจากปัจจัยดังต่อไปนี้

(๑) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

(๒) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๓) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๔) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้สามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่างๆ ด้วยหรือไม่ เพียงใด

(๕) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

(๖) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๗) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

(๘) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

๘.๒ ตัวอย่างการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้น มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด

โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าวต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่าง	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
๑	ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
๒	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
๓	ระบบไฟฟ้าใน Call center ของคณะ ส่วนงาน หน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราวส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งานเนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูล

ตัวอย่าง	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	คอมพิวเตอร์ของคณะ ส่วนงาน หน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว			ส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
๔	ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง
๕	ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร ๑ ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน ๒๔ ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน ๑๐ ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล ๑๐ ราย ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม

ตัวอย่าง	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
๖	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั่วไหลบนอินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตีเป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย
๗	เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล เกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคล	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบเนื่องจากยังไม่เกิดปัญหา	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกตามทางไซเบอร์ เว็บไซต์ผู้ให้บริการ Web

ตัวอย่าง	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
				Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
๘	โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา ๓๐ ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวบุคคลได้	ต้องแจ้งเนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบ	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุและตรวจสอบข้อมูลเพิ่มเติม
๙	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าว ไม่มีการเข้ารหัสและเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
๑๐	บริษัทแห่งหนึ่งทำการตลาดแบบตรงโดยการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคล	ต้องแจ้งเนื่องจากเป็นการส่งข้อมูลของเจ้าของข้อมูลส่วนบุคคลจำนวน	ต้องแจ้งเนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และ	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลบุคคลหรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วน

ตัวอย่าง	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	ที่รับอีเมลทั้ง ๑๐๐ คน เข้าไปในช่อง TO หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น	มาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูล แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	บุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วย หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำไม่จำเป็นต้องแจ้งเหตุ

ข้อ ๙. การรายงาน

เมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ได้แจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรียบร้อยแล้ว ให้รายงานเหตุละเมิดข้อมูลส่วนบุคคลต่อผู้อำนวยการทราบต่อไป

๑๐. แผนผัง (flowchart) แสดงขั้นตอนแนวปฏิบัติเมื่อเกิดเหตุละเมิดให้เป็นไปตามแนบท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๓ เดือน เมษายน พ.ศ. ๒๕๖๙

(ผู้ช่วยศาสตราจารย์อนุชา ทีรคานนท์)
ผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย

แนบท้ายประกาศสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

เรื่อง แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล แผนผัง (Flowchart) การปฏิบัติงาน กระบวนการในการปฏิบัติงานกรณีที่มีเหตุละเมิดข้อมูลส่วนบุคคลของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)