

คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เวอร์ชัน ๑.๐

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๑๕ ธันวาคม ๒๕๖๕

คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลฉบับนี้จัดทำขึ้น เพื่อเป็นแนวทางประกอบการพิจารณาของผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและช้อยกเว้นให้เป็นไปตาม **ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕** ซึ่งข้อ ๔ ได้กล่าวถึงประเภทของการละเมิดข้อมูล และข้อ ๑๒ กำหนดปัจจัยต่าง ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ในการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไว้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจึงได้จัดทำตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลเพื่อเป็นแนวทางสำหรับผู้ควบคุมข้อมูลส่วนบุคคลศึกษาเพิ่มเติม

หมายเหตุ ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลดังกล่าว เป็นเพียงแนวทางในการประเมินความเสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

การแก้ไขปรับปรุงเอกสาร (Version history)

เวอร์ชัน	วันที่	หมายเหตุ
เวอร์ชัน ๑.๐	๑๕ ธันวาคม ๒๕๖๕	ตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด

โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าวต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
๑. ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่นำเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่นำเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
๒. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
๓. ระบบไฟฟ้าใน call center ของผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราวส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของ	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งาน เนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว			ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
๔. ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคล จึงต้องแจ้งเหตุ
๕. ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร ๑ ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน ๒๔ ชั่วโมง พบว่า มีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน ๑๐ ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล ๑๐ ราย ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม ธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอก

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
			หรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
<p>๖. ผู้ควบคุมข้อมูลส่วนบุคคล ให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการรหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต</p>	<p>ต้องแจ้ง</p>	<p>ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั่วไหลบนอินเทอร์เน็ต</p>	<p>ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย</p>
<p>๗. เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล เกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้</p>	<p>ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้</p>	<p>ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา</p>	<p>ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์ เว็บไซต์ผู้ให้บริการ Web Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล</p>

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
			ต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
๘. โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา ๓๐ ชั่วโมง	ต้องแจ้ง เนื่องจาก ข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว และสามารถระบุตัวบุคคลได้	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหว ผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุ และตรวจสอบข้อมูลเพิ่มเติม
๙. โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
๑๐. บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูล	ต้องแจ้ง เนื่องจาก เป็นการส่งข้อมูล	ต้องแจ้ง เนื่องจากข้อมูล	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
<p>ส่วนบุคคลไปยังผู้รับข้อมูล แต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง ๑๐๐ คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น</p>	<p>ของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ</p>	<p>ส่วนบุคคลในอีเมลดังกล่าว อาจถูกนำไปใช้ และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ภายหลังได้</p>	<p>หรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไป และลักษณะของข้อมูลด้วย หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำ ไม่จำเป็นต้องแจ้งเหตุ</p>

หมายเหตุ ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลดังกล่าว เป็นเพียงแนวทางในการประเมินความเสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) ประกอบมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศฉบับนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย เหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั่นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจ หรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ข้อ ๕ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าจะโดยทางวาจา เป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเอง ว่ามีหรือน่าจะมี เหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

(๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด ข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่าการละเมิด ข้อมูลส่วนบุคคลหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรฐานการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และ มาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าว ทั้งในส่วนที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคล นั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่าการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยง ที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๒) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตาม (๑) พบว่า มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ ด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระวัง หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติม โดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี ที่จำเป็นและเหมาะสม

(๓) เมื่อพิจารณาจากข้อเท็จจริงตาม (๑) แล้วเห็นว่า มีเหตุอันควรเชื่อว่าการละเมิดข้อมูล ส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดแก่สำนักงานโดยไม่ชักช้าภายใน เจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยง ที่จะผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๔) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

(๕) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๖ ในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดตามที่สำนักงานกำหนด โดยในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้

(๑) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคลหรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๔) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ข้อ ๗ ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสอง ชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณาเว้นความผิดจากการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานโดยเร็ว ทั้งนี้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

สำนักงานอาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานพิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุ การละเมิดข้อมูลส่วนบุคคลแก่สำนักงานตามกำหนดเวลาในมาตรา ๓๗ (๔)

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดชอบ ของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

ข้อ ๘ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุ การละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน

ข้อ ๙ ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล แก่สำนักงานเพื่อประกอบการพิจารณาได้ หากผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าเหตุการละเมิดข้อมูล ส่วนบุคคลนั้น ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งรวมถึงกรณีที่ข้อมูล ส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของ ข้อมูลส่วนบุคคลได้ หรือข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยี ที่เพียงพอ หรือเหตุอื่นใดที่เชื่อถือได้

ในการยกข้อยกเว้นดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ให้ข้อมูลหรือส่งเอกสารหรือ หลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคง ปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานพิจารณา

ข้อ ๑๐ เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งเหตุ การละเมิดแก่สำนักงานแล้วหรืออยู่ระหว่างการเตรียมการเพื่อแจ้งสำนักงาน หากผู้ควบคุมข้อมูลส่วนบุคคล ได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อ สิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลพร้อม สารสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำ ได้โดยไม่ชักช้า

(๑) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๔) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

ข้อ ๑๑ ในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

การแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไป จะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ข้อ ๑๒ ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้

(๑) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

(๒) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๓) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๔) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพียงใด

(๕) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

(๖) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

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

(๘) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อ ๑๓ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๖ ธันวาคม พ.ศ. ๒๕๖๕

เจียรชัย ณ นคร

ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗

ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

โทรศัพท์: ๑๑๑๑ หรือ ๐๒-๑๔๒-๑๐๓๓ หรือ ๐๒-๑๔๑-๖๙๙๓

เฟสบุ๊ก: <https://www.facebook.com/pdpc.th>

เว็บไซต์: <http://www.pdpc.or.th>

ไปรษณีย์อิเล็กทรอนิกส์สำนักงาน: pdpc@mdes.go.th