สรุป 5 ข้อควรรู้เกี่ยวกับ PDPA

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA นั้น ได้บัญญัติบทบาทหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล หากท่านยังไม่แน่ใจว่าองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล รวมทั้งมีบทลงโทษกรณีละเลยหน้าที่ดังกล่าวตามกฎหมายอย่างไร ท่านสามารถอ่านเพิ่มเติมได้ที่ “รู้ก่อนโดนปรับ! การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล สิ่งที่องค์กรไม่ควรละเลย” อย่างไรก็ตาม ก่อนที่องค์กรจะพิจารณาดำเนินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลส่วนบุคคล เมื่อเกิดเหตุการณ์ที่เชื่อได้ว่ามีการละเมิดกับข้อมูลส่วนบุคคลที่อยู่ภายใต้การดูแลขององค์กร หลายองค์กรซึ่งอยู่ในสถานะผู้ควบคุมข้อมูลส่วนบุคคลอาจกังวล สงสัย และมีคำถามว่าองค์กรจะมีวิธีการหรือขั้นตอนในการรับมือเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวอย่างไร ให้สอดคล้องกับ PDPA และเมื่อเกิดเหตุละเมิดจะต้องแจ้งเหตุละเมิดแก่ สคส. และเจ้าของข้อมูลส่วนบุคคลในทันทีที่เกิดเหตุที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเลยหรือไม่ เพื่อคลายความสงสัยดังกล่าว สคส. ได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม เรื่อง “หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565” ซึ่งมีผลบังคับใช้เมื่อวันที่ 15 ธันวาคม 2565 ที่ผ่านมา เพื่อกำหนดแนวทางในการบริหารจัดการเหตุละเมิดข้อมูลส่วนบุคคล แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เมื่อได้รับแจ้งข้อมูลในเบื้องต้นว่ามีเหตุการละเมิดข้อมูลส่วนบุคคล

อะไรคือนิยามการละเมิดข้อมูลส่วนบุคคล ? ประกาศฯ ดังกล่าวได้นิยามการละเมิดข้อมูลส่วนบุคคล ไว้ว่าเป็นกรณีการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด โดย**เหตุการละเมิดข้อมูลส่วนบุคคลที่องค์กรมีหน้าที่จะต้องแจ้ง สคส. และเจ้าของข้อมูลส่วนบุคคลตาม PDPA นั้น จะต้องเป็นการละเมิดที่มีลักษณะที่เกี่ยวข้องกับการละเมิดความลับของข้อมูลส่วนบุคคล** หรือการละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล หรือ การละเมิดความพร้อมใช้งานของข้อมูล ส่วนบุคคล

5 ขั้นตอน แผนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

เมื่อองค์กรของท่านได้รับแจ้งข้อมูลเบื้องต้นว่าเกิดเหตุการณ์ไม่ปกติ เข้าข่ายเป็นเหตุการละเมิดข้อมูลส่วนบุคคล องค์กรของท่านในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจำต้อง**ดำเนินการตาม 5 ขั้นตอน** ดังต่อไปนี้

(1) ประเมินความน่าเชื่อถือของข้อมูลการละเมิดที่ได้รับแจ้งและตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้น โดยไม่ชักช้าเท่าที่จะสามารถทำได้ องค์กรจะต้องดำเนินการประเมินว่าข้อมูลการละเมิดที่ได้รับแจ้งเบื้องต้นนั้น มีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลจริงหรือไม่ โดย

ผู้ควบคุมข้อมูลส่วนบุคคลควรดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) เช่น นโยบายความมั่นคงปลอดภัยของข้อมูล การประเมินความเสี่ยง การสร้างความตระหนักและการอบรมความรู้แก่บุคลากรภายในองค์กร เป็นต้น และมาตรการเชิงเทคนิค เช่น ระบบการเข้ารหัสข้อมูล การทำข้อมูลแฝง เป็นต้น ซึ่งอาจรวมถึงมาตรการทางกายภาพ เช่น การมีระบบความปลอดภัย กล้องวงจรปิดสอดส่องดูแลบริเวณที่มีการเก็บเซิร์ฟเวอร์ขององค์กร เป็นต้น ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลเอง เพื่อยืนยันว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นจริงหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เพื่อประกอบพิจารณาในการดำเนินการขั้นตอนต่อไป ในส่วนของการระงับเหตุละเมิด และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าว

(2) ป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที หากผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิด รวมทั้งประเมินความเสี่ยงของเหตุการละเมิดข้อมูลส่วนบุคคลแล้วพบว่าเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการใช้มาตรการในการป้องกัน ระงับ หรือแก้ไขให้เหตุการณ์ละเมิดนั้นสิ้นสุดลง หรือทุเลาลงเท่าที่สามารถกระทำได้โดยทันที เช่น กรณีเว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล เกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลไม่สามารถเข้าใช้บริการได้ .

กรณีดังกล่าว เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งเหตุจากผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องตรวจสอบข้อเท็จจริงของเหตุดังกล่าว และประเมินความเสี่ยงของเหตุละเมิดดังกล่าวว่ามีผลกระทบอย่างไร อย่างในกรณีนี้ เป็นกรณีที่เกิดเหตุผิดพลาดบกพร่องของระบบที่ทำให้เจ้าของข้อมูลไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ ซึ่งเป็นเหตุละเมิดข้อมูลส่วนบุคคล เมื่อประเมินเหตุละเมิดดังกล่าวเรียบร้อยแล้ว ผู้ควบคุมข้อมูลจะต้องสั่งการให้ผู้ประมวลผลข้อมูลดำเนินการแก้ไขข้อบกพร่องของโปรแกรมในการตรวจสอบสิทธิการเข้าถึงดังกล่าวโดยทันที เพื่อระงับผลกระทบที่เกิดจากเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้ ในการดำเนินการเช่นว่านั้น ผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม เพื่อระงับเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว

(3) แจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ซึ่งปรากฏว่าเหตุการละเมิดดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลนั้น จะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้

แต่อย่างไรก็ตาม กรณีมีเหตุจำเป็นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถแจ้งเหตุละเมิดที่ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลภายใน 72 ชั่วโมงดังกล่าวได้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องกับการแจ้งเหตุล่าช้าแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่ สคส. โดยเร็วไม่เกินสิบห้าวันนับแต่ทราบเหตุ โดย สคส. จะพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าตามที่เห็นสมควร

(4) แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงนั้นให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดดังกล่าวโดยไม่ชักช้า พร้อมกับแจ้งแนวทางในการเยียวยาผลกระทบที่เกิดจากเหตุละเมิดดังกล่าวไปด้วย

อย่างไรก็ตาม หากโดยสภาพผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถดำเนินการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคล เป็นรายบุคคล เป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคม ออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ หรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ เช่น เว็บไซต์ที่ให้บริการแก่ลูกค้าขององค์กร เป็นต้น ทั้งนี้ การแจ้งในลักษณะดังกล่าวจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

(5) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องดำเนินการป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับ

หน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

อนึ่ง 5 ขั้นตอน ในการรับมือเหตุการละเมิดข้อมูลส่วนบุคคลข้างต้น เป็นแนวทางเบื้องต้นแก่ผู้ควบคุมข้อมูลส่วนบุคคลในการพิจารณาแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดบทบาทหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลไว้ อย่างไรก็ตาม องค์กรต่างๆ สามารถศึกษารายละเอียดเพิ่มเติมเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลได้ใน คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0 เพื่อเป็นแนวทางในการบริหารจัดการเหตุละเมิดข้อมูลส่วนบุคคลต่อไป

กฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

ผู้จัดทำ/เรียบเรียง : นางสาวณัฏฐนันท์ คงทน / นสม.ชก

หน่วยงาน : ฝ่ายข่าวและรายการ สวท.ปัตตานี

แหล่งที่มา : PDPA Thailand https://shorturl.asia/5rz2H