คู่มือขั้นตอนการแจ้งเหตุภารณ์ละเมิดข้อมูลส่วนบุคคล เพื่อแจ้งเหตุแก่หน่วยงาน และ/หรือเจ้าของข้อมูลส่วนบุคคล

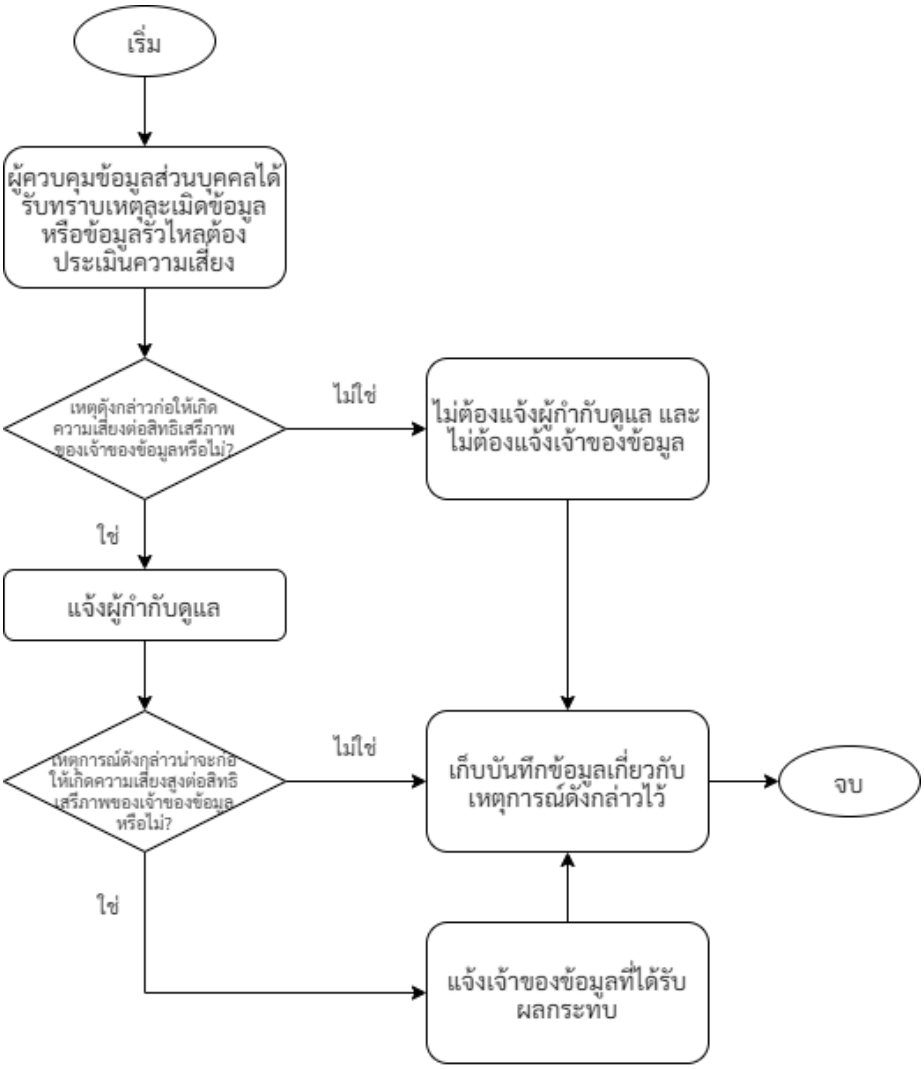
ดย. จะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (data breach) ซึ่งคำว่า “ข้อมูลส่วนบุคคลรั่วไหล” มีความหมายกว้างและครอบคลุมการที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษาหรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุก็ตาม

การพิจารณาเหตุละเมิดข้อมูลส่วนบุคคลเป็นเรื่องที่ละเอียดอ่อนมาก เพราะการดำเนินการอาจนำมาซึ่งการเปิดเผยข้อมูลส่วนบุคคลโดยไม่เจตนา อันกลฉ้อฉลที่ทำให้เจ้าหน้าที่ของ ดย. เปิดเผยข้อมูลส่วนบุคคลหรือโดยหลงผิดตัวบุคคลผู้เป็นเจ้าของข้อมูลที่แท้จริง อนึ่งการดำเนินการป้องกันภัยต่อเหตุละเมิด หรือตอบสนองต่อเหตุนั้นอาจเป็นเหตุให้เกิดการเปิดเผยข้อมูลส่วนบุคคลให้แก่เจ้าหน้าที่ ดย. ผู้ไม่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลอีกด้วย

โดยสรุปสาระสำคัญของกระบวนการได้ดังนี้

- เจ้าหน้าที่ต้องแจ้งแก่คณะทำงาน กรณีข้อมูลส่วนบุคคลรั่วไหลภายใน ๗๒ ชั่วโมงนับแต่ได้ทราบ เว้นแต่เหตุที่เกิดนั้นไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล กรณีที่ไม่อาจแจ้งเหตุได้ภายใน ๗๒ ชั่วโมง เจ้าหน้าที่จะต้องแจ้งเหตุผลแห่งการแจ้งเหตุล่าช้าต่อคณะทำงานด้วย โดยข้อมูลที่ต้องแจ้งมีดังต่อไปนี้
- คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง
- ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม
- คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว
- คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น
- ดย. แจ้งหน่วยงานกำกับดูแลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยประกอบด้วยข้อมูลประกอบเหตุละเมิดและข้อมูลที่หน่วยงานกำกับดูแลหรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลร้องขอเพิ่มเติม
- ดย. แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าต่อเมื่อการรั่วไหลของข้อมูลนั้นก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ในกรณีเช่นว่านี้จะต้องแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่เข้าใจง่ายและมีความชัดเจนและมีรายละเอียดอย่างน้อยดังต่อไปนี้
- คำอธิบายลักษณะของการรั่วไหลของข้อมูล
- ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบหรือ (ถ้ามี) เจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer)
- ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล ซึ่งรวมถึงความเสี่ยงต่อเจ้าของข้อมูล

- มาตรการที่เสนอแนะหรือแนวทางเยียวยาให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้
- ในกรณีที่มีการตั้งข้อสังเกตถึงความเกี่ยวพันกับเหตุละเมิดภัยคุกคามทางไซเบอร์ ให้คณะทำงานแจ้งไปยังศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ ดย. โดยให้ข้อมูลเฉพาะที่เกี่ยวข้องกับภัยคุกคามและหลีกเลี่ยงการให้ข้อมูลส่วนบุคคลอ่อนไหวแก่เจ้าหน้าที่ปฏิบัติการ เว้นแต่เป็นคำสั่งจากคณะทำงานคุ้มครองข้อมูลส่วนบุคคล ดย. หรือคณะกรรมที่มีส่วนเกี่ยวข้อง
- กระบวนการในการดำเนินการกรณีที่มีการละเมิดข้อมูลหรือข้อมูลรั่วไหลของ ดย.



ภาพที่ ๓ กระบวนการตอบสนองเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล