ประกาศสำนักงานเศรษฐกิจการคลัง
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

โดยที่มาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ในการดำเนินการตามบทบัญญัติดังกล่าว คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้มีประกาศ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ เพื่อกำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับแล้ว ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานเศรษฐกิจการคลังจึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ สำนักงานเศรษฐกิจการคลังได้สร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมให้บุคลากรสำนักงานเศรษฐกิจการคลัง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง และทรัพยากรที่ต้องใช้ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศนี้อย่างเคร่งครัด

/ข้อ ๕ สำนักงาน ...

ข้อ ๕ สำนักงานเศรษฐกิจการคลังได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือ เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมีมาตรการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยที่ครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัย ประกอบด้วยมาตรการเชิงองค์กร (Organization Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม และมาตรการทางกายภาพ (Physical Measures) ที่จำเป็น โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยได้คำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็น เหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(๔) มาตรการรักษาความมั่นคงปลอดภัยได้คำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไว้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(๕) มาตรการรักษาความมั่นคงปลอดภัย สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์จะครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Servers) เครื่องคอมพิวเตอร์ลูกข่าย (Clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์ และแอปพลิเคชันอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple Layers of Security Controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

/(๖) มาตรการ ...

(๖) มาตรการรักษาความมั่นคงปลอดภัยในส่วนที่เกี่ยวข้องกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยจะต้องประกอบด้วยการดำเนินการที่เหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน ดังนี้

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (Access Control) ที่มีการพิสูจน์และยืนยันตัวตน (Identity Proofing and Authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (Authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (Need -to -Know Basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (User Registration and De -registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of Privileged Access Rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit Trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๖ สำนักงานเศรษฐกิจการคลังได้กำหนดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น หรือการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๔ (๑) (๔) หรือมาตรา ๒๖ (๔) (๕) (ก) หรือ (ข) หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

/ข้อ ๗ สำนักงาน ...

ข้อ ๗ สำนักงานเศรษฐกิจการคลังจะพิจารณาทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ ๕ ในกรณีมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

กรณีมีเหตุการละเมิดข้อมูลส่วนบุคคล สำนักงานเศรษฐกิจการคลังมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๘ กำหนดให้มีข้อตกลงระหว่างสำนักงานเศรษฐกิจการคลังในฐานะผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล โดยให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งให้สำนักงานเศรษฐกิจการคลังทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อ ๙ ในกรณีที่สำนักงานเศรษฐกิจการคลังมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้สำนักงานเศรษฐกิจการคลังดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของสำนักงานเศรษฐกิจการคลังจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศฉบับนี้ด้วย

ประกาศ ณ วันที่ ๓ เมษายน พ.ศ. ๒๕๖๘

(นายพรชัย ฐีระเวช)
ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

สำนักงานเศรษฐกิจการคลัง กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) ตามมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมีทั้งหมด ๕ ข้อ ดังนี้

มาตรา ๓๗ (๑) *จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด*

ให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมอย่างน้อย ๓ ประเด็นดังนี้

๑) การธำรงไว้ซึ่งความลับ (confidentiality)

๒) ความถูกต้องครบถ้วน (integrity) และ

๓) สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยดำเนินการ ดังนี้

๑. <u>มาตรการรักษาความมั่นคงปลอดภัยเชิงองค์กร</u> (Organizational Measures)

สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน การอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็นและการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น โดยกำหนดให้มีมาตรการ ดังนี้

๑.๑ การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control)

(๑) กำหนดความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกัน การสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย รวมทั้งการล่วงรู้ไม่ว่าด้วยประการใด ๆ การทำสำเนา ข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญโดยไม่ได้รับอนุญาต ปราศจากอำนาจหรือ โดยมิชอบด้วยกฎหมาย ตลอดจนเพื่อป้องกันการทำสำเนา การนำอุปกรณ์ที่ใช้สำหรับจัดเก็บหรือประมวลผล ข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศไปโดยปราศจากมูลเหตุอันจะอ้างกฎหมายได้

(๒) บริหารจัดการและกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศที่อยู่ในระบบสารสนเทศของผู้ใช้งาน (User Responsibilities) ในรูปแบบต่าง ๆ เช่น สิทธิการเข้าถึง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและ ทำลาย รวมทั้งการเข้าถึงพื้นที่ที่สามารถเข้าถึงอุปกรณ์ทั้งหมดที่เกี่ยวข้อง เป็นต้น และต้องจัดให้มีการทบทวน ปรับปรุงบริหารจัดการและกำหนดสิทธิให้เป็นปัจจุบันอยู่เสมอ

(๓) จัดให้มีกระบวนการในการพิสูจน์และยืนยันตัวตน สำหรับการเข้าถึงและใช้งานระบบสารสนเทศที่มีการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ และการเก็บรวบรวมข้อมูลการขอสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศ

/(๔) จัดให้มี ...

(๔) จัดให้มีการตรวจสอบยืนยันตัวตนและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย ตลอดจนพื้นที่อื่นใดที่จัดเก็บอุปกรณ์ที่ใช้สำหรับจัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

จัดให้มีมาตรการในการลงทะเบียนและการถอนสิทธิผู้ใช้งานตลอดจนการจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิการบริหารจัดการ ข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และการถอดถอน หรือปรับปรุงสิทธิการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลายข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศ

๑.๓ มาตรการรักษาความมั่นคงปลอดภัยตามกฎหมาย (Legal Measures for Private Security) กรณีที่มีกฎหมายอื่นกำหนดให้สำนักงานเศรษฐกิจการคลังต้องกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น ให้สำนักงานเศรษฐกิจการคลังดำเนินการตามที่กฎหมายอื่นกำหนด แต่ต้องมีมาตรฐานไม่ต่ำกว่ากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๒. <u>มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิค</u> (Technical Measures)

สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ที่ครอบคลุมส่วนประกอบของระบบสารสนเทศที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple – Layered of Security Controls) เพื่อลดความเสี่ยงในบางสถานการณ์ โดยกำหนดให้มีมาตรการ ดังนี้

๒.๑ จัดให้มีวิธีการเพื่อสามารถตรวจสอบย้อนกลับเกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๒.๒ จัดให้มีกระบวนการบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลายข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบสารสนเทศหรือ บริการต่าง ๆ ยังดำเนินการได้อย่างต่อเนื่อง

๓. <u>มาตรการรักษาความมั่นคงปลอดภัยเชิงกายภาพ</u> (Physical Measures)

สำหรับป้องกันข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ตลอดจนอาคารและอุปกรณ์ที่เกี่ยวข้องให้ได้รับความปลอดภัยจากการถูกทำลาย ทั้งจากภัยธรรมชาติและการกระทำโดยมิชอบด้วยกฎหมาย ที่ประกอบด้วยมาตรการการควบคุมการเข้าถึง สิ่งปลูกสร้าง อาคาร พื้นที่ปฏิบัติงาน ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน และการควบคุมการใช้อุปกรณ์ และส่วนประกอบของระบบสารสนเทศ โดยกำหนดให้มีมาตรการดังนี้

/๓.๑ หน่วยงาน ...

๓.๑ หน่วยงานภายใน สศค. (สำนักงานเลขานุการกรม/กอง/ศูนย์/กลุ่ม) ที่เก็บรวบรวมข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศในทุกรูปแบบทั้งข้อมูลเอกสารและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ การจัดทำบันทึกการเข้าออกพื้นที่สำหรับบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ติดตั้งระบบกล้องวงจรปิด จัดให้มีทางเข้าออกด้วยระบบที่สามารถตรวจสอบกำหนดสิทธิเฉพาะบุคคลในการผ่านเข้าออกได้โดยใช้บัตรผ่าน ลายนิ้วมือ หรือวิธีการอื่นใดในการยืนยันตัวตน มีการล็อคประตูทุกครั้ง เป็นต้น เพื่อตรวจสอบผู้มีสิทธิเข้าออกหรือ ตรวจสอบและเฝ้าระวังผู้เข้าออกพื้นที่ และการเก็บข้อมูลส่วนบุคคลที่เป็นเอกสารในที่เก็บที่ควบคุมการเข้าถึงได้ ทั้งนี้ ให้กำหนดแต่เฉพาะผู้ที่เกี่ยวข้องเท่านั้นที่เป็นผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

ทั้งนี้ ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๔. มาตรการเสริมสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Measures to Enhance Understanding of Personal Data Security)

ส่งเสริมให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือ บุคคลอื่นใดที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ การล่วงรู้ไม่ว่าด้วยประการใด ๆ หรือการเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ มีความรู้ความเข้าใจและตระหนักรู้ถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแจ้งให้บุคคลดังกล่าวทราบและถือปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการที่เกี่ยวข้อง รวมทั้งกรณีที่ มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

๕. มาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล (Risk Management Measures in Personal Data Protection)

จัดให้มีมาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล โดยดำเนินการระบุความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลอันประกอบไปด้วยความเสี่ยงที่สำคัญที่อาจ เกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) ที่สำคัญ เพื่อการป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น และเพื่อการตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล เมื่อมีการ ตรวจพบเหตุอันเป็นภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ตลอดจนการรักษาและฟื้นฟู ความเสียหายที่เกิดจากภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็น เหมาะสม และเป็นไปได้ตามประเภทและระดับความเสี่ยง และให้ดำเนินการแจ้งให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่น ที่เป็นผู้ใช้งาน (User) หรือบุคคลอื่นใดที่เกี่ยวข้องทราบ และดำเนินการตามมาตรการอย่างเคร่งครัด

/๖. การทบทวน ...

๖. การทบทวนมาตรการรักษาความมั่นคงปลอดภัย (Review of Security Measures)

จัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล อยู่เสมอ และในกรณีเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกันที่มี ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน โดยกำหนดให้ต้องมีการทบทวนมาตรการรักษาความมั่นคงปลอดภัย ดังนี้

๖.๑ เมื่อมีเหตุละเมิดหรือกระทำการโดยมิชอบด้วยกฎหมายต่อข้อมูลส่วนบุคคล ให้ถือว่าสำนักงานเศรษฐกิจการคลังมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่เหตุหรือการกระทำนั้นไม่มีความเสี่ยงในการเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๖.๒ เมื่อสำนักงานเศรษฐกิจการคลังเห็นว่า มีการเปลี่ยนแปลงที่มีนัยสำคัญทางเทคโนโลยีสารสนเทศที่มีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย

๖.๓ ทบทวนมาตรการในการรักษาความมั่นคง ปลอดภัย อย่างน้อยปีละ ๑ ครั้ง

๗. มาตรการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processors Controlling Measures)

จัดให้มีมาตรการในการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ หรือการกระทำที่มิชอบด้วยกฎหมาย และต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลฉบับนี้ โดยกำหนดให้มีมาตรการ ดังนี้

๗.๑ ควบคุมบุคคลหรือนิติบุคคลที่เป็นผู้ให้บริการด้านการจัดเก็บข้อมูล ผู้พัฒนา ระบบสารสนเทศ ผู้รับจ้างบันทึกข้อมูล หรือผู้เกี่ยวข้องภายนอกที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศ รวมถึงผู้ใช้งานข้อมูลส่วนบุคคลที่สำนักงานเศรษฐกิจการคลังเป็นผู้ควบคุมข้อมูลส่วนบุคคลให้เป็นไปตามมาตรการรักษาความมั่นคงปลอดภัยเชิงกายภาพ

๗.๒ จัดให้มีข้อตกลงระหว่างสำนักงานเศรษฐกิจการคลังและผู้ประมวลผลข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร โดยต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้สำนักงานเศรษฐกิจการคลังทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

มาตรา ๓๗ (๒) *ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ*

โดยมีการดำเนินการ ดังต่อไปนี้

๑. <u>การประเมินก่อนส่งมอบข้อมูล</u>

๑.๑ ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

/๑.๒ ให้สอบถาม ...

๑.๒ ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด เพื่อให้ทราบระดับความละเอียดของข้อมูลที่ต้องการ โดยคำนึงถึงการใช้เท่าที่จำเป็นต้องใช้เท่านั้น เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล เช่น ชื่อ-นามสกุล เลขประจำตัว ๑๓ หลัก หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

๒. <u>เมื่อส่งมอบข้อมูล</u>

๒.๑ จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

๒.๒ ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๒.๓ แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

๓. <u>หลังส่งมอบข้อมูล</u>

๓.๑ ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก ๓ เดือน ๖ เดือน หรือ ๑ ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้น ลบทำลายข้อมูล

๓.๒ กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

มาตรา ๓๗ (๓) *จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม*

มีการดำเนินการ ดังต่อไปนี้

๑. มีการติดตามเป็นระยะว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

/๒. กรณีเจ้าของ ...

๒. กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๓. การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา ๓๗ (๔) *แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด*

มีการดำเนินการ ดังต่อไปนี้

๑. แจ้งให้พนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลังในฐานะตัวแทนของสำนักงานเศรษฐกิจการคลังให้ชัดเจน เช่น การส่งอีเมล และ แจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

๒. กำหนดวิธีปฏิบัติให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลังต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน ๗๒ ชั่วโมง (นับแต่ทราบเหตุ)

๓. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น

/๓.๑ ตัวอย่าง ...

๓.๑ <u>ตัวอย่างกรณีความเสี่ยงต่ำ:</u> ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

๓.๒ <u>ตัวอย่างกรณีความเสี่ยงสูง:</u> เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์ (ตรวจพบ ๑ เดือน หลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน ๗๒ ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

๓.๓ <u>ตัวอย่างกรณีความเสี่ยงต่ำ:</u> เจ้าหน้าที่ของหน่วยงานส่งอีเมลไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมล และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง ๒ คน ใน ๑๕ คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตาม แม้ข้อมูลสุขภาพจะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

<u>หมายเหตุ</u> กรณีตัวอย่างและวิธีปฏิบัติข้างต้นอ้างอิงจาก Guidelines ๐๑/๒๐๒๑ on Examples regarding Data Breach Notification สามารถศึกษาวิธีการปฏิบัติเพิ่มเติมได้จาก https://edpb.europa.eu/our-work-tools/public-consultations-art-๗๐๔/๒๐๒๑/guidelines-๐๑๒๐๒๑-examples-regarding-data-breach_en

---

มาตรา ๓๗ (๕) *ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล*

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในข้อนี้ ยังไม่มีความจำเป็นที่สำนักงานเศรษฐกิจการคลังต้องดำเนินการใด ๆ