



มาตรการรักษาความมั่นคงปลอดภัย ของผู้ควบคุมข้อมูลส่วนบุคคล

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 “ข้อ 4 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(4) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยงโดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน”



และมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) มาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม รวมทั้งมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล



ทั้งนี้ ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลของทุกสาย/ฝ่ายปฏิบัติให้เป็นไปตามมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเคร่งครัด เพื่อมิให้เกิดความเสียหายแก่บริษัทฯ