ข้อควรรู้...การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

โดย นางลลิตา สีพนมวัน
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
Email: lalita@opsmoac.go.th
สังกัดกลุ่มบริหารข้อมูลการเกษตร
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

“มาตรา 37 ข้อ (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด ” ซึ่งหากพิจารณาในภาพรวมที่นอกเหนือจากประเด็นด้านกฎหมายแล้ว ก็จะเกี่ยวข้องกับการดำเนินการด้านเทคโนโลยีดิจิทัล ซึ่งจะครอบคลุมถึงการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีดิจิทัล และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เพื่อจัดการความเสี่ยง ตลอดจนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ทั้งนี้ เนื่องจากปัจจุบันการประมวลผลข้อมูลส่วนบุคคลมีการนำเทคโนโลยีดิจิทัลมาเกี่ยวข้องในขั้นตอนต่างๆ ไม่มากก็น้อย ขึ้นอยู่กับนโยบาย ภารกิจและวัฒนธรรมการทำงานของแต่ละองค์กร เช่น การใช้เว็บไซต์แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงนโยบายความเป็นส่วนตัว ใช้แอปพลิเคชันในการจัดเก็บ รวบรวม แลกเปลี่ยนข้อมูลส่วนบุคคลเป็นต้น ดังนั้น เทคโนโลยีดิจิทัลจึงมีบทบาทเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างมาก

หากขยายความเพื่อให้เกิดความเข้าใจที่ชัดเจนเพิ่มมากขึ้น ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จะหมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล มาตรการรักษาความมั่นคงปลอดภัยจึงต้องครอบคลุมการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลนั้นจะอยู่ในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม โดยที่การเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ จะครอบคลุมถึงส่วนประกอบต่างๆ ของระบบสารสนเทศ อุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (client) และอุปกรณ์ต่างๆที่ใช้ ระบบเครือข่าย ซอฟต์แวร์ และแอปพลิเคชันอย่างเหมาะสม หากเราไม่สามารถ (1) รักษาความลับของข้อมูลส่วนบุคคลได้ (confidentiality) ก็จะเกิดปัญหาทำให้ข้อมูลส่วนบุคคลรั่วไหลออกไปได้ ซึ่งอาจจะเกิดขึ้นจากผู้ไม่ประสงค์ดีเจาะเข้าสู่ระบบ หรือเกิดจากความไม่ตั้งใจหรือตั้งใจของพนักงาน ตัวอย่างเช่น เอกสารหรือสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคล ถูกนำไปใช้งานต่อโดยไม่ได้ทำลายก่อน

หรือข้อมูลส่วนบุคคลถูกนำไปเผยแพร่ไว้บนเว็บไซต์ต่างๆ หรือเว็บไซต์ที่ผิดกฎหมาย การตั้งค่าเว็บไซต์หรือบริการคลาวด์ผิด ทำให้ข้อมูลส่วนบุคคลถูกเข้าถึงจากสาธารณะ (2) การป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ (integrity) จะมีผลกระทบทำให้ข้อมูลขาดความสมบูรณ์และขาดความน่าเชื่อถือ เช่น ข้อมูลในระบบทะเบียน ถูกไขโดยผู้ไม่มีสิทธิ หรือเสียหายจากการประมวลผลที่ผิดพลาดของโปรแกรมคอมพิวเตอร์ จำเป็นต้องใช้ข้อมูลจากเอกสารแทน ทำให้การปฏิบัติงานล่าช้า (3) การทำให้ผู้ที่มีสิทธิสามารถเข้าถึงและใช้ข้อมูลได้เมื่อมีความต้องการในการใช้งาน (availability) สามารถป้องกันข้อมูลเสียหายหรือสูญหาย ซึ่งอาจจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล เช่น ไฟล์ข้อมูลเกิดความเสียหายไม่สามารถเปิดใช้งานได้ ต้องนำไฟล์ข้อมูลที่ Backup ไว้กลับมาใช้แทน เป็นต้น

ดังนั้น เพื่อช่วยให้องค์กรหรือหน่วยงานสามารถปฏิบัติได้ตามกฎหมายฉบับนี้ *ผู้ควบคุมข้อมูลส่วนบุคคล* จำเป็นต้องให้ข้อเสนอแนะ ข้อสังเกต เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล สำหรับเป็นแนวปฏิบัติในการใช้งานข้อมูลส่วนบุคคล อย่างน้อยดังนี้

1. การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์จัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงมาตรการใช้งานและความมั่นคงปลอดภัย
2. การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
4. การกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาข้อมูลส่วนบุคคล
5. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและอปุกรณ์ที่ใช้ในการเก็บ รวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล

กล่าวโดยสรุป หน่วยงานที่มีการใช้ข้อมูลส่วนบุคคล การกำหนดมาตรการ หรือหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน มีความจำเป็นสำหรับผู้ปฏิบัติที่เกี่ยวข้อง และยังเป็นการสร้างภาพลักษณ์ที่ดีขององค์กรต่อประชาชน หรือผู้รับบริการ เพราะจะช่วยสร้างความมั่นใจว่าข้อมูลส่วนบุคคลที่ได้มอบให้แก่หน่วยงานไปนั้น จะได้รับการดูแลรักษาความปลอดภัยมิให้บุคคลอื่นล่วงรู้หรือนำไปใช้ในทางมิชอบ

อ้างอิง

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคค พ.ศ.2562
2. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563
3. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล,ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2564