สรุปการฝึกอบรม หลักสูตร กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ
ผ่านระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ ดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning)

ผู้รับการฝึกอบรม : นางสาวศุภกานต์ ล้อมนะลา
ตำแหน่ง : เจ้าพนักงานธุรการปฏิบัติงาน
สังกัด : กลุ่มช่วยอำนวยการและประสานราชการ สำนักงานเลขานุการกรม

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act: PDPA) เป็นกฎหมายที่กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของประชาชน เพื่อสร้างความเชื่อมั่นในกระบวนการบริหารราชการและการให้บริการสาธารณะ โดยหน่วยงานภาครัฐต้องดำเนินการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างมีมาตรฐาน โปร่งใส และเป็นไปตามกฎหมาย

- ผู้ควบคุมข้อมูลส่วนบุคคลต้อง ขอความยินยอม จากเจ้าของข้อมูล ก่อนการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล เว้นแต่มีข้อยกเว้นตามกฎหมาย ได้แก่
  - การจัดทำเอกสารทางประวัติศาสตร์หรือจดหมายเหตุ
  - การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
  - การดำเนินการเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา
  - การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือตามอำนาจหน้าที่ที่กฎหมายกำหนด
- หน่วยงานภาครัฐต้องดำเนินการเก็บรักษาข้อมูลส่วนบุคคลด้วยมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และปฏิบัติตามหลักธรรมาภิบาลข้อมูล
- การใช้ข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ที่ชัดเจน และแจ้งให้เจ้าของข้อมูลทราบอย่างโปร่งใส

๑. ขอบเขตของข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลที่สามารถระบุตัวบุคคลได้โดยตรงหรือโดยอ้อม เช่น ชื่อ-สกุล, เลขประจำตัวประชาชน, หมายเลขโทรศัพท์, ที่อยู่, อีเมล, เชื้อชาติ, ศาสนา, พฤติกรรมทางเพศ, ข้อมูลสุขภาพ ประวัติการทำงาน, รายละเอียดทางการเงิน และประวัติอาชญากรรม

ข้อยกเว้น ข้อมูลของผู้ที่ถึงแก่ความตายและข้อมูลของนิติบุคคลไม่ถือเป็นข้อมูลส่วนบุคคลตามกฎหมายนี้

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

เช่น เชื้อชาติ, ความเชื่อทางศาสนาหรือปรัชญา, ความคิดเห็นทางการเมือง, พฤติกรรมทางเพศ, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลชีวภาพ, ข้อมูลพันธุกรรม, และข้อมูลสหภาพแรงงาน ซึ่งข้อมูลประเภทนี้ต้องได้รับความยินยอมเป็นลายลักษณ์อักษร และต้องมีมาตรการคุ้มครองอย่างเข้มงวด

๒. บทบาทของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคล ที่มีอำนาจในการตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคล ต้องปฏิบัติดังนี้

๒.๑ การเก็บรวบรวมข้อมูล: ต้องมีเหตุผลที่ชอบด้วยกฎหมาย และแจ้งเจ้าของข้อมูลถึงวัตถุประสงค์และวิธีการใช้งาน

๒.๒ การใช้และเปิดเผยข้อมูล: ใช้ข้อมูลเฉพาะตามวัตถุประสงค์ที่กำหนด และต้องได้รับความยินยอมหรือมีข้อกฎหมายรองรับ

๒.๓ การจัดเก็บและรักษาความปลอดภัย: จัดเก็บข้อมูลในระบบที่ปลอดภัย พร้อมมาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหล หรือการถูกดัดแปลงข้อมูล

๒.๔ สิทธิของเจ้าของข้อมูล: ต้องอำนวยความสะดวกให้เจ้าของข้อมูลเข้าถึง แก้ไข ปรับปรุง ระงับ หรือเพิกถอนข้อมูลของตนได้ หรือการทำให้ข้อมูลไม่สามารถระบุตัวตนได้

๓. หลักการขอความยินยอม (Consent)

การขอความยินยอมต้องมีความโปร่งใส ชัดเจน ระบุวัตถุประสงค์อย่างชัดเจน เจ้าของข้อมูลสามารถถอนความยินยอมได้ตลอดเวลา สำหรับข้อมูลอ่อนไหวต้องขอความยินยอมเป็นลายลักษณ์อักษรหรือเทียบเท่า

๔. การคุ้มครองข้อมูลและการรายงานเหตุละเมิด (Data Breach)

- ต้องใช้มาตรการด้านเทคนิค เช่น การเข้ารหัสข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูล
- หากเกิดเหตุข้อมูลรั่วไหล ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และแจ้งเจ้าของข้อมูลทันทีหากมีความเสี่ยงต่อสิทธิและเสรีภาพ

๕. บทกำหนดโทษกรณีไม่ปฏิบัติตาม

การละเมิดกฎหมายอาจมีโทษทั้งทางปกครอง แพ่ง และอาญา เช่น การปรับทางปกครอง การชดใช้ค่าเสียหาย หรือโทษจำคุกและปรับตามกฎหมายที่เกี่ยวข้อง

๖. ข้อคิดสำคัญสำหรับหน่วยงานภาครัฐ

การปฏิบัติตาม PDPA ไม่เพียงป้องกันการละเมิดกฎหมาย แต่ยังสร้างความเชื่อมั่น โปร่งใส และความน่าเชื่อถือให้กับภาครัฐ อีกทั้งยังเป็นการเคารพสิทธิของประชาชนอย่างแท้จริง บุคลากรควรนำความรู้ที่ได้รับจากหลักสูตรนี้ไปประยุกต์ใช้ในการปฏิบัติงาน เช่น การจัดเก็บและใช้ข้อมูลอย่างเป็นระบบ การจัดทำคู่มือภายใน และการใช้เทคโนโลยีเพื่อบริหารจัดการข้อมูลได้อย่างมีประสิทธิภาพ

ทั้งนี้ ผู้เข้ารับการอบรมสามารถนำความรู้ที่ได้รับจาก หลักสูตรกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ มีความสำคัญต่อการยกระดับการทำงานของหน่วยงานภาครัฐให้เป็นไปตามมาตรฐานสากล ลดความเสี่ยงทางกฎหมาย และสร้างความมั่นใจแก่ประชาชนว่าข้อมูลของตนได้รับการปกป้องอย่างเหมาะสม
