

กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ (PDPA for Government Officer)

โดย นางสาวสุพัตรา ชันศรี
นักวิชาการแผนกที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

- เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) สำหรับเจ้าหน้าที่และผู้ปฏิบัติงานในหน่วยงานภาครัฐ
- เพื่อให้ผู้ปฏิบัติงานสามารถเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลในการปฏิบัติราชการได้อย่างถูกต้อง สอดคล้องกับกฎหมาย และไม่ละเมิดสิทธิขั้นพื้นฐานของประชาชน
- เพื่อสร้างความตระหนักรู้เกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงการรับมือและจัดการเมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในหน่วยงานภาครัฐ
- เพื่อสนับสนุนการเปลี่ยนผ่านสู่การเป็นรัฐบาลดิจิทัล (Digital Government) ที่มีธรรมาภิบาล และความน่าเชื่อถือในการบริหารจัดการข้อมูล

สรุปเนื้อหา

๑. นิยามและขอบเขตของข้อมูลส่วนบุคคล

๑.๑ ข้อมูลส่วนบุคคล (Personal Data): ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, อีเมล, พิกัดตำแหน่งที่อยู่ (Location Data), ภาพถ่ายใบหน้า, ข้อมูลชีวมิติ (Biometrics)

๑.๒ ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data): ข้อมูลที่ต้องได้รับการคุ้มครองเป็นพิเศษตามมาตรา ๒๖ เช่น เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ/ศาสนา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ข้อมูลพันธุกรรม, ข้อมูลชีวมิติ ซึ่งการประมวลผลต้องได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent) หรือเข้าข้อยกเว้นตามที่กฎหมายกำหนดไว้เท่านั้น

๒. ผู้มีส่วนเกี่ยวข้องตามกฎหมาย PDPA

๒.๑ เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เจ้าของข้อมูลส่วนบุคคล หรือ Data Subject ก็คือคนที่ข้อมูลส่วนบุคคลชุดนั้นๆ จะเข้ามาที่ตัวตนของบุคคลนั้นได้ ซึ่งก็คือตัวเรานั่นเอง ภายใต้ PDPA เจ้าของข้อมูลเป็นผู้ได้รับการปกป้องคุ้มครองและมีสิทธิต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคลของตน

๒.๒ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller คือคน บริษัทหรือองค์กรต่าง ๆ ที่เป็นคนตัดสินใจว่า จะมีการประมวลผลข้อมูลส่วนบุคคลอะไร เพื่ออะไร อย่างไร ภายใต้ PDPA ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติตาม PDPA ให้ครบถ้วน เช่น นางเอขายของออนไลน์ และรับข้อมูลที่อยู่สำหรับจัดส่งสินค้าให้ลูกค้า นางเอก็จัดเป็น Data Controller และบริษัทถึงแม้จะมีพนักงานคนแรก และคนเดียว ก็เป็น Data Controller เพราะต้องใช้ข้อมูลเพื่อจ่ายเงินเดือนให้พนักงาน

๓. หลักการประมวลผลข้อมูลส่วนบุคคลและฐานอำนาจกฎหมาย (Lawful Basis)

การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของภาครัฐ ต้องกระทำโดยมีฐานกฎหมายรองรับ (Lawful Basis) ได้แก่:

๑) ฐานภารกิจเพื่อประโยชน์สาธารณะ หรือการใช้อำนาจรัฐ (Public Task / Official Authority): การปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานภาครัฐ (ฐานหลักที่ภาครัฐใช้มากที่สุด)

๒) ฐานการปฏิบัติตามกฎหมาย (Legal Obligation): การปฏิบัติตามบทบัญญัติแห่งกฎหมายที่บังคับใช้กับหน่วยงาน

๓) ฐานสัญญา (Contractual Obligation): การปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา

๔) ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest): ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลอื่น (เว้นแต่ประโยชน์ดังกล่าวขัดแย้งกับสิทธิขั้นพื้นฐานของเจ้าของข้อมูล)

๕) ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ (Vital Interest)

๖) ฐานความยินยอม (Consent): ใช้เมื่อไม่มีฐานกฎหมายอื่นรองรับ โดยการขอความยินยอมต้องทำโดยชัดแจ้ง เป็นอิสระ และสามารถถอนความยินยอมได้ตลอดเวลา

๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

๔.๑ สิทธิได้รับการแจ้งให้ทราบ (Right to be Informed): ผ่านหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice)

๔.๒ สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (Right of Access)

๔.๓ สิทธิในการแก้ไขข้อมูลให้ถูกต้อง (Right to Rectification)

๔.๔ สิทธิในการขอใหลบ หรือทำลายข้อมูล (Right to Erasure / Right to be Forgotten)

๔.๕ สิทธิในการระงับการใช้ข้อมูล (Right to Restriction of Processing)

๔.๖ สิทธิในการคัดค้านการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล (Right to Object)

๔.๗ สิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability)

๕. ผู้ควบคุมข้อมูลส่วนบุคคล จะสามารถรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ได้อย่างไร

บุคคลธรรมดา หรือนิติบุคคล (บริษัท ห้างร้าน มูลนิธิ สมาคม หน่วยงาน องค์กร ร้านค้า หรืออื่นใดก็ตาม) หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ หรือมีการนำข้อมูลส่วนบุคคลไปใช้ หรือนำไปเปิดเผยไม่ว่าจะวัตถุประสงค์ใดก็ตาม จำเป็นต้องได้รับ คำยินยอม (Consent) จากเจ้าของข้อมูลด้วย เว้นแต่จะเป็นไปตามข้อยกเว้นที่ พ.ร.บ.กำหนดไว้ โดยมีข้อยกเว้นดังต่อไปนี้

๕.๑ ข้อยกเว้นสำหรับข้อมูลส่วนบุคคลทั่วไป (Personal Data)

๑) จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ที่เกี่ยวข้องกับการศึกษาวิจัยหรือการจัดทำสถิติ

๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓) จำเป็นเพื่อปฏิบัติตามสัญญากับเจ้าของข้อมูล เช่น การซื้อขายของออนไลน์ ต้องใช้ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล

๔) จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

๕) จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น

๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ส่งข้อมูลพนักงานให้กรมสรรพากรเรื่องภาษี เป็นต้น

๕.๒ ข้อยกเว้นสำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๒) การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิสมาคมองค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ เป็นต้น

๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความยินยอมของเจ้าของข้อมูล

๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๕) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เกี่ยวกับ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ เช่น การเก็บข้อมูลสุขภาพของพนักงานซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) องค์กรมักใช้ข้อนี้ในการอ้างสิทธิที่จำเป็นต้องเก็บข้อมูลนี้ไว้ เป็นต้น ประโยชน์ด้านสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม, หลักประกันสุขภาพแห่งชาติ / การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์สถิติ หรือประโยชน์สาธารณะอื่น / ประโยชน์สาธารณะที่สำคัญ

๖. มาตรการรักษาความมั่นคงปลอดภัยและความรับผิดชอบตามกฎหมาย

มาตรการความปลอดภัย (Security Measures): ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งทางเทคนิค (Technical Measures) และทางองค์กร (Organizational Measures) เช่น การกำหนดสิทธิ์เข้าถึงข้อมูล (Access Control), การเข้ารหัสข้อมูล (Encryption), และการอบรมเจ้าหน้าที่การแจ้งเหตุการณ์ละเมิด (Data Breach Notification): หากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต้องแจ้งสำนักงาน คปส. ภายใน ๗๒ ชั่วโมง และแจ้งเจ้าของข้อมูลทราบหากมีความเสี่ยงสูง

บทลงโทษของผู้ที่ไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) มี ๓ บทลงโทษ ได้แก่

๑) โทษทางแพ่ง

โทษทางแพ่งกำหนดให้ชดเชยค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก ๒ เท่าของค่าเสียหายจริง

๒) โทษทางอาญา

โทษทางอาญามีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ ประเภทข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) ส่วนกรณีหากผู้กระทำความผิด คือ บริษัท (นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ ผู้บริหาร กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน

๓) โทษทางปกครอง

โทษทางปกครอง ปรับ ตั้งแต่ ๑ ล้านบาทจนถึงสูงสุดไม่เกิน ๕ ล้านบาท ซึ่งโทษปรับสูงสุด ๕ ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดเชยค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

ประโยชน์ที่ได้รับตนเอง

1. มีความรู้ความเข้าใจอย่างถูกต้องในหลักการและข้อกฎหมาย PDPA ลดความเสี่ยงในการปฏิบัติงานผิดพลาดที่อาจนำไปสู่ความเสียหายทางอาญา หรือทางปกครอง
2. สามารถนำแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลไปประยุกต์ใช้กับงานวิชาการแผนที่ภาพถ่าย เช่น การจัดการข้อมูลแผนที่ดิน ข้อมูลภาพถ่ายทางอากาศ หรือข้อมูลพิกัดเชิงพื้นที่ที่มีการเชื่อมโยงกับข้อมูลชื่อ-นามสกุล และสิทธิถือครองของประชาชน
3. พัฒนาทักษะดิจิทัล (Digital Literacy) และเพิ่มพูนความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ เสริมสร้างความเป็นมืออาชีพในการเป็นข้าราชการยุคดิจิทัล

ประโยชน์ต่อองค์กร

1. ช่วยให้หน่วยงานปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลได้อย่างถูกต้อง ลดความเสี่ยงถูกดำเนินคดีหรือเปรียบเทียบปรับ
2. เพิ่มประสิทธิภาพการบริหารจัดการระบบข้อมูลแผนที่: สร้างมาตรฐานในการจัดเก็บ รักษา และประมวลผลข้อมูลภาพถ่ายและแผนที่ดิจิทัลให้มีระบบการเข้าถึงที่ปลอดภัย ป้องกันการรั่วไหลของข้อมูล
3. ยกระดับภาพลักษณ์ของหน่วยงานราชการให้เป็นองค์กรทันสมัย มีความโปร่งใส และใส่ใจในการคุ้มครองข้อมูลของประชาชน
4. ขับเคลื่อนองค์กรสู่รัฐบาลดิจิทัล: ส่งเสริมให้บุคลากรภายในหน่วยงานมีความพร้อมในการปรับเปลี่ยนองค์กรไปสู่การเป็นหน่วยงานรัฐบาลดิจิทัล (Digital Government Alignment)

ประโยชน์ต่อสาธารณะ

1. สร้างความคุ้มครองและสร้างความมั่นใจแก่ประชาชน: ประชาชนได้รับความมั่นใจว่าข้อมูลส่วนบุคคล ข้อมูลที่ดิน และข้อมูลตำแหน่งที่มอบให้แก่หน่วยงานรัฐจะได้รับการดูแลรักษาอย่างปลอดภัย ไม่ถูกนำไปใช้ผิดวัตถุประสงค์
2. ส่งเสริมการให้บริการภาครัฐที่ปลอดภัยและโปร่งใส: ช่วยให้การพัฒนาบริการภาครัฐผ่านระบบดิจิทัลมีความสะดวกรวดเร็ว โปร่งใส และปลอดภัย สามารถเข้าถึงบริการได้ง่ายโดยไม่มีความกังวลเรื่องข้อมูลรั่วไหล
3. ยกระดับบรรทัดฐานการคุ้มครองสิทธิในสังคม: เป็นการสร้างมาตรฐานใหม่ทางสังคมในการเคารพสิทธิความเป็นส่วนตัว (Privacy Right) ของประชาชนทุกคนอย่างเท่าเทียม

แหล่งที่มา

หลักสูตร : กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ (PDPA for Government Officer)

บรรยายโดย : ดร.มนต์ศักดิ์ โชติเจริญธรรม ผู้อำนวยการฝ่ายดาตาโซลูชัน สำนักงานพัฒนารัฐบาลดิจิทัล

สถาบัน/หน่วยงาน/ระบบ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

รูปแบบหลักสูตร : หลักสูตรออนไลน์ (TDGA E-Learning)

ช่วงเวลาการฝึกอบรม : ช่วงสิงหาคม - กันยายน ๒๕๖๔