แบบรายงานผลการเข้ารับการฝึกอบรม/สัมมนา

ด้วยข้าพเจ้า นายคำรณ จันทร์ต้น ตำแหน่ง ผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบลบ้านห้วยเคียน สังกัด โรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังทอง กองสาธารณสุขและสิ่งแวดล้อม ได้เข้าร่วมโครงการอบรมเชิงปฏิบัติการ หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง (e-learning) ในวันที่ ๒๒ พฤศจิกายน พ.ศ.๒๕๖๘ นั้น

บัดนี้ ข้าพเจ้าได้เข้ารับการฝึกอบรมหลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการฝึกอบรมให้ทราบ ดังนี้

๑. การฝึกอบรมดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ สร้างความรู้ความเข้าใจในการปฏิบัติหน้าที่ วัตถุประสงค์หลักของการฝึกอบรมคือเพื่อให้กลุ่มเป้าหมายมีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับ "การปฏิบัติหน้าที่" ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยครอบคลุมบทบาทของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller), ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor), เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO), รวมถึงลูกจ้างและผู้รับจ้างที่เกี่ยวข้อง

๒. ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้ และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่หน่วยงานรัฐ ภาคเอกชน และประชาชนทั่วไป เพื่อให้สามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. เนื้อหาและหัวข้อวิชาของหลักสูตรการฝึกอบรม มีดังนี้

บทที่	เนื้อหาหลักสูตร
๑	ความรู้เบื้องต้น และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
๒	ข้อมูลส่วนบุคคล
๓	ผู้ควบคุมคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
๔	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๕	สิทธิของเจ้าของข้อมูลส่วนบุคคล
๖	หน้าที่ในการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๗	การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
๘	แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
๙	การรักษาความมั่นคงปลอดภัยขอของข้อมูลส่วนบุคคล
๑๐	ความรับผิดชอบ
๑๑	การกำกับดูแลและบังคับใช้กฎหมาย

สรุปหลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง และผู้รับจ้าง

เอกสารสรุปฉบับนี้สังเคราะห์เนื้อหาหลักจากหลักสูตรการปฏิบัติหน้าที่ของผู้เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยมุ่งเน้นกรอบกฎหมายและแนวปฏิบัติที่สำคัญภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ประเด็นสำคัญคือการกำหนดนิยามของ "ข้อมูลส่วนบุคคล" และการจำแนกบทบาทของผู้มีส่วนได้เสียหลัก ได้แก่ เจ้าของข้อมูล (Data Subject) ผู้ควบคุมข้อมูล (Data Controller) ผู้ประมวลผลข้อมูล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งแต่ละฝ่ายมีหน้าที่และความรับผิดชอบที่แตกต่างกัน

หัวใจสำคัญของการปฏิบัติตามกฎหมายคือการประมวลผลข้อมูล (การเก็บรวบรวม ใช้ หรือเปิดเผย) ต้องเป็นไปตามหลักการพื้นฐาน ๘ ประการ เช่น การจำกัดการเก็บรวบรวม การกำหนดวัตถุประสงค์ที่ชัดเจน และการรักษาความมั่นคงปลอดภัย นอกจากนี้ การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมายที่เหมาะสม อาทิ ความยินยอม สัญญา หรือประโยชน์อันชอบด้วยกฎหมาย กฎหมายยังให้ความสำคัญกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมถึงสิทธิในการเข้าถึง แก้ไข ลบ และโอนย้ายข้อมูลของตนเอง ครอบคลุมถึงความท้าทายในยุคดิจิทัล เช่น การใช้ข้อมูลในบริบทของการจ้างงาน การทำงานจากที่บ้าน (WFH) การตลาดแบบตรง การใช้เทคโนโลยีเฝ้าระวังอย่างกล้องวงจรปิด (CCTV) และเทคโนโลยีจดจำใบหน้า (FRT) รวมถึงการประมวลผลข้อมูลบนระบบคลาวด์และปัญญาประดิษฐ์ (AI) ท้ายที่สุด เอกสารได้ชี้แจงกลไกการบังคับใช้กฎหมายซึ่งประกอบด้วยความรับผิดทางแพ่ง โทษทางปกครอง และโทษทางอาญาที่รุนแรง เพื่อสร้างความตระหนักและรับประกันการปฏิบัติตามกฎหมายอย่างเคร่งครัด

๑. หลักการพื้นฐานและกฎหมายที่เกี่ยวข้อง

๑.๑ นิยามและองค์ประกอบของ "ข้อมูลส่วนบุคคล"

ข้อมูลที่จะถือว่าเป็น "ข้อมูลส่วนบุคคล" ตามกฎหมาย จะต้องมีองค์ประกอบครบถ้วนทั้ง ๔ ประการ ดังนี้

- **ต้องเป็นข้อมูล** เป็นข้อเท็จจริงหรือสิ่งที่สามารถสื่อความหมายได้
- **ต้องเกี่ยวข้องกับบุคคล** ข้อมูลดังกล่าวต้องมีความสัมพันธ์กับบุคคลใดบุคคลหนึ่ง
- **สามารถระบุตัวบุคคลนั้นได้** ข้อมูลนั้นสามารถระบุตัวบุคคลได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม
- **บุคคลนั้นต้องเป็นบุคคลธรรมดาที่มีชีวิตอยู่** ไม่รวมถึงข้อมูลของนิติบุคคลหรือผู้ที่ถึงแก่กรรมแล้ว

ตัวอย่างของข้อมูลส่วนบุคคล

- เลขบัตรประจำตัวประชาชน
- ชื่อ - นามสกุล
- ที่อยู่, เบอร์โทรศัพท์, อีเมล
- ข้อมูลทางการเงิน
- เชื้อชาติ, ศาสนา
- ข้อมูลสุขภาพ, ประวัติอาชญากรรม
- ข้อมูลสภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลเกี่ยวกับเพศสภาพ

๑.๒ หลักการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลต้องยึดถือตามหลักการสำคัญ ๘ ประการ ดังนี้:

๑. **หลักข้อจำกัดในการเก็บรวบรวมข้อมูล** (Collection Limitation Principle) เก็บข้อมูลเท่าที่จำเป็นและโดยชอบด้วยกฎหมาย

๒. **หลักคุณภาพของข้อมูล** (Data Quality Principle) ข้อมูลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

๓. **หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ** (Purpose Specification Principle) ต้องแจ้งวัตถุประสงค์ให้ชัดเจนก่อนหรือขณะเก็บ

๔. **หลักข้อจำกัดในการนำไปใช้** (Use Limitation Principle) ใช้หรือเปิดเผยข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

๕. **หลักการรักษาความมั่นคงปลอดภัย** (Security Safeguards Principle) มีมาตรการป้องกันการเข้าถึงหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต

๖. **หลักความโปร่งใส** (Openness Principle) เปิดเผยนโยบายและแนวปฏิบัติเกี่ยวกับการจัดการข้อมูล

๗. **หลักการมีส่วนร่วมของบุคคล** (Individual Participation Principle) เจ้าของข้อมูลมีสิทธิเข้าถึง แก้ไข และคัดค้านข้อมูลของตน

๘. **หลักความรับผิดชอบ** (Accountability Principle) ผู้ควบคุมข้อมูลต้องรับผิดชอบและสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการข้างต้นได้

๑.๓ กฎหมายอื่นที่เกี่ยวข้อง

การคุ้มครองข้อมูลส่วนบุคคลมีความเชื่อมโยงกับกฎหมายฉบับอื่น ๆ ดังนี้:

- **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒** มีเจตนาเพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ความมั่นคงของรัฐ และความสงบเรียบร้อย โดยกำหนดให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยง ๓ ระดับ คือไม่ร้ายแรง ร้ายแรง และวิกฤติ
- **พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐** ส่งเสริมความโปร่งใสโดยให้ประชาชนมีสิทธิเข้าถึงข้อมูลข่าวสารของราชการตามหลัก "เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น" เพื่อให้สามารถแสดงความคิดเห็นทางการเมืองได้อย่างถูกต้อง
- **พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒** มุ่งสู่การเป็นรัฐบาลดิจิทัล โดยบูรณาการฐานข้อมูลของหน่วยงานรัฐให้เชื่อมโยงกันอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (Data Governance)
- **พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔** รองรับสถานะทางกฎหมายของข้อมูลและลายมือชื่ออิเล็กทรอนิกส์ให้มีผลเช่นเดียวกับเอกสารที่เป็นหนังสือ เพื่อส่งเสริมความน่าเชื่อถือของธุรกรรมทางอิเล็กทรอนิกส์

๒. บทบาทและความรับผิดชอบ

๒.๑ การจำแนกบทบาท

ตามกฎหมาย PDPA สามารถจำแนกบทบาทของผู้ที่เกี่ยวข้องได้ ๓ ฝ่ายหลัก ดังตัวอย่างต่อไปนี้:

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** นาย ก. ซึ่งเป็นบุคคลที่ข้อมูลของตนถูกเก็บรวบรวมใช้ หรือเปิดเผย
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** บริษัทค้าปลีก ซึ่งมีอำนาจตัดสินใจว่าจะเก็บข้อมูลของนาย ก. เพื่อวัตถุประสงค์ใด
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** บริษัทบริหารจัดการเงินเดือน ซึ่งดำเนินการเกี่ยวกับข้อมูลตามคำสั่งของบริษัทค้าปลีก เช่น การโอนเงินเดือนให้นาย ก.

๒.๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บางองค์กรจำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยเฉพาะหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด ตัวอย่างเช่น

- กรมบัญชีกลาง กระทรวงการคลัง
- กรมการกงสุล กระทรวงการต่างประเทศ
- กรมการขนส่งทางบก กระทรวงคมนาคม
- กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์
- การรถไฟแห่งประเทศไทย
- ธนาคารแห่งประเทศไทย
- มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด

ถึงแม้กฎหมายไม่ได้บังคับ องค์กรก็สามารถเลือกที่จะแต่งตั้ง DPO ได้เพื่อช่วยในการจัดการและสร้างความมั่นใจว่าได้ปฏิบัติตามกฎหมายอย่างถูกต้อง

๒.๓ ข้อยกเว้นสำหรับกิจการขนาดเล็ก

กิจการขนาดเล็กบางประเภทได้รับการยกเว้นไม่ต้องดำเนินการตามมาตรา ๓๙ บางส่วน โดยต้องมีลักษณะอย่างใดอย่างหนึ่งดังนี้

- วิสาหกิจขนาดย่อมหรือขนาดกลาง (SMEs)
- วิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- วิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- สหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- มูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร
- กิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

๓. ฐานทางกฎหมายในการประมวลผลข้อมูล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้ต่อเมื่อมีฐานทางกฎหมายรองรับ ซึ่งมีหลายฐานดังนี้

- **ฐานความยินยอม (Consent)** ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง
- **ฐานสัญญา (Contract)** จำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา
- **ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)** จำเป็นเพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล
- **ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest):** เพื่อป้องกัน ระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ

- **ฐานภารกิจของรัฐ** (Public Interest/Public Task) จำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐ
- **ฐานประโยชน์อันชอบด้วยกฎหมาย** (Legitimate Interest) จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลอื่น
- **ฐานเอกสารประวัติศาสตร์/วิจัย** (Archiving/Research) เพื่อการจัดทำเอกสารประวัติศาสตร์ วิจัย หรือสถิติ

๓.๑ ฐานการประมวลผลข้อมูลอ่อนไหว (มาตรา ๒๖)

สำหรับข้อมูลอ่อนไหว (เช่น เชื้อชาติ, ข้อมูลสุขภาพ, ข้อมูลชีวภาพ) การประมวลผลจะต้องมีฐานที่เฉพาะเจาะจงมากขึ้น เช่น

- **เพื่อวัตถุประสงค์ทางการแพทย์** เช่น เวชศาสตร์ป้องกัน, การวินิจฉัยโรค, การให้บริการด้านสุขภาพโดยผู้ประกอบวิชาชีพ
- **กิจกรรมขององค์กรไม่แสวงหากำไร** การดำเนินกิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม ที่มีวัตถุประสงค์ด้านการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน สำหรับข้อมูลของสมาชิก
- **การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ** เพื่อบรรลุวัตถุประสงค์ดังกล่าวเท่าที่จำเป็นและมีมาตรการคุ้มครองที่เหมาะสม

๓.๒ ขอบเขตการบังคับใช้และข้อยกเว้น ได้แก่

- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการยุติธรรม
- การดำเนินงานของบริษัทข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต
- การดำเนินงานของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่เกี่ยวข้อง
- การเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว (Private Use)

๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมายได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ เพื่อให้สามารถควบคุมข้อมูลของตนเองได้

๔.๑ สิทธิในการแก้ไขข้อมูล (Right to Rectification)

เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลของตนให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์ (มาตรา ๓๕) หากผู้ควบคุมข้อมูลปฏิเสธคำร้อง จะต้องบันทึกคำร้องและเหตุผลของการปฏิเสธไว้ และเจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้ (มาตรา ๓๖)

๔.๒ สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)

สิทธินี้มีวัตถุประสงค์เพื่อให้บุคคลสามารถย้ายข้อมูลส่วนบุคคลของตนจากบริการหนึ่งไปยังอีกบริการหนึ่งได้ เช่น การย้ายข้อมูลจาก Spotify ไปยัง Apple Music หรือจาก Google Photos ไปยัง Amazon Photos โดยผู้ควบคุมข้อมูลต้องจัดเตรียมข้อมูลในรูปแบบที่เครื่องมือหรืออุปกรณ์สามารถอ่านและใช้งานได้โดยอัตโนมัติ (เช่น ผ่าน API) เพื่อให้เกิดความสามารถในการทำงานร่วมกัน (interoperability) ซึ่งจะช่วยเพิ่มอำนาจให้ผู้บริโภคและสร้างโอกาสทางนวัตกรรม

๕. ประเด็นเฉพาะทางและกรณีศึกษา

๕.๑ การตลาดแบบตรง (Direct Marketing) การทำตลาดสินค้าหรือบริการโดยสื่อสารข้อมูลเพื่อเสนอขายโดยตรงต่อผู้บริโภคที่อยู่ห่างไกล และมุ่งหวังให้เกิดการตอบกลับเพื่อซื้อสินค้า

ขั้นตอนการดำเนินการ

๑. **การระบุ (Identify)** ระบุฐานทางกฎหมายและวัตถุประสงค์

๒. **การวางแผน (Plan)** วางแผนการจัดการข้อมูล

๓. **การเก็บรวบรวม (Collect)** เก็บข้อมูลอย่างโปร่งใสและเท่าที่จำเป็น

๔. **การเคารพสิทธิ (Respect)** เคารพสิทธิของเจ้าของข้อมูลในการคัดค้าน,ถอนความยินยอม

๕.๒ การจ้างงานและ Work From Home (WFH)

- **บริบทการจ้างงาน** นายจ้างสามารถประมวลผลข้อมูลของลูกจ้างเพื่อบรรลุวัตถุประสงค์ตามสัญญาจ้างแรงงาน หรืออ้างอิงฐานประโยชน์อันชอบด้วยกฎหมายเพื่อรักษาความปลอดภัยของระบบสารสนเทศ โดยไม่จำเป็นต้องขอความยินยอมแบบบังคับ
- **ความท้าทายของ WFH** แม้พนักงานจะทำงานจากนอกสถานที่ องค์กรยังคงมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อธำรงไว้ซึ่ง ความลับ (Confidentiality),ความถูกต้องครบถ้วน (Integrity), และ สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

๕.๓ การเฝ้าระวังและข้อมูลชีวภาพ

- **ข้อมูลชีวภาพ (Biometric Data)** เป็นข้อมูลอ่อนไหว เช่น ข้อมูลจำลองลายนิ้วมือ, ภาพจำลองใบหน้า, ข้อมูลจำลองม่านตา, เสียง, รูปแบบการเดิน
- **กล้องวงจรปิด (CCTV)** องค์กรต้องมีนโยบายที่ชัดเจน เช่น กำหนดระยะเวลาการเก็บรักษาข้อมูล (เช่น ๓๐ วัน) และจำกัดการเข้าถึงข้อมูลเฉพาะบุคคลที่ได้รับอนุญาต

๕.๔ การส่งข้อมูลไปต่างประเทศ การโอนข้อมูลข้ามพรมแดนต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล โดยต้องอาศัยกลไกอย่างใดอย่างหนึ่ง ดังนี้

- **มาตรฐานการคุ้มครองที่เพียงพอ (Adequacy decisions):** ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอตามที่คณะกรรมการฯ กำหนด
- **มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard):** เช่น การมีนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)
- **ข้อยกเว้นตามกฎหมาย (Derogations):** เป็นกรณีจำเป็นตามข้อยกเว้นที่กฎหมายกำหนด

๕.๕ เทคโนโลยีและความท้าทายใหม่ๆ

- **Cloud Computing** องค์กรยังคงมีความกังวลในการใช้ระบบคลาวด์ในด้านความมั่นคงปลอดภัย, การปฏิบัติตามกฎหมาย, และความเสี่ยงในการควบคุมข้อมูล กรณีศึกษาจากศาลเยอรมนีชี้ให้เห็นว่าการใช้บริการคลาวด์ที่ตั้งอยู่ในประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลเพียงพอ (เช่น สหรัฐอเมริกา) อาจถือเป็นการโอนข้อมูลไปต่างประเทศที่ไม่ชอบด้วยกฎหมาย
- **AI (Generative AI)** ในการใช้งาน Generative AI เช่น Grok ของ xAI/Twitter ผู้ใช้งาน (end user) จะอยู่ในฐานะ "ผู้ควบคุมข้อมูลส่วนบุคคล" และผู้ให้บริการ AI จะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล"
- **Cookies:** Cookie IDs บางประเภทที่สามารถใช้ระบุตัวตนของบุคคลได้ ถือเป็น "ข้อมูลส่วนบุคคล" ซึ่งสอดคล้องกับแนวทางของ GDPR และคำตัดสินของศาลยุติธรรมแห่งสหภาพยุโรป

๖. การบังคับใช้กฎหมายและบทลงโทษ กฎหมาย PDPA กำหนดมาตรการบังคับใช้ ๓ รูปแบบ คือ

ประเภทความรับผิด	รายละเอียด
ความรับผิดทางแพ่ง	เจ้าของข้อมูลสามารถฟ้องร้องเรียกค่าสินไหมทดแทนจากความเสียหายที่เกิดขึ้นจริงได้
โทษทางปกครอง	คณะกรรมการผู้เชี่ยวชาญสามารถสั่งปรับได้ โดยพิจารณาตามความร้ายแรงของการกระทำผิด
โทษทางอาญา	มีโทษจำคุกและ/หรือปรับ สำหรับการกระทำความผิดในบางมาตรา

๖.๑ โทษทางปกครอง คณะกรรมการผู้เชี่ยวชาญจะพิจารณาออกคำสั่งตามระดับความร้ายแรง

- **กรณีไม่ร้ายแรง** อาจมีคำสั่งให้ตักเตือน หรือแก้ไขให้ถูกต้องภายในเวลาที่กำหนด
- **กรณีร้ายแรง** อาจมีคำสั่งลงโทษปรับทางปกครอง หรือสั่งให้หยุดการกระทำที่ฝ่าฝืนกฎหมาย

๖.๒ โทษทางอาญา

- **มาตรา ๗๙** กำหนดโทษสำหรับผู้ควบคุมข้อมูลที่ใช้หรือเปิดเผยข้อมูลอ่อนไหว (ตามมาตรา ๒๖) โดยไม่ได้รับความยินยอม และเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย มีโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ
- **ข้อยกเว้น "การใช้เพื่อประโยชน์ส่วนตน"** มาตรา ๔(๑) ยกเว้นการบังคับใช้กฎหมายกับการเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว อย่างไรก็ตาม การนำข้อมูลผู้อื่นไปโพสต์ประจานในโซเชียลมีเดีย เช่น โพสต์ภาพใบสำคัญการหย่า หรือสำเนาบัตรประชาชนของลูกหนี้ ไม่ถือเป็นการใช้เพื่อประโยชน์ส่วนตน และอาจมีความผิดทางอาญาได้
- **ความรับผิดของนิติบุคคลและกรรมการ** หากการกระทำผิดของนิติบุคคลเกิดจากการสั่งการหรือการละเว้นการสั่งการของกรรมการหรือผู้จัดการ บุคคลดังกล่าวต้องรับโทษทางอาญาด้วย (มาตรา ๘๑)

๗. หน่วยงานกำกับดูแล

๗.๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) เป็นองค์กรหลักในการกำกับดูแล ประกอบด้วย

- ประธานกรรมการ
- รองประธานกรรมการ (ปลัดกระทรวงดิจิทัลฯ)
- กรรมการโดยตำแหน่ง ๕ คน (ปลัดสำนักนายกฯ, เลขาธิการกฤษฎีกา, เลขาธิการ สคบ., อธิบดีกรมคุ้มครองสิทธิฯ, อัยการสูงสุด)
- กรรมการผู้ทรงคุณวุฒิ ๙ คน
- เลขาธิการ (เป็นกรรมการและเลขานุการ)

อำนาจหน้าที่หลัก จัดทำแผนแม่บทด้านการคุ้มครองข้อมูลส่วนบุคคล, ส่งเสริมและสนับสนุนการดำเนินงานของภาครัฐและเอกชน

๗.๒ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เป็นหน่วยงานธุรการของ กคส. มีอำนาจหน้าที่สำคัญ ได้แก่

- จัดทำร่างแผนแม่บทฯ เสนอต่อ กคส.
- ส่งเสริมและสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวข้อง
- เป็นศูนย์กลางในการให้บริการทางวิชาการและให้ความรู้แก่ประชาชน
- กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้เกี่ยวข้อง
- ทำความตกลงและร่วมมือกับองค์กรทั้งในและต่างประเทศ
- ติดตามและประเมินผลการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

๓. ประโยชน์ที่ได้รับจากการฝึกอบรม

๓.๑ ประโยชน์ต่อตนเอง

๑. ความรู้ความเข้าใจที่ถูกต้อง ทำให้ทราบถึงสิทธิและหน้าที่ตามกฎหมาย ทั้งในฐานะ "เจ้าของข้อมูลส่วนบุคคล" ที่ได้รับการคุ้มครองสิทธิ (เช่น สิทธิขอเข้าถึง, ขอให้ลบ, หรือคัดค้าน) และในฐานะผู้ปฏิบัติงานที่ต้องจัดการข้อมูลของผู้อื่น

๒. ลดความเสี่ยงในการกระทำผิด: ช่วยให้ทราบขอบเขตการปฏิบัติงานที่ถูกต้อง ป้องกันการละเมิดข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์ ซึ่งมีบทลงโทษทั้งทางแพ่ง อาญา และปกครอง

๓. พัฒนาทักษะวิชาชีพ: เพิ่มพูนทักษะด้านการบริหารจัดการข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นทักษะที่จำเป็นในยุคดิจิทัล

๓.๒ ประโยชน์ต่อหน่วยงาน

๑. การปฏิบัติตามกฎหมาย (Compliance) : ช่วยให้องค์กรดำเนินงานสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ลดความเสี่ยงในการถูกฟ้องร้องหรือถูกลงโทษปรับทางปกครองที่มีอัตราสูง

๒. สร้างความเชื่อมั่น (Trust) : การมีมาตรการคุ้มครองข้อมูลที่ได้มาตรฐาน ช่วยสร้างภาพลักษณ์ที่ดีและความน่าเชื่อถือให้กับองค์กรในสายตาของบุคลากร และผู้รับบริการ

๓.ยกระดับความมั่นคงปลอดภัย : การปฏิบัติตามหลักการ CIA (Confidentiality, Integrity, Availability) ช่วยป้องกันภัยคุกคามทางไซเบอร์และเหตุละเมิดข้อมูลรั่วไหล

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการฝึกอบรมครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน

๔.๑ การตรวจสอบและจัดทำบันทึกรายการกิจกรรม (Data Inventory & RoPA)

- เริ่มสำรวจกระบวนการทำงานว่ามีการเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง และจัดทำ บันทึกรายการกิจกรรมการประมวลผล (RoPA) ตามที่กฎหมายกำหนด (มาตรา ๓๙) เพื่อให้สามารถตรวจสอบเส้นทางการไหลของข้อมูลและวัตถุประสงค์การใช้งานได้ชัดเจน

๔.๒ การกำหนดฐานทางกฎหมายและการแจ้งความเป็นส่วนตัว (Lawful Basis & Privacy Notice)

- จัดทำหรือปรับปรุง **ประกาศความเป็นส่วนตัว (Privacy Notice)** เพื่อแจ้งวัตถุประสงค์และรายละเอียดให้เจ้าของข้อมูลทราบอย่างโปร่งใส ก่อนหรือขณะเก็บรวบรวมข้อมูล

๔.๓ การยกระดับมาตรการรักษาความมั่นคงปลอดภัย (Security Measures)

- นำความรู้เรื่องมาตรการเชิงองค์กรและเชิงเทคนิคมาปรับใช้ เช่น การกำหนดสิทธิการเข้าถึงข้อมูล (Access Control) ให้เฉพาะผู้ที่เกี่ยวข้อง, การเข้ารหัสข้อมูล (Encryption), และการทำข้อมูลให้เป็นนิรนาม (Anonymization) เพื่อลดความเสี่ยง

๔.๔ การบริหารจัดการสิทธิของเจ้าของข้อมูล

- วางระบบหรือขั้นตอนการปฏิบัติงาน (SOP) เพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล เช่น ช่องทางรับคำร้องขอเข้าถึงข้อมูล, การลบทำลายข้อมูลเมื่อหมดความจำเป็น หรือการคัดค้านการประมวลผล เพื่อให้สามารถตอบสนองได้ตามกรอบเวลาที่กฎหมายกำหนด

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

๕.๑ ความซับซ้อนในการตีความและการปฏิบัติ

- การจำแนกบทบาทระหว่าง "ผู้ควบคุมข้อมูล" และ "ผู้ประมวลผลข้อมูล" ในบางกิจกรรมอาจมีความก้ำกึ่งหรือไม่ชัดเจน ซึ่งส่งผลต่อขอบเขตความรับผิดชอบ

- การพิจารณา "ฐานประโยชน์โดยชอบด้วยกฎหมาย" (Legitimate Interest) ต้องใช้ความระมัดระวังในการชั่งน้ำหนักระหว่างประโยชน์ขององค์กรกับสิทธิของเจ้าของข้อมูล ซึ่งอาจเกิดข้อโต้แย้งได้ง่าย

๕.๒ ภาระงานด้านเอกสารและเทคนิค

- การจัดทำบันทึกรายการกิจกรรม (RoPA) ให้เป็นปัจจุบันตลอดเวลา และการจัดการคำขอใช้สิทธิ (เช่น การขอโอนย้ายข้อมูล หรือ Data Portability) ต้องอาศัยระบบเทคโนโลยีสารสนเทศที่รองรับ ซึ่งหากระบบเดิม (Legacy System) ไม่เอื้ออำนวย อาจต้องใช้งบประมาณและเวลาในการพัฒนา

- การลบข้อมูล (Right to be Erasure) อาจทำได้ยากในทางปฏิบัติ หากข้อมูลถูกเผยแพร่สู่สาธารณะหรือส่งต่อไปยังบุคคลที่สามแล้ว

๕.๓ ความตระหนักรู้ของบุคลากร

- แม้จะมีมาตรการที่ดี แต่หากบุคลากรขาดความตระหนักรู้ (Privacy Awareness) เช่น การเผลอส่งข้อมูลผิด หรือการตั้งรหัสผ่านที่ไม่ปลอดภัย ก็ยังเป็นจุดอ่อนที่ทำให้เกิดเหตุละเมิดข้อมูลได้

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

๖.๑ การกำหนดนโยบายที่ชัดเจน (Policy & Governance)

- ขอให้ผู้บริหารประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ที่ชัดเจน เพื่อใช้เป็นแนวทางปฏิบัติหลักขององค์กร และสนับสนุนให้เกิดวัฒนธรรมการเคารพสิทธิข้อมูลส่วนบุคคล

๖.๒ การสนับสนุนด้านทรัพยากร (Resources)

- **งบประมาณ** สำหรับจัดหาเครื่องมือด้านความปลอดภัยทางเทคโนโลยี (เช่น Firewall, ระบบ Encryption) และระบบบริหารจัดการข้อมูล

- **บุคลากร** สนับสนุนการแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือคณะทำงานเฉพาะกิจเพื่อรับผิดชอบงานด้านนี้โดยตรง หากองค์กรเข้าข่ายตามเงื่อนไขกฎหมาย

๖.๓ การฝึกอบรมและสื่อสาร (Training & Communication)

- สนับสนุนให้มีการจัดฝึกอบรมบุคลากรทุกระดับอย่างต่อเนื่อง เพื่อสร้างความเข้าใจและลดความเสี่ยงจากความผิดพลาดของคน (Human Error) ในการปฏิบัติงาน

๖.๔ การตัดสินใจในกรณีที่มีความเสี่ยงสูง

- สนับสนุนการตัดสินใจในการทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) สำหรับโครงการใหม่ๆ ที่มีความเสี่ยงสูง เพื่อให้มั่นใจว่าองค์กรได้ปิดความเสี่ยงก่อนเริ่มดำเนินการ

จึงเรียนมาเพื่อโปรดทราบ

(ลงชื่อ) .....

(นายคำรณ จันทร์ต้น)

ผู้เข้ารับการฝึกอบรม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณคำรณ จันทร์ต้น

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 22 พฤศจิกายน 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680302500

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณคำรณ จันทร์ต้น

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 22 พฤศจิกายน 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680302500

แบบรายงานผลการเข้ารับการฝึกอบรม/สัมมนา

ด้วยข้าพเจ้า นางสาวศจิษฐา รีรักษ์ ตำแหน่ง นักวิชาการสาธารณสุขชำนาญการ โรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังทอง สังกัด กองสาธารณสุขและสิ่งแวดล้อม ได้เข้าร่วมโครงการอบรมเชิงปฏิบัติการหลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง (e-learning) ในวันที่ ๒๑ พฤศจิกายน พ.ศ.๒๕๖๘ นั้น

บัดนี้ ข้าพเจ้าได้เข้ารับการฝึกอบรมหลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการฝึกอบรมให้ทราบ ดังนี้

๑. การฝึกอบรมดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ สร้างความรู้ความเข้าใจในการปฏิบัติหน้าที่ วัตถุประสงค์หลักของการฝึกอบรมคือเพื่อให้กลุ่มเป้าหมายมีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับ "การปฏิบัติหน้าที่" ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยครอบคลุมบทบาทของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller), ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor), เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO), รวมถึงลูกจ้างและผู้รับจ้างที่เกี่ยวข้อง

๒. ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้ และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่หน่วยงานรัฐ ภาคเอกชน และประชาชนทั่วไป เพื่อให้สามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. เนื้อหาและหัวข้อวิชาของหลักสูตรการฝึกอบรม มีดังนี้

บทที่	เนื้อหาหลักสูตร
๑	ความรู้เบื้องต้น และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
๒	ข้อมูลส่วนบุคคล
๓	ผู้ควบคุมคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
๔	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๕	สิทธิของเจ้าของข้อมูลส่วนบุคคล
๖	หน้าที่ในการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๗	การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
๘	แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
๙	การรักษาความมั่นคงปลอดภัยขอของข้อมูลส่วนบุคคล
๑๐	ความรับผิดชอบ
๑๑	การกำกับดูแลและบังคับใช้กฎหมาย

สรุปหลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง และผู้รับจ้าง

เอกสารสรุปฉบับนี้สังเคราะห์เนื้อหาหลักจากหลักสูตรการปฏิบัติหน้าที่ของผู้เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยมุ่งเน้นกรอบกฎหมายและแนวปฏิบัติที่สำคัญภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ประเด็นสำคัญคือการกำหนดนิยามของ "ข้อมูลส่วนบุคคล" และการจำแนกบทบาทของผู้มีส่วนได้เสียหลัก ได้แก่ เจ้าของข้อมูล (Data Subject) ผู้ควบคุมข้อมูล (Data Controller) ผู้ประมวลผลข้อมูล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งแต่ละฝ่ายมีหน้าที่และความรับผิดชอบที่แตกต่างกัน

หัวใจสำคัญของการปฏิบัติตามกฎหมายคือการประมวลผลข้อมูล (การเก็บรวบรวม ใช้ หรือเปิดเผย) ต้องเป็นไปตามหลักการพื้นฐาน ๘ ประการ เช่น การจำกัดการเก็บรวบรวม การกำหนดวัตถุประสงค์ที่ชัดเจน และการรักษาความมั่นคงปลอดภัย นอกจากนี้ การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมายที่เหมาะสม อาทิ ความยินยอม สัญญา หรือประโยชน์อันชอบด้วยกฎหมาย กฎหมายยังให้ความสำคัญกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมถึงสิทธิในการเข้าถึง แก้ไข ลบ และโอนย้ายข้อมูลของตนเอง ครอบคลุมถึงความท้าทายในยุคดิจิทัล เช่น การใช้ข้อมูลในบริบทของการจ้างงาน การทำงานจากที่บ้าน (WFH) การตลาดแบบตรง การใช้เทคโนโลยีเฝ้าระวังอย่างกล้องวงจรปิด (CCTV) และเทคโนโลยีจดจำใบหน้า (FRT) รวมถึงการประมวลผลข้อมูลบนระบบคลาวด์และปัญญาประดิษฐ์ (AI) ท้ายที่สุด เอกสารได้ชี้แจงกลไกการบังคับใช้กฎหมายซึ่งประกอบด้วยความรับผิดทางแพ่ง โทษทางปกครอง และโทษทางอาญาที่รุนแรง เพื่อสร้างความตระหนักและรับประกันการปฏิบัติตามกฎหมายอย่างเคร่งครัด

๑. หลักการพื้นฐานและกฎหมายที่เกี่ยวข้อง

๑.๑ นิยามและองค์ประกอบของ "ข้อมูลส่วนบุคคล"

ข้อมูลที่จะถือว่าเป็น "ข้อมูลส่วนบุคคล" ตามกฎหมาย จะต้องมีองค์ประกอบครบถ้วนทั้ง ๔ ประการ ดังนี้

- **ต้องเป็นข้อมูล** เป็นข้อเท็จจริงหรือสิ่งที่สามารถสื่อความหมายได้
- **ต้องเกี่ยวข้องกับบุคคล** ข้อมูลดังกล่าวต้องมีความสัมพันธ์กับบุคคลใดบุคคลหนึ่ง
- **สามารถระบุตัวบุคคลนั้นได้** ข้อมูลนั้นสามารถระบุตัวบุคคลได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม
- **บุคคลนั้นต้องเป็นบุคคลธรรมดาที่มีชีวิตอยู่** ไม่รวมถึงข้อมูลของนิติบุคคลหรือผู้ที่ถึงแก่กรรมแล้ว

ตัวอย่างของข้อมูลส่วนบุคคล

- เลขบัตรประจำตัวประชาชน
- ชื่อ - นามสกุล
- ที่อยู่, เบอร์โทรศัพท์, อีเมล
- ข้อมูลทางการเงิน
- เชื้อชาติ, ศาสนา
- ข้อมูลสุขภาพ, ประวัติอาชญากรรม
- ข้อมูลสภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลเกี่ยวกับเพศสภาพ

๑.๒ หลักการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลต้องยึดถือตามหลักการสำคัญ ๘ ประการ ดังนี้:

๑. **หลักข้อจำกัดในการเก็บรวบรวมข้อมูล** (Collection Limitation Principle) เก็บข้อมูลเท่าที่จำเป็นและโดยชอบด้วยกฎหมาย

๒. **หลักคุณภาพของข้อมูล** (Data Quality Principle) ข้อมูลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

๓. **หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ** (Purpose Specification Principle) ต้องแจ้งวัตถุประสงค์ให้ชัดเจนก่อนหรือขณะเก็บ

๔. **หลักข้อจำกัดในการนำไปใช้** (Use Limitation Principle) ใช้หรือเปิดเผยข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

๕. **หลักการรักษาความมั่นคงปลอดภัย** (Security Safeguards Principle) มีมาตรการป้องกันการเข้าถึงหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต

๖. **หลักความโปร่งใส** (Openness Principle) เปิดเผยนโยบายและแนวปฏิบัติเกี่ยวกับการจัดการข้อมูล

๗. **หลักการมีส่วนร่วมของบุคคล** (Individual Participation Principle) เจ้าของข้อมูลมีสิทธิเข้าถึง แก้ไข และคัดค้านข้อมูลของตน

๘. **หลักความรับผิดชอบ** (Accountability Principle) ผู้ควบคุมข้อมูลต้องรับผิดชอบและสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการข้างต้นได้

๑.๓ กฎหมายอื่นที่เกี่ยวข้อง

การคุ้มครองข้อมูลส่วนบุคคลมีความเชื่อมโยงกับกฎหมายฉบับอื่น ๆ ดังนี้:

- **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒** มีเจตนาเพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ความมั่นคงของรัฐ และความสงบเรียบร้อย โดยกำหนดให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยง ๓ ระดับ คือไม่ร้ายแรง ร้ายแรง และวิกฤติ
- **พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐** ส่งเสริมความโปร่งใสโดยให้ประชาชนมีสิทธิเข้าถึงข้อมูลข่าวสารของราชการตามหลัก "เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น" เพื่อให้สามารถแสดงความคิดเห็นทางการเมืองได้อย่างถูกต้อง
- **พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒** มุ่งสู่การเป็นรัฐบาลดิจิทัล โดยบูรณาการฐานข้อมูลของหน่วยงานรัฐให้เชื่อมโยงกันอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (Data Governance)
- **พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔** รองรับสถานะทางกฎหมายของข้อมูลและลายมือชื่ออิเล็กทรอนิกส์ให้มีผลเช่นเดียวกับเอกสารที่เป็นหนังสือ เพื่อส่งเสริมความน่าเชื่อถือของธุรกรรมทางอิเล็กทรอนิกส์

๒. บทบาทและความรับผิดชอบ

๒.๑ การจำแนกบทบาท

ตามกฎหมาย PDPA สามารถจำแนกบทบาทของผู้ที่เกี่ยวข้องได้ ๓ ฝ่ายหลัก ดังตัวอย่างต่อไปนี้:

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** นาย ก. ซึ่งเป็นบุคคลที่ข้อมูลของตนถูกเก็บรวบรวมใช้ หรือเปิดเผย
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** บริษัทค้าปลีก ซึ่งมีอำนาจตัดสินใจว่าจะเก็บข้อมูลของนาย ก. เพื่อวัตถุประสงค์ใด
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** บริษัทบริหารจัดการเงินเดือน ซึ่งดำเนินการเกี่ยวกับข้อมูลตามคำสั่งของบริษัทค้าปลีก เช่น การโอนเงินเดือนให้นาย ก.

๒.๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บางองค์กรจำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยเฉพาะหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด ตัวอย่างเช่น

- กรมบัญชีกลาง กระทรวงการคลัง
- กรมการกงสุล กระทรวงการต่างประเทศ
- กรมการขนส่งทางบก กระทรวงคมนาคม
- กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์
- การรถไฟแห่งประเทศไทย
- ธนาคารแห่งประเทศไทย
- มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด

ถึงแม้กฎหมายไม่ได้บังคับ องค์กรก็สามารถเลือกที่จะแต่งตั้ง DPO ได้เพื่อช่วยในการจัดการและสร้างความมั่นใจว่าได้ปฏิบัติตามกฎหมายอย่างถูกต้อง

๒.๓ ข้อยกเว้นสำหรับกิจการขนาดเล็ก

กิจการขนาดเล็กบางประเภทได้รับการยกเว้นไม่ต้องดำเนินการตามมาตรา ๓๙ บางส่วน โดยต้องมีลักษณะอย่างใดอย่างหนึ่งดังนี้

- วิสาหกิจขนาดย่อมหรือขนาดกลาง (SMEs)
- วิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- วิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- สหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- มูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร
- กิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

๓. ฐานทางกฎหมายในการประมวลผลข้อมูล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้ต่อเมื่อมีฐานทางกฎหมายรองรับ ซึ่งมีหลายฐานดังนี้

- **ฐานความยินยอม (Consent)** ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง
- **ฐานสัญญา (Contract)** จำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา
- **ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)** จำเป็นเพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล
- **ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest):** เพื่อป้องกัน ระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ

- **ฐานภารกิจของรัฐ** (Public Interest/Public Task) จำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐ
- **ฐานประโยชน์อันชอบด้วยกฎหมาย** (Legitimate Interest) จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลอื่น
- **ฐานเอกสารประวัติศาสตร์/วิจัย** (Archiving/Research) เพื่อการจัดทำเอกสารประวัติศาสตร์ วิจัย หรือสถิติ

๓.๑ ฐานการประมวลผลข้อมูลอ่อนไหว (มาตรา ๒๖)

สำหรับข้อมูลอ่อนไหว (เช่น เชื้อชาติ, ข้อมูลสุขภาพ, ข้อมูลชีวภาพ) การประมวลผลจะต้องมีฐานที่เฉพาะเจาะจงมากขึ้น เช่น

- **เพื่อวัตถุประสงค์ทางการแพทย์** เช่น เวชศาสตร์ป้องกัน, การวินิจฉัยโรค, การให้บริการด้านสุขภาพโดยผู้ประกอบวิชาชีพ
- **กิจกรรมขององค์กรไม่แสวงหากำไร** การดำเนินกิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม ที่มีวัตถุประสงค์ด้านการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน สำหรับข้อมูลของสมาชิก
- **การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ** เพื่อบรรลุวัตถุประสงค์ดังกล่าวเท่าที่จำเป็นและมีมาตรการคุ้มครองที่เหมาะสม

๓.๒ ขอบเขตการบังคับใช้และข้อยกเว้น ได้แก่

- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการยุติธรรม
- การดำเนินงานของบริษัทข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต
- การดำเนินงานของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่เกี่ยวข้อง
- การเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว (Private Use)

๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมายได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ เพื่อให้สามารถควบคุมข้อมูลของตนเองได้

๔.๑ สิทธิในการแก้ไขข้อมูล (Right to Rectification)

เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลของตนให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์ (มาตรา ๓๕) หากผู้ควบคุมข้อมูลปฏิเสธคำร้อง จะต้องบันทึกคำร้องและเหตุผลของการปฏิเสธไว้ และเจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้ (มาตรา ๓๖)

๔.๒ สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)

สิทธินี้มีวัตถุประสงค์เพื่อให้บุคคลสามารถย้ายข้อมูลส่วนบุคคลของตนจากบริการหนึ่งไปยังอีกบริการหนึ่งได้ เช่น การย้ายข้อมูลจาก Spotify ไปยัง Apple Music หรือจาก Google Photos ไปยัง Amazon Photos โดยผู้ควบคุมข้อมูลต้องจัดเตรียมข้อมูลในรูปแบบที่เครื่องมือหรืออุปกรณ์สามารถอ่านและใช้งานได้โดยอัตโนมัติ (เช่น ผ่าน API) เพื่อให้เกิดความสามารถในการทำงานร่วมกัน (interoperability) ซึ่งจะช่วยเพิ่มอำนาจให้ผู้บริโภคและสร้างโอกาสทางนวัตกรรม

๕. ประเด็นเฉพาะทางและกรณีศึกษา

๕.๑ การตลาดแบบตรง (Direct Marketing) การทำตลาดสินค้าหรือบริการโดยสื่อสารข้อมูลเพื่อเสนอขายโดยตรงต่อผู้บริโภคที่อยู่ห่างไกล และมุ่งหวังให้เกิดการตอบกลับเพื่อซื้อสินค้า

ขั้นตอนการดำเนินการ

๑. **การระบุ (Identify)** ระบุฐานทางกฎหมายและวัตถุประสงค์

๒. **การวางแผน (Plan)** วางแผนการจัดการข้อมูล

๓. **การเก็บรวบรวม (Collect)** เก็บข้อมูลอย่างโปร่งใสและเท่าที่จำเป็น

๔. **การเคารพสิทธิ (Respect)** เคารพสิทธิของเจ้าของข้อมูลในการคัดค้าน,ถอนความยินยอม

๕.๒ การจ้างงานและ Work From Home (WFH)

- **บริบทการจ้างงาน** นายจ้างสามารถประมวลผลข้อมูลของลูกจ้างเพื่อบรรลุวัตถุประสงค์ตามสัญญาจ้างแรงงาน หรืออ้างอิงฐานประโยชน์อันชอบด้วยกฎหมายเพื่อรักษาความปลอดภัยของระบบสารสนเทศ โดยไม่จำเป็นต้องขอความยินยอมแบบบังคับ
- **ความท้าทายของ WFH** แม้พนักงานจะทำงานจากนอกสถานที่ องค์กรยังคงมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อธำรงไว้ซึ่ง ความลับ (Confidentiality),ความถูกต้องครบถ้วน (Integrity), และ สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

๕.๓ การเฝ้าระวังและข้อมูลชีวภาพ

- **ข้อมูลชีวภาพ (Biometric Data)** เป็นข้อมูลอ่อนไหว เช่น ข้อมูลจำลองลายนิ้วมือ, ภาพจำลองใบหน้า, ข้อมูลจำลองม่านตา, เสียง, รูปแบบการเดิน
- **กล้องวงจรปิด (CCTV)** องค์กรต้องมีนโยบายที่ชัดเจน เช่น กำหนดระยะเวลาการเก็บรักษาข้อมูล (เช่น ๓๐ วัน) และจำกัดการเข้าถึงข้อมูลเฉพาะบุคคลที่ได้รับอนุญาต

๕.๔ การส่งข้อมูลไปต่างประเทศ การโอนข้อมูลข้ามพรมแดนต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล โดยต้องอาศัยกลไกอย่างใดอย่างหนึ่ง ดังนี้

- **มาตรฐานการคุ้มครองที่เพียงพอ (Adequacy decisions):** ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอตามที่คณะกรรมการฯ กำหนด
- **มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard):** เช่น การมีนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)
- **ข้อยกเว้นตามกฎหมาย (Derogations):** เป็นกรณีจำเป็นตามข้อยกเว้นที่กฎหมายกำหนด

๕.๕ เทคโนโลยีและความท้าทายใหม่ๆ

- **Cloud Computing** องค์กรยังคงมีความกังวลในการใช้ระบบคลาวด์ในด้านความมั่นคงปลอดภัย, การปฏิบัติตามกฎหมาย, และความเสี่ยงในการควบคุมข้อมูล กรณีศึกษาจากศาลเยอรมนีชี้ให้เห็นว่าการใช้บริการคลาวด์ที่ตั้งอยู่ในประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลเพียงพอ (เช่น สหรัฐอเมริกา) อาจถือเป็นการโอนข้อมูลไปต่างประเทศที่ไม่ชอบด้วยกฎหมาย
- **AI (Generative AI)** ในการใช้งาน Generative AI เช่น Grok ของ xAI/Twitter ผู้ใช้งาน (end user) จะอยู่ในฐานะ "ผู้ควบคุมข้อมูลส่วนบุคคล" และผู้ให้บริการ AI จะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล"
- **Cookies:** Cookie IDs บางประเภทที่สามารถใช้ระบุตัวตนของบุคคลได้ ถือเป็น "ข้อมูลส่วนบุคคล" ซึ่งสอดคล้องกับแนวทางของ GDPR และคำตัดสินของศาลยุติธรรมแห่งสหภาพยุโรป

๖. **การบังคับใช้กฎหมายและบทลงโทษ** กฎหมาย PDPA กำหนดมาตรการบังคับใช้ ๓ รูปแบบ คือ

ประเภทความรับผิด	รายละเอียด
ความรับผิดทางแพ่ง	เจ้าของข้อมูลสามารถฟ้องร้องเรียกค่าสินไหมทดแทนจากความเสียหายที่เกิดขึ้นจริงได้
โทษทางปกครอง	คณะกรรมการผู้เชี่ยวชาญสามารถสั่งปรับได้ โดยพิจารณาตามความร้ายแรงของการกระทำผิด
โทษทางอาญา	มีโทษจำคุกและ/หรือปรับ สำหรับการกระทำความผิดในบางมาตรา

๖.๑ โทษทางปกครอง คณะกรรมการผู้เชี่ยวชาญจะพิจารณาออกคำสั่งตามระดับความร้ายแรง

- **กรณีไม่ร้ายแรง** อาจมีคำสั่งให้ตักเตือน หรือแก้ไขให้ถูกต้องภายในเวลาที่กำหนด
- **กรณีร้ายแรง** อาจมีคำสั่งลงโทษปรับทางปกครอง หรือสั่งให้หยุดการกระทำที่ฝ่าฝืนกฎหมาย

๖.๒ โทษทางอาญา

- **มาตรา ๗๙** กำหนดโทษสำหรับผู้ควบคุมข้อมูลที่ใช้หรือเปิดเผยข้อมูลอ่อนไหว (ตามมาตรา ๒๖) โดยไม่ได้รับความยินยอม และเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย มีโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ
- **ข้อยกเว้น "การใช้เพื่อประโยชน์ส่วนตน"** มาตรา ๔(๑) ยกเว้นการบังคับใช้กฎหมายกับการเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว อย่างไรก็ตาม การนำข้อมูลผู้อื่นไปโพสต์ประจานในโซเชียลมีเดีย เช่น โพสต์ภาพใบสำคัญการหย่า หรือสำเนาบัตรประชาชนของลูกหนี้ ไม่ถือเป็นการใช้เพื่อประโยชน์ส่วนตน และอาจมีความผิดทางอาญาได้
- **ความรับผิดของนิติบุคคลและกรรมการ** หากการกระทำผิดของนิติบุคคลเกิดจากการสั่งการหรือการละเว้นการสั่งการของกรรมการหรือผู้จัดการ บุคคลดังกล่าวต้องรับโทษทางอาญาด้วย (มาตรา ๘๑)

๗. หน่วยงานกำกับดูแล

๗.๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) เป็นองค์กรหลักในการกำกับดูแล ประกอบด้วย

- ประธานกรรมการ
- รองประธานกรรมการ (ปลัดกระทรวงดิจิทัลฯ)
- กรรมการโดยตำแหน่ง ๕ คน (ปลัดสำนักนายกฯ, เลขาธิการกฤษฎีกา, เลขาธิการ สคบ., อธิบดีกรมคุ้มครองสิทธิฯ, อัยการสูงสุด)
- กรรมการผู้ทรงคุณวุฒิ ๙ คน
- เลขาธิการ (เป็นกรรมการและเลขานุการ)

อำนาจหน้าที่หลัก จัดทำแผนแม่บทด้านการคุ้มครองข้อมูลส่วนบุคคล, ส่งเสริมและสนับสนุนการดำเนินงานของภาครัฐและเอกชน

๗.๒ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เป็นหน่วยงานธุรการของ กคส. มีอำนาจหน้าที่สำคัญ ได้แก่

- จัดทำร่างแผนแม่บทฯ เสนอต่อ กคส.
- ส่งเสริมและสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวข้อง
- เป็นศูนย์กลางในการให้บริการทางวิชาการและให้ความรู้แก่ประชาชน
- กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้เกี่ยวข้อง
- ทำความตกลงและร่วมมือกับองค์กรทั้งในและต่างประเทศ
- ติดตามและประเมินผลการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

๓. ประโยชน์ที่ได้รับจากการฝึกอบรม

๓.๑ ประโยชน์ต่อตนเอง

๑. ความรู้ความเข้าใจที่ถูกต้อง ทำให้ทราบถึงสิทธิและหน้าที่ตามกฎหมาย ทั้งในฐานะ "เจ้าของข้อมูลส่วนบุคคล" ที่ได้รับการคุ้มครองสิทธิ (เช่น สิทธิขอเข้าถึง, ขอให้ลบ, หรือคัดค้าน) และในฐานะผู้ปฏิบัติงานที่ต้องจัดการข้อมูลของผู้อื่น

๒. ลดความเสี่ยงในการกระทำผิด: ช่วยให้ทราบขอบเขตการปฏิบัติงานที่ถูกต้อง ป้องกันการละเมิดข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์ ซึ่งมีบทลงโทษทั้งทางแพ่ง อาญา และปกครอง

๓. พัฒนาทักษะวิชาชีพ: เพิ่มพูนทักษะด้านการบริหารจัดการข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นทักษะที่จำเป็นในยุคดิจิทัล

๓.๒ ประโยชน์ต่อหน่วยงาน

๑. การปฏิบัติตามกฎหมาย (Compliance) : ช่วยให้องค์กรดำเนินงานสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ลดความเสี่ยงในการถูกฟ้องร้องหรือถูกลงโทษปรับทางปกครองที่มีอัตราสูง

๒. สร้างความเชื่อมั่น (Trust) : การมีมาตรการคุ้มครองข้อมูลที่ได้มาตรฐาน ช่วยสร้างภาพลักษณ์ที่ดีและความน่าเชื่อถือให้กับองค์กรในสายตาของบุคลากร และผู้รับบริการ

๓.ยกระดับความมั่นคงปลอดภัย : การปฏิบัติตามหลักการ CIA (Confidentiality, Integrity, Availability) ช่วยป้องกันภัยคุกคามทางไซเบอร์และเหตุละเมิดข้อมูลรั่วไหล

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการฝึกอบรมครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน

๔.๑ การตรวจสอบและจัดทำบันทึกรายการกิจกรรม (Data Inventory & RoPA)

- เริ่มสำรวจกระบวนการทำงานว่ามีการเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง และจัดทำ บันทึกรายการกิจกรรมการประมวลผล (RoPA) ตามที่กฎหมายกำหนด (มาตรา ๓๙) เพื่อให้สามารถตรวจสอบเส้นทางการไหลของข้อมูลและวัตถุประสงค์การใช้งานได้ชัดเจน

๔.๒ การกำหนดฐานทางกฎหมายและการแจ้งความเป็นส่วนตัว (Lawful Basis & Privacy Notice)

- จัดทำหรือปรับปรุง **ประกาศความเป็นส่วนตัว (Privacy Notice)** เพื่อแจ้งวัตถุประสงค์และรายละเอียดให้เจ้าของข้อมูลทราบอย่างโปร่งใส ก่อนหรือขณะเก็บรวบรวมข้อมูล

๔.๓ การยกระดับมาตรการรักษาความมั่นคงปลอดภัย (Security Measures)

- นำความรู้เรื่องมาตรการเชิงองค์กรและเชิงเทคนิคมาปรับใช้ เช่น การกำหนดสิทธิการเข้าถึงข้อมูล (Access Control) ให้เฉพาะผู้ที่เกี่ยวข้อง, การเข้ารหัสข้อมูล (Encryption), และการทำข้อมูลให้เป็นนิรนาม (Anonymization) เพื่อลดความเสี่ยง

๔.๔ การบริหารจัดการสิทธิของเจ้าของข้อมูล

- วางระบบหรือขั้นตอนการปฏิบัติงาน (SOP) เพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล เช่น ช่องทางรับคำร้องขอเข้าถึงข้อมูล, การลบทำลายข้อมูลเมื่อหมดความจำเป็น หรือการคัดค้านการประมวลผล เพื่อให้สามารถตอบสนองได้ตามกรอบเวลาที่กฎหมายกำหนด

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

๕.๑ ความซับซ้อนในการตีความและการปฏิบัติ

- การจำแนกบทบาทระหว่าง "ผู้ควบคุมข้อมูล" และ "ผู้ประมวลผลข้อมูล" ในบางกิจกรรมอาจมีความก้ำกึ่งหรือไม่ชัดเจน ซึ่งส่งผลต่อขอบเขตความรับผิดชอบ

- การพิจารณา "ฐานประโยชน์โดยชอบด้วยกฎหมาย" (Legitimate Interest) ต้องใช้ความระมัดระวังในการชั่งน้ำหนักระหว่างประโยชน์ขององค์กรกับสิทธิของเจ้าของข้อมูล ซึ่งอาจเกิดข้อโต้แย้งได้ง่าย

๕.๒ ภาระงานด้านเอกสารและเทคนิค

- การจัดทำบันทึกรายการกิจกรรม (RoPA) ให้เป็นปัจจุบันตลอดเวลา และการจัดการคำขอใช้สิทธิ (เช่น การขอโอนย้ายข้อมูล หรือ Data Portability) ต้องอาศัยระบบเทคโนโลยีสารสนเทศที่รองรับ ซึ่งหากระบบเดิม (Legacy System) ไม่เอื้ออำนวย อาจต้องใช้งบประมาณและเวลาในการพัฒนา

- การลบข้อมูล (Right to be Erasure) อาจทำได้ยากในทางปฏิบัติ หากข้อมูลถูกเผยแพร่สู่สาธารณะหรือส่งต่อไปยังบุคคลที่สามแล้ว

๕.๓ ความตระหนักรู้ของบุคลากร

- แม้จะมีมาตรการที่ดี แต่หากบุคลากรขาดความตระหนักรู้ (Privacy Awareness) เช่น การเผลอส่งข้อมูลผิด หรือการตั้งรหัสผ่านที่ไม่ปลอดภัย ก็ยังเป็นจุดอ่อนที่ทำให้เกิดเหตุละเมิดข้อมูลได้

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล

๖.๑ การกำหนดนโยบายที่ชัดเจน (Policy & Governance)

- ขอให้ผู้บริหารประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ที่ชัดเจน เพื่อใช้เป็นแนวทางปฏิบัติหลักขององค์กร และสนับสนุนให้เกิดวัฒนธรรมการเคารพสิทธิข้อมูลส่วนบุคคล

๖.๒ การสนับสนุนด้านทรัพยากร (Resources)

- **งบประมาณ** สำหรับจัดหาเครื่องมือด้านความปลอดภัยทางเทคโนโลยี (เช่น Firewall, ระบบ Encryption) และระบบบริหารจัดการข้อมูล

- **บุคลากร** สนับสนุนการแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือคณะทำงานเฉพาะกิจเพื่อรับผิดชอบงานด้านนี้โดยตรง หากองค์กรเข้าข่ายตามเงื่อนไขกฎหมาย

๖.๓ การฝึกอบรมและสื่อสาร (Training & Communication)

- สนับสนุนให้มีการจัดฝึกอบรมบุคลากรทุกระดับอย่างต่อเนื่อง เพื่อสร้างความเข้าใจและลดความเสี่ยงจากความผิดพลาดของคน (Human Error) ในการปฏิบัติงาน

๖.๔ การตัดสินใจในกรณีที่มีความเสี่ยงสูง

- สนับสนุนการตัดสินใจในการทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) สำหรับโครงการใหม่ๆ ที่มีความเสี่ยงสูง เพื่อให้มั่นใจว่าองค์กรได้ปิดความเสี่ยงก่อนเริ่มดำเนินการ

จึงเรียนมาเพื่อโปรดทราบ

(ลงชื่อ) .....

(นางสาวศจิษฐา รีรักษ์)

ผู้เข้ารับการฝึกอบรม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณศจิษฐา รีรักษ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 21 พฤศจิกายน 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPCC80302378

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณศจิษฐา รีรักษ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 21 พฤศจิกายน 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680302378

สำเนาถูกต้อง
ศจิษฐา รีรักษ์
นักบริหารการโรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังทอง

สรุปประเด็นสำคัญจากหลักสูตรการปฏิบัติหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคล
สรุปหลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง และผู้รับจ้าง

เอกสารฉบับนี้สังเคราะห์เนื้อหาหลักจากหลักสูตรการปฏิบัติหน้าที่ของผู้เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยมุ่งเน้นกรอบกฎหมายและแนวปฏิบัติที่สำคัญภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ประเด็นสำคัญคือการกำหนดนิยามของ "ข้อมูลส่วนบุคคล" และการจำแนกบทบาทของผู้มีส่วนได้เสียหลัก ได้แก่ เจ้าของข้อมูล (Data Subject) ผู้ควบคุมข้อมูล (Data Controller) ผู้ประมวลผลข้อมูล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งแต่ละฝ่ายมีหน้าที่และความรับผิดชอบที่แตกต่างกัน

หัวใจสำคัญของการปฏิบัติตามกฎหมายคือการประมวลผลข้อมูล (การเก็บรวบรวม ใช้ หรือเปิดเผย) ต้องเป็นไปตามหลักการพื้นฐาน 8 ประการ เช่น การจำกัดการเก็บรวบรวม การกำหนดวัตถุประสงค์ที่ชัดเจน และการรักษาความมั่นคงปลอดภัย นอกจากนี้ การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมายที่เหมาะสม อาทิ ความยินยอม สัญญา หรือประโยชน์อันชอบด้วยกฎหมาย กฎหมายยังให้ความสำคัญกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมถึงสิทธิในการเข้าถึง แก้ไข ลบ และโอนย้ายข้อมูลของตนเอง

เอกสารยังครอบคลุมถึงความท้าทายในยุคดิจิทัล เช่น การใช้ข้อมูลในบริบทของการจ้างงาน การทำงานจากที่บ้าน (WFH) การตลาดแบบตรง การใช้เทคโนโลยีเฝ้าระวังอย่างกล้องวงจรปิด (CCTV) และเทคโนโลยีจดจำใบหน้า (FRT) รวมถึงการประมวลผลข้อมูลบนระบบคลาวด์และปัญญาประดิษฐ์ (AI) ท้ายที่สุด เอกสารได้ชี้แจงกลไกการบังคับใช้กฎหมายซึ่งประกอบด้วยความรับผิดทางแพ่ง โทษทางปกครอง และโทษทางอาญาที่รุนแรง เพื่อสร้างความตระหนักและรับประกันการปฏิบัติตามกฎหมายอย่างเคร่งครัด

1. หลักการพื้นฐานและกฎหมายที่เกี่ยวข้อง

1.1 นิยามและองค์ประกอบของ "ข้อมูลส่วนบุคคล"

ข้อมูลที่จะถือว่าเป็น "ข้อมูลส่วนบุคคล" ตามกฎหมาย จะต้องมีองค์ประกอบครบถ้วนทั้ง 4 ประการ ดังนี้

- **ต้องเป็นข้อมูล:** เป็นข้อเท็จจริงหรือสิ่งที่สามารถสื่อความหมายได้
- **ต้องเกี่ยวข้องกับบุคคล:** ข้อมูลดังกล่าวต้องมีความสัมพันธ์กับบุคคลใดบุคคลหนึ่ง
- **สามารถระบุตัวบุคคลนั้นได้:** ข้อมูลดังกล่าวทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม
- **บุคคลนั้นต้องเป็นบุคคลธรรมดาที่มีชีวิตอยู่:** ไม่รวมถึงข้อมูลของนิติบุคคลหรือผู้ที่ถึงแก่กรรมแล้ว

ตัวอย่างของข้อมูลส่วนบุคคล:

- เลขบัตรประจำตัวประชาชน
- ชื่อ - นามสกุล
- ที่อยู่, เบอร์โทรศัพท์, อีเมล
- ข้อมูลทางการเงิน

- เชื้อชาติ, ศาสนา
- ข้อมูลสุขภาพ, ประวัติอาชญากรรม
- ข้อมูลสภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลเกี่ยวกับเพศสภาพ

1.2 หลักการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลต้องยึดถือตามหลักการสำคัญ 8 ประการ ดังนี้:

1. **หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle):** เก็บข้อมูลเท่าที่จำเป็นและโดยชอบด้วยกฎหมาย
2. **หลักคุณภาพของข้อมูล (Data Quality Principle):** ข้อมูลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน
3. **หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle):** ต้องแจ้งวัตถุประสงค์ให้ชัดเจนก่อนหรือขณะเก็บ
4. **หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle):** ใช้หรือเปิดเผยข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น
5. **หลักการรักษาความมั่นคงปลอดภัย (Security Safeguards Principle):** มีมาตรการป้องกันการเข้าถึงหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต
6. **หลักความโปร่งใส (Openness Principle):** เปิดเผยนโยบายและแนวปฏิบัติเกี่ยวกับการจัดการข้อมูล
7. **หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle):** เจ้าของข้อมูลมีสิทธิเข้าถึง แก้ไข และคัดค้านข้อมูลของตน
8. **หลักความรับผิดชอบ (Accountability Principle):** ผู้ควบคุมข้อมูลต้องรับผิดชอบและสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการข้างต้นได้

1.3 กฎหมายอื่นที่เกี่ยวข้อง

การคุ้มครองข้อมูลส่วนบุคคลมีความเชื่อมโยงกับกฎหมายฉบับอื่น ๆ ดังนี้:

- **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562:** มีเจตนาเพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ความมั่นคงของรัฐ และความสงบเรียบร้อย โดยกำหนดให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยง 3 ระดับ คือ ไม่ร้ายแรง ร้ายแรง และวิกฤติ
- **พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540:** ส่งเสริมความโปร่งใสโดยให้ประชาชนมีสิทธิเข้าถึงข้อมูลข่าวสารของราชการตามหลัก "เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น" เพื่อให้สามารถแสดงความคิดเห็นทางการเมืองได้อย่างถูกต้อง
- **พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562:** มุ่งสู่การเป็นรัฐบาลดิจิทัล โดยบูรณาการฐานข้อมูลของหน่วยงานรัฐให้เชื่อมโยงกันอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และโปร่งใส สนับสนุน Open Government Data และธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)

- **พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544:** รองรับสถานะทางกฎหมายของข้อมูลและลายมือชื่ออิเล็กทรอนิกส์ให้มีผลเช่นเดียวกับเอกสารที่เป็นหนังสือ เพื่อส่งเสริมความน่าเชื่อถือของธุรกรรมทางอิเล็กทรอนิกส์

2. บทบาทและความรับผิดชอบ

2.1 การจำแนกบทบาท

ตามกฎหมาย PDPA สามารถจำแนกบทบาทของผู้ที่เกี่ยวข้องได้ 3 ฝ่ายหลัก ดังตัวอย่างต่อไปนี้:

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject):** นาย ก. ซึ่งเป็นบุคคลที่ข้อมูลของตนถูกเก็บรวบรวม ใช้ หรือเปิดเผย
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller):** บริษัทค้าปลีก ซึ่งมีอำนาจตัดสินใจว่าจะเก็บข้อมูลของนาย ก. เพื่อวัตถุประสงค์ใด
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor):** บริษัทบริหารจัดการเงินเดือน ซึ่งดำเนินการเกี่ยวกับข้อมูลตามคำสั่งของบริษัทค้าปลีก เช่น การโอนเงินเดือนให้นาย ก.

2.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บางองค์กรจำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยเฉพาะหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด ตัวอย่างเช่น:

- กรมบัญชีกลาง กระทรวงการคลัง
- กรมการกงสุล กระทรวงการต่างประเทศ
- กรมการขนส่งทางบก กระทรวงคมนาคม
- กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์
- การรถไฟแห่งประเทศไทย
- ธนาคารแห่งประเทศไทย
- มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด

ถึงแม้กฎหมายไม่ได้บังคับ องค์กรก็สามารถเลือกที่จะแต่งตั้ง DPO ได้เพื่อช่วยในการจัดการและสร้างความมั่นใจว่าได้ปฏิบัติตามกฎหมายอย่างถูกต้อง

2.3 ข้อยกเว้นสำหรับกิจการขนาดเล็ก

กิจการขนาดเล็กบางประเภทได้รับการยกเว้นไม่ต้องดำเนินการตามมาตรา 39 บางส่วน โดยต้องมีลักษณะอย่างใดอย่างหนึ่งดังนี้:

- วิสาหกิจขนาดย่อมหรือขนาดกลาง (SMEs)
- วิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน
- วิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม
- สหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกร
- มูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร
- กิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

3. ฐานทางกฎหมายในการประมวลผลข้อมูล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะกระทำได้ต่อเมื่อมีฐานทางกฎหมายรองรับ ซึ่งมีหลายฐาน ดังนี้:

- **ฐานความยินยอม (Consent):** ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง
- **ฐานสัญญา (Contract):** จำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา
- **ฐานการปฏิบัติตามกฎหมาย (Legal Obligation):** เป็นการจำเป็นเพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล
- **ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest):** เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
- **ฐานภารกิจของรัฐ (Public Interest/Public Task):** จำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือใช้อำนาจรัฐ
- **ฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest):** จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลอื่น
- **ฐานเอกสารประวัติศาสตร์/วิจัย (Archiving/Research):** เพื่อการจัดทำเอกสารประวัติศาสตร์ วิจัย หรือสถิติ

3.1 ฐานการประมวลผลข้อมูลอ่อนไหว (มาตรา 26)

สำหรับข้อมูลอ่อนไหว (เช่น เชื้อชาติ, ข้อมูลสุขภาพ, ข้อมูลชีวภาพ) การประมวลผลจะต้องมีฐานที่เฉพาะเจาะจงมากขึ้น เช่น:

- **เพื่อวัตถุประสงค์ทางการแพทย์:** เช่น เวชศาสตร์ป้องกัน, การวินิจฉัยโรค, การให้บริการด้านสุขภาพโดยผู้ประกอบวิชาชีพ
- **กิจกรรมขององค์กรไม่แสวงหากำไร:** การดำเนินกิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม ที่มีวัตถุประสงค์ด้านการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน สำหรับข้อมูลของสมาชิก
- **การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ:** เพื่อบรรลุวัตถุประสงค์ดังกล่าวเท่าที่จำเป็นและมีมาตรการคุ้มครองที่เหมาะสม

3.2 ขอบเขตการบังคับใช้และข้อยกเว้น

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ไม่ใช้บังคับกับกิจกรรมบางประเภท ได้แก่:

- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการยุติธรรม
- การดำเนินงานของบริษัทข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต
- การดำเนินงานของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่เกี่ยวข้อง
- การเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว (Private Use)

4. สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมายได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ เพื่อให้สามารถควบคุมข้อมูลของตนเองได้

4.1 สิทธิในการแก้ไขข้อมูล (Right to Rectification)

เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลของตนให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์ (มาตรา 35) หากผู้ควบคุมข้อมูลปฏิเสธคำร้อง จะต้องบันทึกคำร้องและเหตุผลของการปฏิเสธไว้ และเจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้ (มาตรา 36)

4.2 สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)

สิทธินี้มีวัตถุประสงค์เพื่อให้บุคคลสามารถย้ายข้อมูลส่วนบุคคลของตนจากบริการหนึ่งไปยังอีกบริการหนึ่งได้ เช่น การย้ายข้อมูลจาก Spotify ไปยัง Apple Music หรือจาก Google Photos ไปยัง Amazon Photos โดยผู้ควบคุมข้อมูลต้องจัดเตรียมข้อมูลในรูปแบบที่เครื่องมือหรืออุปกรณ์สามารถอ่านและใช้งานได้โดยอัตโนมัติ (เช่น ผ่าน API) เพื่อให้เกิดความสามารถในการทำงานร่วมกัน (interoperability) ซึ่งจะช่วยเพิ่มอำนาจให้ผู้บริโภคและสร้างโอกาสทางนวัตกรรม

5. ประเด็นเฉพาะทางและกรณีศึกษา

5.1 การตลาดแบบตรง (Direct Marketing)

- **นิยาม:** การทำตลาดสินค้าหรือบริการโดยสื่อสารข้อมูลเพื่อเสนอขายโดยตรงต่อผู้บริโภคที่อยู่ห่างไกล และมุ่งหวังให้เกิดการตอบกลับเพื่อซื้อสินค้า
- **ขั้นตอนการดำเนินการ:**
    1. **การระบุ (Identify):** ระบุฐานทางกฎหมายและวัตถุประสงค์
    2. **การวางแผน (Plan):** วางแผนการจัดการข้อมูล
    3. **การเก็บรวบรวม (Collect):** เก็บข้อมูลอย่างโปร่งใสและเท่าที่จำเป็น
    4. **การเคารพสิทธิ (Respect):** เคารพสิทธิของเจ้าของข้อมูลในการคัดค้านหรือถอนความยินยอม
- **ความท้าทาย:** การประมวลผลข้อมูลเพื่อการตลาดมักขาดความโปร่งใสและขาดการควบคุมจากเจ้าของข้อมูล เช่น กรณีโมเดลธุรกิจ “Consent or Pay” ของ Facebook ที่ให้ผู้ใช้เลือกระหว่างการยินยอมให้ใช้ข้อมูลเพื่อการโฆษณา หรือจ่ายเงินเพื่อใช้บริการแบบไม่มีโฆษณา ซึ่ง European Data Protection Board (EDPB) ได้ตั้งคำถามถึงความชอบด้วยกฎหมายของความยินยอมในลักษณะนี้

5.2 การจ้างงานและ Work From Home (WFH)

- **บริบทการจ้างงาน:** นายจ้างสามารถประมวลผลข้อมูลของลูกจ้างเพื่อบรรลุวัตถุประสงค์ตามสัญญาจ้างแรงงาน หรืออ้างอิงฐานประโยชน์อันชอบด้วยกฎหมายเพื่อรักษาความปลอดภัยของระบบสารสนเทศ โดยไม่จำเป็นต้องขอความยินยอมแบบบังคับ
- **ความท้าทายของ WFH:** แม้พนักงานจะทำงานจากนอกสถานที่ องค์กรยังคงมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อธำรงไว้ซึ่ง **ความลับ (Confidentiality)**, **ความถูกต้องครบถ้วน (Integrity)**, และ **สภาพพร้อมใช้งาน (Availability)** ของข้อมูลส่วนบุคคล

5.3 การเฝ้าระวังและข้อมูลชีวภาพ

- **ข้อมูลชีวภาพ (Biometric Data):** เป็นข้อมูลอ่อนไหว เช่น ข้อมูลจำลองลายนิ้วมือ, ภาพจำลองใบหน้า, ข้อมูลจำลองม่านตา, เสียง, รูปแบบการเดิน
- **กล้องวงจรปิด (CCTV):** องค์กรต้องมีนโยบายที่ชัดเจน เช่น กำหนดระยะเวลาการเก็บรักษาข้อมูล (เช่น 30 วัน) และจำกัดการเข้าถึงข้อมูลเฉพาะบุคคลที่ได้รับอนุญาต
- **กรณีศึกษา Clearview AI:** บริษัทที่ใช้เทคโนโลยีจดจำใบหน้า (FRT) โดยรวบรวมภาพใบหน้ากว่า 3 หมื่นล้านภาพจากอินเทอร์เน็ตเพื่อช่วยค้นหาผู้กระทำผิด ซึ่งการกระทำดังกล่าวอาจขัดต่อกฎหมายคุ้มครองข้อมูลอย่าง GDPR และ PDPA ของไทย เนื่องจากข้อมูลภาพจำลองใบหน้าถือเป็นข้อมูลอ่อนไหวที่ต้องได้รับความยินยอมโดยชัดแจ้ง อย่างไรก็ตาม มาตรา 4(5) ของ PDPA ได้ยกเว้นการบังคับใช้กับการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

5.4 การส่งข้อมูลไปต่างประเทศ

การโอนข้อมูลข้ามพรมแดนต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล โดยต้องอาศัยกลไกอย่างใดอย่างหนึ่ง ดังนี้:

- **มาตรฐานการคุ้มครองที่เพียงพอ (Adequacy decisions):** ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอตามที่คณะกรรมการฯ กำหนด
- **มาตรการคุ้มครองที่เหมาะสม (Appropriate safeguard):** เช่น การมีนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules - BCRs)
- **ข้อยกเว้นตามกฎหมาย (Derogations):** เป็นกรณีจำเป็นตามข้อยกเว้นที่กฎหมายกำหนด

5.5 เทคโนโลยีและความท้าทายใหม่ๆ

- **Cloud Computing:** องค์กรยังคงมีความกังวลในการใช้ระบบคลาวด์ในด้านความมั่นคงปลอดภัย, การปฏิบัติตามกฎหมาย, และความเสี่ยงในการควบคุมข้อมูล กรณีศึกษาจากศาลเยอรมนีชี้ให้เห็นว่าการใช้บริการคลาวด์ที่ตั้งอยู่ในประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลเพียงพอ (เช่น สหรัฐอเมริกา) อาจถือเป็นการโอนข้อมูลไปต่างประเทศที่ไม่ชอบด้วยกฎหมาย
- **AI (Generative AI):** ในการใช้งาน Generative AI เช่น Grok ของ xAI/Twitter ผู้ใช้งาน (end user) จะอยู่ในฐานะ "ผู้ควบคุมข้อมูลส่วนบุคคล" และผู้ให้บริการ AI จะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล"
- **Cookies:** Cookie IDs บางประเภทที่สามารถใช้ระบุตัวตนของบุคคลได้ ถือเป็น "ข้อมูลส่วนบุคคล" ซึ่งสอดคล้องกับแนวทางของ GDPR และคำตัดสินของศาลยุติธรรมแห่งสหภาพยุโรป

6. การบังคับใช้กฎหมายและบทลงโทษ

กฎหมาย PDPA กำหนดมาตรการบังคับใช้ 3 รูปแบบ:

ประเภทความรับผิด	รายละเอียด
ความรับผิดทางแพ่ง	เจ้าของข้อมูลสามารถฟ้องร้องเรียกค่าสินไหมทดแทนจากความเสียหายที่เกิดขึ้นจริงได้
โทษทางปกครอง	คณะกรรมการผู้เชี่ยวชาญสามารถสั่งปรับได้ โดยพิจารณาตามความร้ายแรงของการกระทำผิด
โทษทางอาญา	มีโทษจำคุกและ/หรือปรับ สำหรับการกระทำความผิดในบางมาตรา

6.1 โทษทางปกครอง

คณะกรรมการผู้เชี่ยวชาญจะพิจารณาออกคำสั่งตามระดับความร้ายแรง:

- **กรณีไม่ร้ายแรง:** อาจมีคำสั่งให้ตักเตือน หรือแก้ไขให้ถูกต้องภายในเวลาที่กำหนด
- **กรณีร้ายแรง:** อาจมีคำสั่งลงโทษปรับทางปกครอง หรือสั่งให้หยุดการกระทำที่ฝ่าฝืนกฎหมาย

6.2 โทษทางอาญา

- **มาตรา 79:** กำหนดโทษสำหรับผู้ควบคุมข้อมูลที่ใช้หรือเปิดเผยข้อมูลอ่อนไหว (ตามมาตรา 26) โดยไม่ได้รับความยินยอม และเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- **ข้อยกเว้น "การใช้เพื่อประโยชน์ส่วนตน":** มาตรา 4(1) ยกเว้นการบังคับใช้กฎหมายกับการเก็บรวบรวมเพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว อย่างไรก็ตาม การนำข้อมูลผู้อื่นไปโพสต์ประจานในโซเชียลมีเดีย เช่น โพสต์ภาพใบสำคัญการหย่า หรือสำเนาบัตรประชาชนของลูกหนี้ ไม่ถือเป็นการใช้เพื่อประโยชน์ส่วนตน และอาจมีความผิดทางอาญาได้
- **ความรับผิดของนิติบุคคลและกรรมการ:** หากการกระทำผิดของนิติบุคคลเกิดจากการสั่งการหรือการละเว้นการสั่งการของกรรมการหรือผู้จัดการ บุคคลดังกล่าวต้องรับโทษทางอาญาด้วย (มาตรา 81)

7. หน่วยงานกำกับดูแล

7.1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.)

เป็นองค์กรหลักในการกำกับดูแล ประกอบด้วย:

- ประธานกรรมการ
- รองประธานกรรมการ (ปลัดกระทรวงดิจิทัลฯ)
- กรรมการโดยตำแหน่ง 5 คน (ปลัดสำนักนายกฯ, เลขาธิการกฤษฎีกา, เลขาธิการ สคบ., อธิบดีกรมคุ้มครองสิทธิฯ, อัยการสูงสุด)
- กรรมการผู้ทรงคุณวุฒิ 9 คน
- เลขาธิการ (เป็นกรรมการและเลขานุการ)

อำนาจหน้าที่หลัก: จัดทำแผนแม่บทด้านการคุ้มครองข้อมูลส่วนบุคคล, ส่งเสริมและสนับสนุนการดำเนินงานของภาครัฐและเอกชน

7.2 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เป็นหน่วยงานธุรการของ กคส. มีอำนาจหน้าที่สำคัญ ได้แก่:

- จัดทำร่างแผนแม่บทฯ เสนอต่อ กคส.
- ส่งเสริมและสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวข้อง
- เป็นศูนย์กลางในการให้บริการทางวิชาการและให้ความรู้แก่ประชาชน
- กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้เกี่ยวข้อง
- ทำความตกลงและร่วมมือกับองค์กรทั้งในและต่างประเทศ
- ติดตามและประเมินผลการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

เอกสารชุดนี้สรุปสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยอธิบายถึงบทบาทหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล รวมถึงขอบเขตการบังคับใช้และข้อยกเว้นต่างๆ เนื้อหาเน้นย้ำถึงสิทธิของเจ้าของข้อมูล เช่น การเพิกถอนความยินยอมและการขอโอนย้ายข้อมูล ตลอดจนมาตรฐานการรักษาความปลอดภัยที่ต้องครอบคลุมทั้งความลับ ความถูกต้อง และสภาพพร้อมใช้งาน นอกจากนี้ยังระบุถึงกฎหมายอื่นที่เกี่ยวข้อง อาทิ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ ประมวลกฎหมายแพ่งและอาญา เพื่อชี้ให้เห็นถึงความรับผิดชอบและการเยียวยาเมื่อเกิดการละเมิดสิทธิความเป็นส่วนตัว ปิดท้ายด้วยกลไกการร้องเรียนผ่านสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและแบบทดสอบความรู้เพื่อทบทวนความเข้าใจในเชิงปฏิบัติ

สรุปหลักการคุ้มครองข้อมูลส่วนบุคคล ๘ ประการ

๑. บทนำ: ทำไมการคุ้มครองข้อมูลส่วนบุคคลจึงสำคัญ?

ในยุคดิจิทัลปัจจุบันที่เทคโนโลยีก้าวหน้าอย่างรวดเร็ว การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้อย่างง่ายดายและรวดเร็ว ซึ่งนำมาสู่การละเมิดสิทธิความเป็นส่วนตัวที่สร้างความเดือดร้อนรำคาญและความเสียหายให้แก่เจ้าของข้อมูลจำนวนมาก อีกทั้งยังส่งผลกระทบในเชิงลบต่อระบบเศรษฐกิจโดยรวมอีกด้วย

ด้วยเหตุนี้ การมีหลักเกณฑ์และมาตรการกำกับดูแลที่ชัดเจนจึงกลายเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อสร้างความเชื่อมั่นว่าข้อมูลส่วนบุคคลจะได้รับการจัดการอย่างถูกต้องและปลอดภัย การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้เป็นเพียงการปกป้องสิทธิขั้นพื้นฐานของบุคคลเท่านั้น แต่ยังเป็นกลไกสำคัญในการสร้างมาตรฐานและมาตรการเยียวยาที่มีประสิทธิภาพเมื่อเกิดการละเมิดสิทธิขึ้น

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและเป็นที่ยอมรับในระดับสากล แนวทางของ OECD (Organisation for Economic Co-operation and Development) ได้กำหนดหลักการสำคัญ ๘ ประการ ซึ่งได้กลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงเป็นหัวใจสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยด้วย

๒. หลักการคุ้มครองข้อมูลส่วนบุคคล ๘ ประการ

หลักการทั้ง ๘ ประการนี้เป็นกรอบแนวปฏิบัติสากลที่ช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง โปร่งใส และเคารพต่อสิทธิของเจ้าของข้อมูล ซึ่งเป็นรากฐานสำคัญในการสร้างความไว้วางใจในระบบเศรษฐกิจดิจิทัล โดยมีรายละเอียดดังนี้

๒.๑ หลักการจำกัดการเก็บรวบรวม (Data Minimization)

หลักการนี้เน้นย้ำแนวคิด **"เก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น"** ซึ่งหมายความว่าการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องทำเท่าที่จำเป็นภายใต้วัตถุประสงค์ที่ชัดเจนเท่านั้น โดยต้องพิจารณา ๓ องค์ประกอบสำคัญคือ ข้อมูลนั้นต้อง **เพียงพอ (Adequate)**, **เกี่ยวข้อง (Relevant)** และ **จำกัดอยู่เฉพาะ (Limited)** สิ่งที่จำเป็นตามวัตถุประสงค์ที่กำหนดไว้ เพื่อป้องกันการเก็บข้อมูลเกินความจำเป็น

ตัวอย่าง: ร้านค้าออนไลน์ที่ต้องการมอบคูปองส่วนลดในเดือนเกิดของลูกค้า ควรเก็บข้อมูลเพียง วันและเดือนเกิด เท่านั้น ไม่มีความจำเป็นต้องเก็บข้อมูล ปีเกิด เพราะเป็นข้อมูลที่เกินความจำเป็นสำหรับวัตถุประสงค์ดังกล่าว

๒.๒ หลักการระบุวัตถุประสงค์อย่างชัดเจน (Purpose Specification)

ผู้ควบคุมข้อมูล (องค์กรที่เก็บข้อมูล) มีหน้าที่ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจน *ก่อนหรือในขณะที่ทำการเก็บรวบรวม* ข้อมูลนั้นๆ การไม่แจ้งวัตถุประสงค์ถือเป็นความผิดและมีโทษปรับทางปกครองตามกฎหมาย หลักการนี้สร้างความโปร่งใสและทำให้เจ้าของข้อมูลตัดสินใจได้ว่าจะให้ข้อมูลของตนหรือไม่

ตัวอย่าง: แอปพลิเคชันสำหรับสมัครงานต้องระบุในหน้ากรอกข้อมูลให้ชัดเจนว่า 'บริษัทจะนำข้อมูลส่วนบุคคลของผู้สมัครไปใช้เพื่อการพิจารณาคัดเลือกเข้าทำงานเท่านั้น และจะไม่นำไปใช้เพื่อวัตถุประสงค์ทางการตลาดอื่นใด'

๒.๓ หลักการคุณภาพของข้อมูล (Data Quality)

ข้อมูลส่วนบุคคลที่ถูกจัดเก็บจะต้องมีความ **ถูกต้อง (Accurate)**, **เป็นปัจจุบัน (Up-to-date)**, **สมบูรณ์ (Complete)** และ **ไม่ก่อให้เกิดความเข้าใจผิด** หลักการนี้มีความสำคัญอย่างยิ่งต่อการตัดสินใจหรือการดำเนินการต่างๆ ที่เกี่ยวข้องกับเจ้าของข้อมูล การมีข้อมูลที่ผิดพลาดอาจนำไปสู่ความเสียหายได้

ตัวอย่าง: ธนาคารต้องมีกระบวนการให้ลูกค้าสามารถแจ้งปรับปรุงข้อมูลที่อยู่และเบอร์โทรศัพท์ให้เป็นปัจจุบันได้เสมอ เพื่อให้การส่งเอกสารสำคัญทางการเงินหรือการติดต่อในกรณีฉุกเฉินเป็นไปอย่างถูกต้องและไม่เกิดข้อผิดพลาด

๒.๔ หลักการจำกัดการใช้งาน (Use Limitation)

การนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยจะต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ตั้งแต่แรกเท่านั้น หากต้องการนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่แจ้งไว้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเสมอ หรือต้องเป็นกรณีที่มีข้อยกเว้นตามที่กฎหมายกำหนด

ตัวอย่าง: โรงพยาบาลที่เก็บข้อมูลประวัติการรักษาของผู้ป่วยเพื่อใช้ในการวินิจฉัยและรักษาพยาบาล จะไม่สามารถนำข้อมูลสุขภาพดังกล่าวไปเปิดเผยให้กับบริษัทประกันภัยเพื่อเสนอขายผลิตภัณฑ์โดยไม่ได้รับความยินยอมที่ชัดเจนจากผู้ป่วยก่อน

๒.๕ หลักการรักษาความปลอดภัย (Security Safeguards)

ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมและได้มาตรฐาน เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยมาตรการดังกล่าวต้องธำรงไว้ซึ่งองค์ประกอบ ๓ ด้านหลัก ได้แก่

- **ความลับ (Confidentiality):** ป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่มีสิทธิ์
- **ความถูกต้องครบถ้วน (Integrity):** ป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- **สภาพพร้อมใช้งาน (Availability):** ทำให้มั่นใจว่าข้อมูลพร้อมใช้งานเมื่อต้องการ และป้องกันการถูกทำลาย

ตัวอย่าง: บริษัทควรมีมาตรการรักษาความปลอดภัยทั้งทางเทคนิค เช่น การเข้ารหัสข้อมูล (Encryption) และการจำกัดสิทธิ์การเข้าถึง (Access Control), และมาตรการเชิงบริหารจัดการ เช่น การจัดอบรมพนักงานเรื่องความปลอดภัยของข้อมูล และการกำหนดนโยบายโต๊ะสะอาด (Clean Desk Policy) เพื่อป้องกันการเข้าถึงเอกสารสำคัญโดยไม่ได้รับอนุญาต

๒.๖ หลักการจำกัดระยะเวลาการจัดเก็บ (Storage Limitation)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลที่ชัดเจน และต้องมีระบบตรวจสอบเพื่อ **ลบหรือทำลาย** ข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาดังกล่าว หรือเมื่อข้อมูลนั้นหมดความจำเป็นตามวัตถุประสงค์ที่ได้เก็บรวบรวมมาแล้ว

ตัวอย่าง: บริษัทที่จัดกิจกรรมสัมมนาออนไลน์ ควรมีนโยบายลบข้อมูลส่วนบุคคล (เช่น ชื่อ อีเมล เบอร์โทร) ของผู้เข้าร่วมงานหลังจากกิจกรรมสิ้นสุดลงและหมดความจำเป็นในการติดต่อสื่อสารแล้ว เช่น กำหนดนโยบายลบข้อมูลภายใน ๙๐ วันหลังจบงาน

๒.๗ หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและควบคุมข้อมูลของตนเอง ซึ่งรวมถึงสิทธิสำคัญหลายประการ เช่น:

- **สิทธิขอเข้าถึงและรับสำเนาข้อมูล (Right of Access)**
- **สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง (Right to Rectification)**
- **สิทธิขอให้ลบหรือทำลายข้อมูล (Right to Erasure)**
- **สิทธิคัดค้านการประมวลผลข้อมูล (Right to Object)**

ตัวอย่าง: ผู้ใช้งานแพลตฟอร์มโซเชียลมีเดียมีสิทธิขอดูข้อมูลทั้งหมดที่แพลตฟอร์มเก็บรวบรวมเกี่ยวกับตนเอง (เช่น ประวัติการโพสต์, ข้อมูลโปรไฟล์) และมีสิทธิร้องขอให้ลบบัญชีและข้อมูลที่เกี่ยวข้องทั้งหมดออกจากระบบได้

๒.๘ หลักการความรับผิดชอบ (Accountability)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบในการปฏิบัติตามหลักการและมาตรการต่างๆ ที่กฎหมายกำหนดอย่างเคร่งครัด และต้องสามารถแสดงหลักฐานหรือพิสูจน์ให้เห็นถึงการปฏิบัติตามกฎหมายได้อย่างเป็นรูปธรรม (demonstrate compliance) หลักการนี้เป็นเครื่องยืนยันว่าการคุ้มครองข้อมูลจะเกิดขึ้นจริงในทางปฏิบัติ

ตัวอย่าง: หากเกิดเหตุข้อมูลลูกค้ารั่วไหลออกจากระบบของบริษัท บริษัทที่เป็นผู้ควบคุมข้อมูลต้องมีหน้าที่รับผิดชอบในการแจ้งเหตุให้เจ้าของข้อมูลที่ได้รับผลกระทบและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยเร็ว พร้อมทั้งมีมาตรการตรวจสอบและเยียวยาความเสียหายที่เกิดขึ้น

การปฏิบัติตามหลักการทั้ง ๘ ประการนี้อย่างครบถ้วน จะช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีธรรมาภิบาลและสร้างความน่าเชื่อถือให้กับองค์กร

๓. ตารางสรุปหลักการ ๘ ประการ

เพื่อทบทวนความเข้าใจ สามารถสรุปหัวใจสำคัญของแต่ละหลักการได้ดังตารางต่อไปนี้

หลักการ	หัวใจสำคัญ
การจำกัดการเก็บรวบรวม (Data Minimization)	เก็บข้อมูลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนด
การระบุวัตถุประสงค์อย่างชัดเจน (Purpose Specification)	แจ้งให้ชัดเจนว่าจะเก็บข้อมูลไปทำอะไร
คุณภาพของข้อมูล (Data Quality)	ข้อมูลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันเสมอ
การจำกัดการใช้งาน (Use Limitation)	ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น
การรักษาความปลอดภัย (Security Safeguards)	ต้องมีมาตรการป้องกันข้อมูลให้ปลอดภัย
การจำกัดระยะเวลาการจัดเก็บ (Storage Limitation)	เมื่อหมดความจำเป็นแล้วต้องลบหรือทำลาย
การมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation)	เจ้าของข้อมูลมีสิทธิตรวจสอบ แก้ไข และลบข้อมูลตนเอง
ความรับผิดชอบ (Accountability)	ผู้เก็บข้อมูลต้องรับผิดชอบและพิสูจน์ได้ว่าทำตามกฎหมาย

ตารางนี้เป็นเครื่องมือช่วยจำที่ทำให้เห็นภาพรวมของกรอบการคุ้มครองข้อมูลส่วนบุคคลได้อย่างรวดเร็ว

๔. สรุป

การปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลทั้ง ๘ ประการ ไม่เพียงแต่เป็นการดำเนินงานให้สอดคล้องกับข้อกฎหมายเท่านั้น แต่ยังเป็นการแสดงความเคารพต่อสิทธิความเป็นส่วนตัวของบุคคล ซึ่งเป็นรากฐานสำคัญของการสร้าง ความไว้วางใจ (Trust) ระหว่างองค์กรและเจ้าของข้อมูล ไม่ว่าจะเป็นลูกค้า พนักงาน หรือคู่ค้า การสร้างความไว้วางใจนี้จะช่วยส่งเสริมให้เกิดระบบนิเวศดิจิทัลที่ปลอดภัยและน่าเชื่อถือ ซึ่งเป็นประโยชน์ต่อทุกภาคส่วนในระยะยาว ท้ายที่สุดแล้ว การคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพคือความรับผิดชอบร่วมกัน ที่ช่วยปกป้องสิทธิของบุคคลและเสริมสร้างความแข็งแกร่งให้กับองค์กรในโลกดิจิทัลไปพร้อมกัน

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณจันทิมา จันทะบูรณ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 25 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680310825