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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณกัญจน์ชรัตน์ ชุ่มวงศ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 26 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680311115

ห้ามใช้โฆษณาในทางธุรกิจ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณกัญจน์ชรัตน์ ชุ่มวงศ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 25 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680406414

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณพิมพ์ใจ ดวงแก้ว

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 18 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690401036

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณพิมพ์ใจ ดวงแก้ว

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 18 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690301470

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณเมวิกา กัณฑชัยวรรณ

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 23 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690401361

ห้ามใช้โฆษณาในทางธุรกิจ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณเมวิกา กัณฑชัยวรรณ

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 17 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690301426

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมายที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณปภัสสร สุขโข

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 17 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690301433

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณปภัสสร สุขโข

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 23 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690401362

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (Data Governance)

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

2. การปฏิบัติตามกฎหมาย

2.1 การจำแนกบทบาท

ตามกฎหมาย PDPA สามารถจำแนกบทบาทของผู้ที่เกี่ยวข้องได้ 3 ฝ่ายหลัก ดังตัวอย่างต่อไปนี้:

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject):** นาย ก. ซึ่งเป็นบุคคลที่ข้อมูลของตนถูกเก็บรวบรวม ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณกานตญา อีนอ้าย

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 16 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690301305

ห้ามใช้โฆษณาในทางธุรกิจ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณกานตญา อีนอ้าย

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที 15 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690400840

ห้ามใช้โฆษณาในทางธุรกิจ

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณแสงจันทร์ ชำนาญยา

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 14 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690400755

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณแสงจันทร์ ชำนาญยา

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 10 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690300649

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณกรรณิการ์ ใหม่ต๊ะ

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 15 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690400850

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณชุติมันต์ ใจกว้าง

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 18 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690401029

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณชุติมันต์ ใจกว้าง

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 18 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690301460

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 การประมวลผลข้อมูลทุกครั้งจะต้องอ้างอิงฐานทางกฎหมาย ที่ เหมาะสม 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 มีประสิทธิภาพและโปร่งใส สนับสนุน Open Government Data และธรรมภิบาลข้อมูลภาครัฐ (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 ใช้หรือเปิดเผย
- **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

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณณิรินทร์ สุริยาพัชราสกุล

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง

ให้ไว้ ณ วันที่ 26 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690302029

ห้ามใช้โฆษณาในทางธุรกิจ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณณิรินทร์ สุริยาพัชราสกุล

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 16 มกราคม 2569

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC690400945

ห้ามใช้โฆษณาในทางธุรกิจ