**แบบรายงานผลการเข้ารับการฝึกอบรม/สัมมนา**

ด้วยข้าพเจ้า นายคำรณ จันทร์ต้น ตำแหน่ง ผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบลบ้านห้วยเคียน สังกัด โรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังทอง กองสาธารณสุขและสิ่งแวดล้อม ได้เข้าร่วมโครงการอบรมเชิงปฏิบัติการหลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป (e-learning) ในวันที่ ๒ ธันวาคม พ.ศ.๒๕๖๘ นั้น

บัดนี้ ข้าพเจ้าได้เข้ารับการฝึกอบรมหลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการฝึกอบรมให้ทราบ ดังนี้

**๑. การฝึกอบรมดังกล่าวมีวัตถุประสงค์เพื่อ**

ให้ประชาชนตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ซึ่งเป็นสิทธิขั้นพื้นฐานในความเป็นส่วนตัว (Right to Privacy) เพื่อป้องกันการละเมิดสิทธิที่อาจก่อให้เกิดความเดือดร้อนรำคาญหรือความเสียหายแก่เจ้าของข้อมูล โดยเฉพาะในยุคที่เทคโนโลยีทำให้การเก็บรวบรวมและใช้ข้อมูลทำได้ง่ายและรวดเร็ว ทั้งนี้ เพื่อให้มีมาตรการเยียวยาที่มีประสิทธิภาพและสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์และเศรษฐกิจดิจิทัล

**๒. เนื้อหาและหัวข้อวิชาของหลักสูตรการฝึกอบรม มีดังนี้**

| บทที่ | เนื้อหาหลักสูตร |
|---|---|
| ๑ | ความสำคัญ แนวคิด ขอบเขตการคุ้มครองข้อมูลส่วนบุคคล ความหมาย ประเภทของข้อมูล และกฎหมายอื่นๆ |
| ๒ | หลักการคุ้มครองข้อมูลส่วนบุคคล |
| ๓ | ฐานทางกฎหมายในการเก็บรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล |
| ๔ | สิทธิของเจ้าของข้อมูลส่วนบุคคล |
| ๕ | ความรับผิดและบทกำหนดโทษ |
| ๖ | กลไกการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ |
| ๗ | การปฏิบัติเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล |
| ๘ | บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล |
| ๙ | กลโกการคุ้มครองข้อมูลส่วนบุคคลของ สคส. |

**สรุปโครงการอบรมเชิงปฏิบัติการหลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป (e-learning)**

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

**๑. ความสำคัญ แนวคิด ขอบเขต และประเภทของข้อมูล**

แนวคิดหลักของ PDPA คือการให้ "อำนาจ" แก่เจ้าของข้อมูลในการควบคุมข้อมูลของตนเอง ในยุคที่ข้อมูลถูกนำไปใช้ในเชิงพาณิชย์และอาชญากรรมไซเบอร์ ข้อมูลส่วนบุคคลเปรียบเสมือนทรัพย์สินที่ต้องการการล้อมรั้วป้องกัน ขอบเขตของกฎหมายนี้ครอบคลุมทั้งหน่วยงานรัฐและเอกชน ไม่ว่าจะเป็นการเก็บข้อมูลในรูปแบบกระดาษหรือดิจิทัล หากข้อมูลนั้นสามารถระบุตัวตนบุคคลที่ยังมีชีวิตอยู่ได้ (ไม่รวมผู้ถึงแก่กรรม) ถือเป็นข้อมูลส่วนบุคคลทั้งสิ้น ประเภทข้อมูลแบ่งเป็น ๒ ระดับหลัก คือ ข้อมูลทั่วไป (ชื่อ, ที่อยู่, IP Address) และข้อมูลอ่อนไหว (Sensitive Data) ซึ่งประเภทหลังนี้มีความสำคัญมาก เพราะหากรั่วไหลอาจนำไปสู่การเลือกปฏิบัติหรือกระทบต่อศักดิ์ศรีความเป็นมนุษย์ เช่น ข้อมูลสหภาพแรงงาน รสนิยมทางเพศ หรือข้อมูลชีวภาพ (ใบหน้า, ลายนิ้วมือ) การเก็บข้อมูลประเภทนี้จึงต้องได้รับความยินยอมโดยชัดแจ้งและมีมาตรฐานความปลอดภัยที่สูงกว่าปกติ นอกจากนี้ PDPA ยังเชื่อมโยงกับกฎหมายอื่น เช่น พ.ร.บ. ไซเบอร์ฯ เพื่อสร้างโครงสร้างพื้นฐานด้านความปลอดภัยที่ครอบคลุมทั้งประเทศ

**๒. หลักการคุ้มครองข้อมูลส่วนบุคคล (Principles)**

หลักการพื้นฐานที่ผู้ควบคุมข้อมูลต้องยึดถือประกอบด้วย ๓ ส่วนสำคัญคือ

๑. การเก็บรวบรวมอย่างจำกัด (Data Minimization) คือการเก็บเท่าที่ "จำเป็น" จริง ๆ ภายใต้วัตถุประสงค์ที่แจ้งไว้ เช่น หากสมัครสมาชิกร้านอาหาร ไม่จำเป็นต้องขอเลขบัตรประชาชน

๒. ความถูกต้องของข้อมูล ผู้เก็บต้องตรวจสอบให้ข้อมูลทันสมัยและไม่ทำให้เกิดความเข้าใจผิด

๓. การจำกัดระยะเวลาการเก็บ (Storage Limitation) ต้องกำหนดชัดเจนว่าจะเก็บข้อมูลไว้นานแค่ไหน (เช่น ๑๐ ปีตามอายุความทางภาษี) และเมื่อพ้นกำหนดต้องทำลายทิ้งทันที หลักการเหล่านี้มีไว้เพื่อลดความเสี่ยง หากเกิดเหตุข้อมูลรั่วไหล ความเสียหายจะถูกจำกัดวงแคบเพราะเราไม่ได้เก็บข้อมูลที่ไม่จำเป็นไว้ตั้งแต่แรก นอกจากนี้ยังเน้นความโปร่งใสผ่าน "นโยบายความเป็นส่วนตัว" (Privacy Notice) ที่ต้องเขียนด้วยภาษาที่เข้าใจง่าย ไม่ใช้ภาษากฎหมายที่ซับซ้อนเกินไป เพื่อให้ประชาชนทราบว่าข้อมูลของตนจะถูกนำไปใช้อย่างไร ใครเป็นผู้รับข้อมูลต่อ และจะติดต่อผู้ควบคุมข้อมูลได้อย่างไร

**๓. ฐานทางกฎหมาย (Lawful Basis) ในการเก็บรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**

หลายคนเข้าใจผิดว่าต้องขอ "ความยินยอม" (Consent) ในทุกกรณี แต่ในความเป็นจริง Consent คือทางเลือกสุดท้ายหากไม่มีฐานอื่นรองรับ ฐานทางกฎหมายช่วยให้กิจกรรมทางเศรษฐกิจและสังคมดำเนินต่อไปได้ เช่น ฐานสัญญา: ธนาคารต้องเก็บที่อยู่คุณเพื่อส่งใบแจ้งหนี้โดยไม่ต้องขอความยินยอมซ้ำซ้อน

ฐานกฎหมาย นายจ้างต้องเก็บเลขผู้เสียภาษีของลูกจ้างเพื่อส่งกรมสรรพากร

ฐานประโยชน์สาธารณะ: หน่วยงานรัฐเก็บข้อมูลเพื่อสวัสดิการแห่งรัฐ

ฐานประโยชน์อันชอบธรรม: การติดกล้อง CCTV เพื่อความปลอดภัยในอาคาร (แต่ต้องติดป้ายแจ้ง)

ฐานระงับอันตรายต่อชีวิต: เช่น กรณีอุบัติเหตุฉุกเฉิน แพทย์สามารถเข้าถึงประวัติการแพ้ยาได้ทันทีโดยไม่ต้องรอขอความยินยอม

การเลือกใช้ฐานที่ถูกต้องมีความสำคัญมาก เพราะหากองค์กรอ้างฐาน Consent แล้วภายหลังเจ้าของข้อมูลถอนความยินยอม องค์กรนั้นอาจต้องหยุดกิจกรรมทันที แต่หากอ้างฐานอื่น เช่น ฐานกฎหมาย แม้เจ้าของข้อมูลจะไม่พอใจ องค์กรก็ยังมีสิทธิเก็บข้อมูลนั้นไว้ได้ตามที่กฎหมายกำหนด

**๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)**

สิทธิเหล่านี้คือเครื่องมือที่ประชาชนใช้ตรวจสอบและควบคุมข้อมูลของตนเอง เริ่มตั้งแต่

- สิทธิขอเข้าถึง (Right of Access) คุณสามารถเดินไปถามธนาคารหรือแอปพลิเคชันได้ว่า "คุณมีข้อมูลอะไรของฉันบ้าง และเอาไปให้ใครดูบ้าง?" โดยองค์กรต้องตอบกลับภายใน ๓๐ วัน

- สิทธิขอให้ลบ (Right to Erasure) หรือ "สิทธิที่จะถูกลืม" (Right to be forgotten) ใช้ได้เมื่อข้อมูลนั้นหมดความจำเป็นหรือได้มาโดยไม่ชอบ

- สิทธิขอให้โอนย้ายข้อมูล (Right to Data Portability) เช่น คุณต้องการย้ายข้อมูลประกันชีวิตจากบริษัท A ไปบริษัท B ในรูปแบบที่คอมพิวเตอร์อ่านได้ เพื่อความสะดวกในการเปรียบเทียบเบี้ยประกัน

- สิทธิคัดค้าน (Right to Object) โดยเฉพาะการนำข้อมูลไปใช้เพื่อการตลาด (Direct Marketing) คุณมีสิทธิสั่งให้เขาหยุดโทรมาขายประกันได้ทันที การใช้สิทธิเหล่านี้เป็นรากฐานของการสร้างดุลอำนาจระหว่างปัจเจกบุคคลกับองค์กรขนาดใหญ่ เพื่อไม่ให้ข้อมูลถูกนำไปใช้ในทางที่เจ้าของข้อมูลไม่ประสงค์

**๕. ความรับผิดและบทกำหนดโทษ**

PDPA มีบทลงโทษที่ครอบคลุมทุกมิติ เพื่อให้มั่นใจว่ากฎหมายจะถูกบังคับใช้จริง

- **โทษทางแพ่ง** เน้นการเยียวยาผู้เสียหาย โดยศาลสั่งให้ชดใช้ค่าสินไหมทดแทนตามจริง และอาจสั่งให้จ่าย "ค่าสินไหมเชิงลงโทษ" เพิ่มขึ้นอีกไม่เกิน ๒ ของค่าเสียหายจริง เพื่อเป็นการดัดนิสัยหน่วยงานที่ละเลย

- **โทษทางปกครอง** เป็นเงินค่าปรับที่จ่ายให้แก่รัฐ มีตั้งแต่ ๑ ล้านถึง ๕ ล้านบาท ขึ้นอยู่กับความร้ายแรง

- **โทษทางอาญา** เป็นกรณีที่ร้ายแรงที่สุด เช่น การเปิดเผยข้อมูลอ่อนไหวโดยทุจริต หรือมุ่งหวังให้ผู้อื่นได้รับความอับอาย/เสียชื่อเสียง มีโทษจำคุกสูงสุด ๑ ปี และปรับสูงสุด ๑ ล้านบาท ที่สำคัญคือ หากผู้กระทำความผิดเป็นนิติบุคคล (บริษัท) "กรรมการหรือบุคคลที่รับผิดชอบ" ในการดำเนินงานของบริษัทนั้น ๆ อาจต้องรับโทษจำคุกร่วมด้วย หากพิสูจน์ได้ว่าความผิดเกิดจากการสั่งการหรือการละเว้นการสั่งการของตน

**๖. กลไกการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ**

เมื่อเจ้าของข้อมูลรู้สึกว่าถูกละเมิด หรือไม่สามารถใช้สิทธิตามข้อ ๔ ได้ (เช่น ขอเข้าถึงข้อมูลแล้วถูกปฏิเสธโดยไม่มีเหตุผล) ขั้นตอนแรกคือการร้องเรียนไปยังผู้ควบคุมข้อมูลนั้น ๆ ก่อน หากไม่ได้รับการแก้ไข จึงจะเข้าสู่กลไกการร้องเรียนต่อ คณะกรรมการผู้เชี่ยวชาญ ภายใต้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) คณะกรรมการจะทำหน้าที่ตรวจสอบข้อเท็จจริง ไกล่เกลี่ยข้อพิพาท และมีอำนาจสั่งการให้ผู้ควบคุมข้อมูลดำเนินการอย่างใดอย่างหนึ่ง เช่น สั่งให้ลบข้อมูล หรือสั่งให้จ่ายค่าปรับทางปกครอง การร้องเรียนสามารถทำได้ผ่านช่องทางออนไลน์หรือมายื่นด้วยตนเอง ซึ่งเป็นกลไกที่ช่วยให้ประชาชนเข้าถึงความยุติธรรมได้ง่ายขึ้น โดยไม่ต้องเสียค่าใช้จ่ายในการจ้างทนายความฟ้องศาลในเบื้องต้น และคำสั่งของคณะกรรมการถือเป็นคำสั่งทางปกครองที่ต้องปฏิบัติตาม

**๗. การปฏิบัติเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Notification)**

ในโลกไซเบอร์ไม่มีระบบใดปลอดภัย ๑๐๐% กฎหมายจึงเน้นที่ "การจัดการหลังเกิดเหตุ" เมื่อเกิดเหตุข้อมูลรั่วไหล (Data Breach) องค์กรต้องรีบประเมินความเสี่ยงทันที หากพบว่ามีความเสี่ยงต่อเจ้าของข้อมูลต้องแจ้งเหตุให้ สคส. ทราบภายใน ๗๒ ชั่วโมง เพื่อให้เจ้าหน้าที่รัฐเข้ามาประคองสถานการณ์ หากประเมินแล้วพบว่ามีความเสี่ยงสูงมาก (High Risk) เช่น ข้อมูลเลขบัตรประชาชนและเลขหลังบัตรหลุดไป ซึ่งอาจนำไปสู่การสวมรอยทำธุรกรรม องค์กรต้องแจ้ง "เจ้าของข้อมูล" ทุกคนทราบโดยเร็วที่สุด พร้อมทั้งบอกวิธีที่เจ้าของข้อมูลควรทำเพื่อป้องกันตัวเอง (เช่น แนะนำให้ไปเปลี่ยนรหัสผ่าน หรืออายัดบัตร) การซ่อนเร้นความผิดหรือการไม่แจ้งเหตุถือเป็นความผิดร้ายแรงตามกฎหมาย การแจ้งเตือนที่รวดเร็วจะช่วยลดความเสียหายจากการถูกนำข้อมูลไปใช้ในทางมิชอบได้มหาศาล

**๘. บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

DPO คือ "ตัวกลาง" และ "ที่ปรึกษา" ที่กฎหมายบังคับให้หน่วยงานรัฐทุกแห่ง และบริษัทเอกชนที่มีการประมวลผลข้อมูลจำนวนมากหรือข้อมูลอ่อนไหวต้องมี DPO ไม่ได้มีหน้าที่เข้าไปทำความสะอาดข้อมูลด้วยตัวเอง แต่มีบทบาทในการวางนโยบาย ให้คำแนะนำแก่พนักงานในองค์กรว่าการทำแคมเปญการตลาดแบบนี้เสี่ยงผิดกฎหมายหรือไม่ และเป็นผู้ประสานงานหลักเมื่อมีเจ้าของข้อมูลมาใช้สิทธิ หรือเมื่อต้องติดต่อกับ สคส. กฎหมายกำหนดให้ DPO ต้องมีความเป็นอิสระในการปฏิบัติหน้าที่ (ไม่ถูกไล่ออกเพียงเพราะรายงานว่าบริษัททำผิดกฎหมาย) และผู้บริหารต้องสนับสนุนทรัพยากรให้ DPO ทำงานได้จริง การมี DPO ที่เข้มแข็งจะช่วยให้องค์กรสร้างวัฒนธรรม "Privacy by Design" หรือการคำนึงถึงความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบระบบหรือบริการใหม่ ๆ ไม่ใช่มาแก้ไขภายหลังซึ่งจะมีต้นทุนสูงกว่า

**๙. กลไกการคุ้มครองข้อมูลส่วนบุคคลของ สคส. (PDPC)**

สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) ทำหน้าที่เป็น Regulators หรือ "ตำรวจข้อมูล" ของประเทศไทย กลไกของ สคส. ไม่ได้เน้นแค่การลงโทษ แต่เน้นที่การสร้างระบบนิเวศ (Ecosystem) ของการคุ้มครองข้อมูล เช่น การออกกฎหมายลำดับรองเพื่อขยายความให้ชัดเจน (เช่น มาตรฐานความปลอดภัยขั้นต่ำที่บริษัทต้องมีคืออะไร) การสร้างมาตรฐานความร่วมมือกับหน่วยงานกำกับดูแลอื่น ๆ เช่น แบงก์ชาติ หรือ กสทช. นอกจากนี้ สคส. ยังมีหน้าที่ส่งเสริมความรู้ (Digital Literacy) ให้ประชาชนรู้เท่าทันสิทธิ์ของตนเอง และส่งเสริมให้ภาคธุรกิจมีแนวปฏิบัติที่ดี (Code of Practice) เพื่อให้การคุ้มครองข้อมูลเป็นมาตรฐานเดียวกันทั้งประเทศ กลไกเหล่านี้มุ่งหวังจะทำให้ประเทศไทยเป็นที่ยอมรับในระดับสากลว่ามีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ เพื่อประโยชน์ในการไหลเวียนของข้อมูลข้ามพรมแดนและการดึงดูดการลงทุนจากต่างประเทศ

ในยุคดิจิทัลปัจจุบันที่เทคโนโลยีก้าวหน้าอย่างรวดเร็ว การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้อย่างง่ายดายและรวดเร็ว ซึ่งนำมาสู่การละเมิดสิทธิความเป็นส่วนตัวที่สร้างความเดือดร้อนรำคาญและความเสียหายให้แก่เจ้าของข้อมูลจำนวนมาก อีกทั้งยังส่งผลกระทบในเชิงลบต่อระบบเศรษฐกิจโดยรวม ด้วยเหตุนี้ การมีหลักเกณฑ์และมาตรการกำกับดูแลที่ชัดเจนจึงกลายเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อสร้างความเชื่อมั่นว่าข้อมูลส่วนบุคคลจะได้รับการจัดการอย่างถูกต้องและปลอดภัย การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้เป็นเพียงการปกป้องสิทธิขั้นพื้นฐานของบุคคลเท่านั้น แต่ยังเป็นกลไกสำคัญในการสร้างมาตรฐานและมาตรการเยียวยาที่มีประสิทธิภาพเมื่อเกิดการละเมิดสิทธิขึ้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและเป็นที่ยอมรับในระดับสากล แนวทางของ OECD (Organisation for Economic Co-operation and Development) ได้กำหนดหลักการสำคัญ ๘ ประการ ซึ่งได้กลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงเป็นหัวใจสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยด้วย

**หลักการคุ้มครองข้อมูลส่วนบุคคล ๘ ประการ**

หลักการทั้ง ๘ ประการนี้เป็นกรอบแนวปฏิบัติสากลที่ช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง โปร่งใส และเคารพต่อสิทธิของเจ้าของข้อมูล ซึ่งเป็นรากฐานสำคัญในการสร้างความไว้วางใจในระบบเศรษฐกิจดิจิทัล โดยมีรายละเอียดดังนี้

**๒.๑ หลักการจำกัดการเก็บรวบรวม (Data Minimization)**

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

**๒.๒ หลักการระบุวัตถุประสงค์อย่างชัดเจน (Purpose Specification)**

ผู้ควบคุมข้อมูล (องค์กรที่เก็บข้อมูล) มีหน้าที่ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจน *ก่อนหรือในขณะที่ทำการเก็บรวบรวม* ข้อมูลนั้นๆ การไม่แจ้งวัตถุประสงค์ถือเป็นความผิดและมีโทษปรับทางปกครองตามกฎหมาย หลักการนี้สร้างความโปร่งใสและทำให้เจ้าของข้อมูลตัดสินใจได้ว่าจะให้ข้อมูลของตนหรือไม่

**๒.๓ หลักการคุณภาพของข้อมูล (Data Quality)**

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

**๒.๔ หลักการจำกัดการใช้งาน (Use Limitation)**

การนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยจะต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ตั้งแต่แรกเท่านั้น หากต้องการนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่แจ้งไว้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเสมอ หรือต้องเป็นกรณีที่มีข้อยกเว้นตามที่กฎหมายกำหนด

**ตัวอย่าง:** โรงพยาบาลที่เก็บข้อมูลประวัติการรักษาของผู้ป่วยเพื่อใช้ในการวินิจฉัยและรักษาพยาบาลจะไม่สามารถนำข้อมูลสุขภาพดังกล่าวไปเปิดเผยให้กับบริษัทประกันภัยเพื่อเสนอขายผลิตภัณฑ์โดยไม่ได้รับความยินยอมที่ชัดเจนจากผู้ป่วยก่อน

**๒.๕ หลักการรักษาความปลอดภัย (Security Safeguards)**

ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมและได้มาตรฐาน เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยมาตรการดังกล่าวต้องธำรงไว้ซึ่งองค์ประกอบ ๓ ด้านหลัก ได้แก่

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

**ตัวอย่าง:** องค์กรควรมีมาตรการรักษาความปลอดภัยทั้งทางเทคนิค เช่น การเข้ารหัสข้อมูล (Encryption) และการจำกัดสิทธิ์การเข้าถึง (Access Control), และมาตรการเชิงบริหารจัดการ เช่น การจัดอบรมบุคลากรเรื่องความปลอดภัยของข้อมูล และการกำหนดนโยบายโต๊ะสะอาด (Clean Desk Policy) เพื่อป้องกันการเข้าถึงเอกสารสำคัญโดยไม่ได้รับอนุญาต

**๒.๖ หลักการจำกัดระยะเวลาการจัดเก็บ (Storage Limitation)**

ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลที่ชัดเจน และต้องมีระบบตรวจสอบเพื่อ ลบหรือทำลาย ข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาดังกล่าว หรือเมื่อข้อมูลนั้นหมดความจำเป็นตามวัตถุประสงค์ที่ได้เก็บรวบรวมมาแล้ว

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

**๒.๗ หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation)**

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและควบคุมข้อมูลของตนเอง ซึ่งรวมถึงสิทธิสำคัญหลายประการ เช่น:

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

**ตัวอย่าง:** ผู้ใช้งานแพลตฟอร์มโซเชียลมีเดียมีสิทธิขอดูข้อมูลทั้งหมดที่แพลตฟอร์มเก็บรวบรวมเกี่ยวกับตนเอง (เช่น ประวัติการโพสต์, ข้อมูลโปรไฟล์) และมีสิทธิร้องขอให้ลบบัญชีและข้อมูลที่เกี่ยวข้องทั้งหมดออกจากระบบได้

**๒.๘ หลักการความรับผิดชอบ (Accountability)**

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบในการปฏิบัติตามหลักการและมาตรการต่างๆ ที่กฎหมายกำหนดอย่างเคร่งครัด และต้องสามารถแสดงหลักฐานหรือพิสูจน์ให้เห็นถึงการปฏิบัติตามกฎหมายได้อย่างเป็นรูปธรรม หลักการนี้เป็นเครื่องยืนยันว่าการคุ้มครองข้อมูลจะเกิดขึ้นจริงในทางปฏิบัติ

**ตัวอย่าง** หากเกิดเหตุข้อมูลลูกค้ารั่วไหลออกจากระบบของบริษัท บริษัทที่เป็นผู้ควบคุมข้อมูลต้องมีหน้าที่รับผิดชอบในการแจ้งเหตุให้เจ้าของข้อมูลที่ได้รับผลกระทบและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยเร็ว พร้อมทั้งมีมาตรการตรวจสอบและเยียวยาความเสียหายที่เกิดขึ้น

การปฏิบัติตามหลักการทั้ง ๘ ประการนี้อย่างครบถ้วน จะช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีธรรมาภิบาลและสร้างความน่าเชื่อถือให้กับองค์กร

**ตารางสรุปหลักการ ๘ ประการ**

เพื่อทบทวนความเข้าใจ สามารถสรุปหัวใจสำคัญของแต่ละหลักการได้ดังตารางต่อไปนี้

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

ตารางนี้เป็นเครื่องมือช่วยจำที่ทำให้เห็นภาพรวมของกรอบการคุ้มครองข้อมูลส่วนบุคคลได้อย่างรวดเร็ว

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

**๓. ประโยชน์ที่ได้รับจากการฝึกอบรม**

**๓.๑ ต่อตนเอง** ช่วยสร้างความตระหนักรู้ (Awareness) และความเข้าใจที่ถูกต้องเกี่ยวกับสิทธิหน้าที่ตามกฎหมาย PDPA ทำให้สามารถปกป้องข้อมูลส่วนบุคคลของตนเองจากการถูกละเมิดในชีวิตประจำวันได้ นอกจากนี้ยังเป็นการเพิ่มทักษะความเชี่ยวชาญในการจัดการข้อมูลอย่างเป็นระบบ ซึ่งเป็นทักษะที่สำคัญอย่างยิ่งในยุคเศรษฐกิจดิจิทัล ทำให้มีความมั่นใจในการตัดสินใจเมื่อต้องทำหน้าที่เกี่ยวข้องกับการเก็บรวมรวมหรือส่งต่อข้อมูลส่วนบุคคล ไม่ต้องกังวลเรื่องการทำผิดกฎหมายโดยไม่ได้ตั้งใจ

**๓.๒ ต่อองค์กร** ช่วยลดความเสี่ยงจากการถูกฟ้องร้องหรือถูกลงโทษตามกฎหมาย ซึ่งมีโทษปรับที่สูงมาก การที่บุคลากรมีความรู้จะช่วยสร้างภาพลักษณ์ความน่าเชื่อถือ (Trust) ให้กับหน่วยงานว่าเป็นองค์กรที่มีมาตรฐานสากลในการจัดการข้อมูลผู้รับบริการ ช่วยให้กระบวนการทำงานภายในมีความเป็นระเบียบ ลดการเก็บข้อมูลที่ซ้ำซ้อนหรือไม่จำเป็น ซึ่งนำไปสู่การบริหารจัดการทรัพยากรสารสนเทศที่มีประสิทธิภาพมากขึ้น และสร้างความพึงพอใจให้กับผู้มีส่วนได้ส่วนเสียด้วยเช่นกัน

**๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการฝึกอบรมครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน**

**การทบทวนและปรับปรุงเอกสาร** เริ่มจากการสำรวจแบบฟอร์มการขอข้อมูลต่างๆ ในหน่วยงาน เพื่อจัดทำหรือปรับปรุง "ประกาศนโยบายความเป็นส่วนตัว" (Privacy Notice) ให้ชัดเจนตามหลักกฎหมาย โดยระบุวัตถุประสงค์และระยะเวลาการจัดเก็บที่แน่นอน

**การพัฒนาระบบการจัดเก็บข้อมูล** นำหลักการ "Privacy by Design" มาใช้ในการออกแบบระบบงานใหม่ๆ โดยจำกัดสิทธิ์การเข้าถึงข้อมูล (Access Control) ให้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น และตรวจสอบว่ามีการทำลายข้อมูลเมื่อสิ้นสุดระยะเวลาที่จำเป็น

**การถ่ายทอดองค์ความรู้** จัดกิจกรรมแบ่งปันความรู้ (Knowledge Sharing) ให้กับเพื่อนร่วมงานในแผนก เพื่อให้เกิดแนวปฏิบัติที่ตรงกันทั้งองค์กร และช่วยกันเฝ้าระวังไม่ให้เกิดเหตุการณ์ข้อมูลรั่วไหล เช่น การไม่วางเอกสารที่มีข้อมูลส่วนบุคคลทิ้งไว้บนโต๊ะทำงาน หรือการระมัดระวังการส่งข้อมูลผ่านช่องทางที่ไม่ปลอดภัย อย่าง LINE หรือ Messenger โดยไม่จำเป็น

**๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน**

**ความซับซ้อนของขั้นตอนการทำงาน** การต้องขอความยินยอมหรือแจ้งรายละเอียดที่เพิ่มขึ้น อาจทำให้ผู้รับบริการรู้สึกว่าขั้นตอนยุ่งยากขึ้น หรือทำให้เจ้าหน้าที่ต้องใช้เวลาในการอธิบายมากขึ้น ซึ่งอาจส่งผลต่อความรวดเร็วในการให้บริการในระยะแรก

**ข้อจำกัดทางเทคโนโลยี** ระบบฐานข้อมูลเดิมของหน่วยงาน (Legacy System) อาจไม่ได้ออกแบบมาเพื่อรองรับการลบข้อมูลเป็นรายบุคคล หรือการจำกัดสิทธิ์การเข้าถึงที่ละเอียดพอ ทำให้การปรับปรุงระบบต้องใช้เวลาและงบประมาณสูง

**ความเคยชินและวัฒนธรรมองค์กร** การปรับเปลี่ยนพฤติกรรมการทำงานที่เคยปฏิบัติมานาน เช่น การส่งไฟล์ข้อมูลผ่านโซเชียลมีเดียเพื่อความสะดวก อาจได้รับการต่อต้านจากบุคลากรบางส่วนที่มองว่าเป็นการเพิ่มภาระงาน หรือมองว่ากฎหมายมีความยุ่งยากเกินความจำเป็นในการปฏิบัติงานจริง

**๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล**

**ด้านนโยบายและทรัพยากร** ต้องการให้ผู้บังคับบัญชากำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้เป็นวาระสำคัญของหน่วยงาน และสนับสนุนงบประมาณในการปรับปรุงเครื่องมือ อุปกรณ์ หรือซอฟต์แวร์ที่ช่วยในการรักษาความปลอดภัยของข้อมูลให้ทันสมัย

**ด้านการบริหารจัดการ** การจัดตั้งทีมงานหรือแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ที่ชัดเจน เพื่อให้มีที่ปรึกษาเมื่อเกิดข้อสงสัยในการปฏิบัติงาน รวมถึงการสนับสนุนให้มีการอบรมทบทวนความรู้เป็นระยะๆ เนื่องจากแนวปฏิบัติทางกฎหมายอาจมีการเปลี่ยนแปลง

**การเป็นแบบอย่างที่ดี** ควรให้ความสำคัญและปฏิบัติตามหลักการ PDPA อย่างเคร่งครัด เพื่อสร้างวัฒนธรรมองค์กรที่เคารพในความเป็นส่วนตัว ซึ่งจะช่วยสร้างขวัญและกำลังใจให้พนักงานระดับปฏิบัติการกล้าที่จะเปลี่ยนแปลงกระบวนการทำงานให้ถูกต้องตามกฎหมาย

จึงเรียนมาเพื่อโปรดทราบ

(ลงชื่อ) .....

( นายคำรณ จันทร์ต้น )

ผู้เข้ารับการฝึกอบรม

# สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณคำรณ จันทร์ต้น

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 2 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งชำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680402668

# สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า**

## คุณคำรณ จันทร์ต้น

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 2 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680402668

**แบบรายงานผลการเข้ารับการฝึกอบรม/สัมมนา**

ด้วยข้าพเจ้า นางสาวศจิษฐา รีรักษ์ ตำแหน่ง นักวิชาการสาธารณสุขชำนาญการ โรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังทอง สังกัด กองสาธารณสุขและสิ่งแวดล้อม ได้เข้าร่วมโครงการอบรมเชิงปฏิบัติการหลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป (e-learning) ในวันที่ ๒ ธันวาคม พ.ศ.๒๕๖๘ นั้น

บัดนี้ ข้าพเจ้าได้เข้ารับการฝึกอบรมหลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการฝึกอบรมให้ทราบ ดังนี้

**๑. การฝึกอบรมดังกล่าวมีวัตถุประสงค์เพื่อ**

ให้ประชาชนตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ซึ่งเป็นสิทธิขั้นพื้นฐานในความเป็นส่วนตัว (Right to Privacy) เพื่อป้องกันการละเมิดสิทธิที่อาจก่อให้เกิดความเดือดร้อนรำคาญหรือความเสียหายแก่เจ้าของข้อมูล โดยเฉพาะในยุคที่เทคโนโลยีทำให้การเก็บรวบรวมและใช้ข้อมูลทำได้ง่ายและรวดเร็ว ทั้งนี้ เพื่อให้มีมาตรการเยียวยาที่มีประสิทธิภาพและสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์และเศรษฐกิจดิจิทัล

**๒. เนื้อหาและหัวข้อวิชาของหลักสูตรการฝึกอบรม มีดังนี้**

| บทที่ | เนื้อหาหลักสูตร |
|---|---|
| ๑ | ความสำคัญ แนวคิด ขอบเขตการคุ้มครองข้อมูลส่วนบุคคล ความหมาย ประเภทของข้อมูล และกฎหมายอื่นๆ |
| ๒ | หลักการคุ้มครองข้อมูลส่วนบุคคล |
| ๓ | ฐานทางกฎหมายในการเก็บรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล |
| ๔ | สิทธิของเจ้าของข้อมูลส่วนบุคคล |
| ๕ | ความรับผิดและบทกำหนดโทษ |
| ๖ | กลไกการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ |
| ๗ | การปฏิบัติเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล |
| ๘ | บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล |
| ๙ | กลโกการคุ้มครองข้อมูลส่วนบุคคลของ สคส. |

**สรุปโครงการอบรมเชิงปฏิบัติการหลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป (e-learning)**

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

**๑. ความสำคัญ แนวคิด ขอบเขต และประเภทของข้อมูล**

แนวคิดหลักของ PDPA คือการให้ "อำนาจ" แก่เจ้าของข้อมูลในการควบคุมข้อมูลของตนเอง ในยุคที่ข้อมูลถูกนำไปใช้ในเชิงพาณิชย์และอาชญากรรมไซเบอร์ ข้อมูลส่วนบุคคลเปรียบเสมือนทรัพย์สินที่ต้องการการล้อมรั้วป้องกัน ขอบเขตของกฎหมายนี้ครอบคลุมทั้งหน่วยงานรัฐและเอกชน ไม่ว่าจะเป็นการเก็บข้อมูลในรูปแบบกระดาษหรือดิจิทัล หากข้อมูลนั้นสามารถระบุตัวตนบุคคลที่ยังมีชีวิตอยู่ได้ (ไม่รวมผู้ถึงแก่กรรม) ถือเป็นข้อมูลส่วนบุคคลทั้งสิ้น ประเภทข้อมูลแบ่งเป็น ๒ ระดับหลัก คือ ข้อมูลทั่วไป (ชื่อ, ที่อยู่, IP Address) และข้อมูลอ่อนไหว (Sensitive Data) ซึ่งประเภทหลังนี้มีความสำคัญมาก เพราะหากรั่วไหลอาจนำไปสู่การเลือกปฏิบัติหรือกระทบต่อศักดิ์ศรีความเป็นมนุษย์ เช่น ข้อมูลสหภาพแรงงาน รสนิยมทางเพศ หรือข้อมูลชีวภาพ (ใบหน้า, ลายนิ้วมือ) การเก็บข้อมูลประเภทนี้จึงต้องได้รับความยินยอมโดยชัดแจ้งและมีมาตรฐานความปลอดภัยที่สูงกว่าปกติ นอกจากนี้ PDPA ยังเชื่อมโยงกับกฎหมายอื่น เช่น พ.ร.บ. ไซเบอร์ฯ เพื่อสร้างโครงสร้างพื้นฐานด้านความปลอดภัยที่ครอบคลุมทั้งประเทศ

**๒. หลักการคุ้มครองข้อมูลส่วนบุคคล (Principles)**

หลักการพื้นฐานที่ผู้ควบคุมข้อมูลต้องยึดถือประกอบด้วย ๓ ส่วนสำคัญคือ

๑. การเก็บรวบรวมอย่างจำกัด (Data Minimization) คือการเก็บเท่าที่ "จำเป็น" จริง ๆ ภายใต้วัตถุประสงค์ที่แจ้งไว้ เช่น หากสมัครสมาชิกร้านอาหาร ไม่จำเป็นต้องขอเลขบัตรประชาชน

๒. ความถูกต้องของข้อมูล ผู้เก็บต้องตรวจสอบให้ข้อมูลทันสมัยและไม่ทำให้เกิดความเข้าใจผิด

๓. การจำกัดระยะเวลาการเก็บ (Storage Limitation) ต้องกำหนดชัดเจนว่าจะเก็บข้อมูลไว้นานแค่ไหน (เช่น ๑๐ ปีตามอายุความทางภาษี) และเมื่อพ้นกำหนดต้องทำลายทิ้งทันที หลักการเหล่านี้มีไว้เพื่อลดความเสี่ยง หากเกิดเหตุข้อมูลรั่วไหล ความเสียหายจะถูกจำกัดวงแคบเพราะเราไม่ได้เก็บข้อมูลที่ไม่จำเป็นไว้ตั้งแต่แรก นอกจากนี้ยังเน้นความโปร่งใสผ่าน "นโยบายความเป็นส่วนตัว" (Privacy Notice) ที่ต้องเขียนด้วยภาษาที่เข้าใจง่าย ไม่ใช้ภาษากฎหมายที่ซับซ้อนเกินไป เพื่อให้ประชาชนทราบว่าข้อมูลของตนจะถูกนำไปใช้อย่างไร ใครเป็นผู้รับข้อมูลต่อ และจะติดต่อผู้ควบคุมข้อมูลได้อย่างไร

**๓. ฐานทางกฎหมาย (Lawful Basis) ในการเก็บรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**

หลายคนเข้าใจผิดว่าต้องขอ "ความยินยอม" (Consent) ในทุกกรณี แต่ในความเป็นจริง Consent คือทางเลือกสุดท้ายหากไม่มีฐานอื่นรองรับ ฐานทางกฎหมายช่วยให้กิจกรรมทางเศรษฐกิจและสังคมดำเนินต่อไปได้ เช่น ฐานสัญญา: ธนาคารต้องเก็บที่อยู่คุณเพื่อส่งใบแจ้งหนี้โดยไม่ต้องขอความยินยอมซ้ำซ้อน

ฐานกฎหมาย นายจ้างต้องเก็บเลขผู้เสียภาษีของลูกจ้างเพื่อส่งกรมสรรพากร

ฐานประโยชน์สาธารณะ: หน่วยงานรัฐเก็บข้อมูลเพื่อสวัสดิการแห่งรัฐ

ฐานประโยชน์อันชอบธรรม: การติดกล้อง CCTV เพื่อความปลอดภัยในอาคาร (แต่ต้องติดป้ายแจ้ง)

ฐานระงับอันตรายต่อชีวิต: เช่น กรณีอุบัติเหตุฉุกเฉิน แพทย์สามารถเข้าถึงประวัติการแพ้ยาได้ทันทีโดยไม่ต้องรอขอความยินยอม

การเลือกใช้ฐานที่ถูกต้องมีความสำคัญมาก เพราะหากองค์กรอ้างฐาน Consent แล้วภายหลังเจ้าของข้อมูลถอนความยินยอม องค์กรนั้นอาจต้องหยุดกิจกรรมทันที แต่หากอ้างฐานอื่น เช่น ฐานกฎหมาย แม้เจ้าของข้อมูลจะไม่พอใจ องค์กรก็ยังมีสิทธิเก็บข้อมูลนั้นไว้ได้ตามที่กฎหมายกำหนด

**๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)**

สิทธิเหล่านี้คือเครื่องมือที่ประชาชนใช้ตรวจสอบและควบคุมข้อมูลของตนเอง เริ่มตั้งแต่

- สิทธิขอเข้าถึง (Right of Access) คุณสามารถเดินไปถามธนาคารหรือแอปพลิเคชันได้ว่า "คุณมีข้อมูลอะไรของฉันบ้าง และเอาไปให้ใครดูบ้าง?" โดยองค์กรต้องตอบกลับภายใน ๓๐ วัน

- สิทธิขอให้ลบ (Right to Erasure) หรือ "สิทธิที่จะถูกลืม" (Right to be forgotten) ใช้ได้เมื่อข้อมูลนั้นหมดความจำเป็นหรือได้มาโดยไม่ชอบ

- สิทธิขอให้โอนย้ายข้อมูล (Right to Data Portability) เช่น คุณต้องการย้ายข้อมูลประกันชีวิตจากบริษัท A ไปบริษัท B ในรูปแบบที่คอมพิวเตอร์อ่านได้ เพื่อความสะดวกในการเปรียบเทียบเบี้ยประกัน

- สิทธิคัดค้าน (Right to Object) โดยเฉพาะการนำข้อมูลไปใช้เพื่อการตลาด (Direct Marketing) คุณมีสิทธิสั่งให้เขาหยุดโทรมาขายประกันได้ทันที การใช้สิทธิเหล่านี้เป็นรากฐานของการสร้างดุลอำนาจระหว่างปัจเจกบุคคลกับองค์กรขนาดใหญ่ เพื่อไม่ให้ข้อมูลถูกนำไปใช้ในทางที่เจ้าของข้อมูลไม่ประสงค์

**๕. ความรับผิดและบทกำหนดโทษ**

PDPA มีบทลงโทษที่ครอบคลุมทุกมิติ เพื่อให้มั่นใจว่ากฎหมายจะถูกบังคับใช้จริง

- **โทษทางแพ่ง** เน้นการเยียวยาผู้เสียหาย โดยศาลสั่งให้ชดใช้ค่าสินไหมทดแทนตามจริง และอาจสั่งให้จ่าย "ค่าสินไหมเชิงลงโทษ" เพิ่มขึ้นอีกไม่เกิน ๒ ของค่าเสียหายจริง เพื่อเป็นการดัดนิสัยหน่วยงานที่ละเลย

- **โทษทางปกครอง** เป็นเงินค่าปรับที่จ่ายให้แก่รัฐ มีตั้งแต่ ๑ ล้านถึง ๕ ล้านบาท ขึ้นอยู่กับความร้ายแรง

- **โทษทางอาญา** เป็นกรณีที่ร้ายแรงที่สุด เช่น การเปิดเผยข้อมูลอ่อนไหวโดยทุจริต หรือมุ่งหวังให้ผู้อื่นได้รับความอับอาย/เสียชื่อเสียง มีโทษจำคุกสูงสุด ๑ ปี และปรับสูงสุด ๑ ล้านบาท ที่สำคัญคือ หากผู้กระทำความผิดเป็นนิติบุคคล (บริษัท) "กรรมการหรือบุคคลที่รับผิดชอบ" ในการดำเนินงานของบริษัทนั้น ๆ อาจต้องรับโทษจำคุกร่วมด้วย หากพิสูจน์ได้ว่าความผิดเกิดจากการสั่งการหรือการละเว้นการสั่งการของตน

**๖. กลไกการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ**

เมื่อเจ้าของข้อมูลรู้สึกว่าถูกละเมิด หรือไม่สามารถใช้สิทธิตามข้อ ๔ ได้ (เช่น ขอเข้าถึงข้อมูลแล้วถูกปฏิเสธโดยไม่มีเหตุผล) ขั้นตอนแรกคือการร้องเรียนไปยังผู้ควบคุมข้อมูลนั้น ๆ ก่อน หากไม่ได้รับการแก้ไข จึงจะเข้าสู่กลไกการร้องเรียนต่อ คณะกรรมการผู้เชี่ยวชาญ ภายใต้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) คณะกรรมการจะทำหน้าที่ตรวจสอบข้อเท็จจริง ไกล่เกลี่ยข้อพิพาท และมีอำนาจสั่งการให้ผู้ควบคุมข้อมูลดำเนินการอย่างใดอย่างหนึ่ง เช่น สั่งให้ลบข้อมูล หรือสั่งให้จ่ายค่าปรับทางปกครอง การร้องเรียนสามารถทำได้ผ่านช่องทางออนไลน์หรือมายื่นด้วยตนเอง ซึ่งเป็นกลไกที่ช่วยให้ประชาชนเข้าถึงความยุติธรรมได้ง่ายขึ้น โดยไม่ต้องเสียค่าใช้จ่ายในการจ้างทนายความฟ้องศาลในเบื้องต้น และคำสั่งของคณะกรรมการถือเป็นคำสั่งทางปกครองที่ต้องปฏิบัติตาม

**๗. การปฏิบัติเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Notification)**

ในโลกไซเบอร์ไม่มีระบบใดปลอดภัย ๑๐๐% กฎหมายจึงเน้นที่ "การจัดการหลังเกิดเหตุ" เมื่อเกิดเหตุข้อมูลรั่วไหล (Data Breach) องค์กรต้องรีบประเมินความเสี่ยงทันที หากพบว่ามีความเสี่ยงต่อเจ้าของข้อมูลต้องแจ้งเหตุให้ สคส. ทราบภายใน ๗๒ ชั่วโมง เพื่อให้เจ้าหน้าที่รัฐเข้ามาประคองสถานการณ์ หากประเมินแล้วพบว่ามีความเสี่ยงสูงมาก (High Risk) เช่น ข้อมูลเลขบัตรประชาชนและเลขหลังบัตรหลุดไป ซึ่งอาจนำไปสู่การสวมรอยทำธุรกรรม องค์กรต้องแจ้ง "เจ้าของข้อมูล" ทุกคนทราบโดยเร็วที่สุด พร้อมทั้งบอกวิธีที่เจ้าของข้อมูลควรทำเพื่อป้องกันตัวเอง (เช่น แนะนำให้ไปเปลี่ยนรหัสผ่าน หรืออายัดบัตร) การซ่อนเร้นความผิดหรือการไม่แจ้งเหตุถือเป็นความผิดร้ายแรงตามกฎหมาย การแจ้งเตือนที่รวดเร็วจะช่วยลดความเสียหายจากการถูกนำข้อมูลไปใช้ในทางมิชอบได้มหาศาล

**๘. บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

DPO คือ "ตัวกลาง" และ "ที่ปรึกษา" ที่กฎหมายบังคับให้หน่วยงานรัฐทุกแห่ง และบริษัทเอกชนที่มีการประมวลผลข้อมูลจำนวนมากหรือข้อมูลอ่อนไหวต้องมี DPO ไม่ได้มีหน้าที่เข้าไปทำความสะอาดข้อมูลด้วยตัวเอง แต่มีบทบาทในการวางนโยบาย ให้คำแนะนำแก่พนักงานในองค์กรว่าการทำแคมเปญการตลาดแบบนี้เสี่ยงผิดกฎหมายหรือไม่ และเป็นผู้ประสานงานหลักเมื่อมีเจ้าของข้อมูลมาใช้สิทธิ หรือเมื่อต้องติดต่อกับ สคส. กฎหมายกำหนดให้ DPO ต้องมีความเป็นอิสระในการปฏิบัติหน้าที่ (ไม่ถูกไล่ออกเพียงเพราะรายงานว่าบริษัททำผิดกฎหมาย) และผู้บริหารต้องสนับสนุนทรัพยากรให้ DPO ทำงานได้จริง การมี DPO ที่เข้มแข็งจะช่วยให้องค์กรสร้างวัฒนธรรม "Privacy by Design" หรือการคำนึงถึงความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบระบบหรือบริการใหม่ ๆ ไม่ใช่มาแก้ไขภายหลังซึ่งจะมีต้นทุนสูงกว่า

**๙. กลไกการคุ้มครองข้อมูลส่วนบุคคลของ สคส. (PDPC)**

สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) ทำหน้าที่เป็น Regulators หรือ "ตำรวจข้อมูล" ของประเทศไทย กลไกของ สคส. ไม่ได้เน้นแค่การลงโทษ แต่เน้นที่การสร้างระบบนิเวศ (Ecosystem) ของการคุ้มครองข้อมูล เช่น การออกกฎหมายลำดับรองเพื่อขยายความให้ชัดเจน (เช่น มาตรฐานความปลอดภัยขั้นต่ำที่บริษัทต้องมีคืออะไร) การสร้างมาตรฐานความร่วมมือกับหน่วยงานกำกับดูแลอื่น ๆ เช่น แบงก์ชาติ หรือ กสทช. นอกจากนี้ สคส. ยังมีหน้าที่ส่งเสริมความรู้ (Digital Literacy) ให้ประชาชนรู้เท่าทันสิทธิ์ของตนเอง และส่งเสริมให้ภาคธุรกิจมีแนวปฏิบัติที่ดี (Code of Practice) เพื่อให้การคุ้มครองข้อมูลเป็นมาตรฐานเดียวกันทั้งประเทศ กลไกเหล่านี้มุ่งหวังจะทำให้ประเทศไทยเป็นที่ยอมรับในระดับสากลว่ามีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ เพื่อประโยชน์ในการไหลเวียนของข้อมูลข้ามพรมแดนและการดึงดูดการลงทุนจากต่างประเทศ

ในยุคดิจิทัลปัจจุบันที่เทคโนโลยีก้าวหน้าอย่างรวดเร็ว การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้อย่างง่ายดายและรวดเร็ว ซึ่งนำมาสู่การละเมิดสิทธิความเป็นส่วนตัวที่สร้างความเดือดร้อนรำคาญและความเสียหายให้แก่เจ้าของข้อมูลจำนวนมาก อีกทั้งยังส่งผลกระทบในเชิงลบต่อระบบเศรษฐกิจโดยรวม ด้วยเหตุนี้ การมีหลักเกณฑ์และมาตรการกำกับดูแลที่ชัดเจนจึงกลายเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อสร้างความเชื่อมั่นว่าข้อมูลส่วนบุคคลจะได้รับการจัดการอย่างถูกต้องและปลอดภัย การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้เป็นเพียงการปกป้องสิทธิขั้นพื้นฐานของบุคคลเท่านั้น แต่ยังเป็นกลไกสำคัญในการสร้างมาตรฐานและมาตรการเยียวยาที่มีประสิทธิภาพเมื่อเกิดการละเมิดสิทธิขึ้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและเป็นที่ยอมรับในระดับสากล แนวทางของ OECD (Organisation for Economic Co-operation and Development) ได้กำหนดหลักการสำคัญ ๘ ประการ ซึ่งได้กลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงเป็นหัวใจสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยด้วย

**หลักการคุ้มครองข้อมูลส่วนบุคคล ๘ ประการ**

หลักการทั้ง ๘ ประการนี้เป็นกรอบแนวปฏิบัติสากลที่ช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง โปร่งใส และเคารพต่อสิทธิของเจ้าของข้อมูล ซึ่งเป็นรากฐานสำคัญในการสร้างความไว้วางใจในระบบเศรษฐกิจดิจิทัล โดยมีรายละเอียดดังนี้

**๒.๑ หลักการจำกัดการเก็บรวบรวม (Data Minimization)**

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

**๒.๒ หลักการระบุวัตถุประสงค์อย่างชัดเจน (Purpose Specification)**

ผู้ควบคุมข้อมูล (องค์กรที่เก็บข้อมูล) มีหน้าที่ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจน *ก่อนหรือในขณะที่ทำการเก็บรวบรวม* ข้อมูลนั้นๆ การไม่แจ้งวัตถุประสงค์ถือเป็นความผิดและมีโทษปรับทางปกครองตามกฎหมาย หลักการนี้สร้างความโปร่งใสและทำให้เจ้าของข้อมูลตัดสินใจได้ว่าจะให้ข้อมูลของตนหรือไม่

**๒.๓ หลักการคุณภาพของข้อมูล (Data Quality)**

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

**๒.๔ หลักการจำกัดการใช้งาน (Use Limitation)**

การนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยจะต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ตั้งแต่แรกเท่านั้น หากต้องการนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่แจ้งไว้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเสมอ หรือต้องเป็นกรณีที่มีข้อยกเว้นตามที่กฎหมายกำหนด

**ตัวอย่าง:** โรงพยาบาลที่เก็บข้อมูลประวัติการรักษาของผู้ป่วยเพื่อใช้ในการวินิจฉัยและรักษาพยาบาล จะไม่สามารถนำข้อมูลสุขภาพดังกล่าวไปเปิดเผยให้กับบริษัทประกันภัยเพื่อเสนอขายผลิตภัณฑ์โดยไม่ได้รับความยินยอมที่ชัดเจนจากผู้ป่วยก่อน

**๒.๕ หลักการรักษาความปลอดภัย (Security Safeguards)**

ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมและได้มาตรฐาน เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยมาตรการดังกล่าวต้องธำรงไว้ซึ่งองค์ประกอบ ๓ ด้านหลัก ได้แก่

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

**ตัวอย่าง:** องค์กรควรมีมาตรการรักษาความปลอดภัยทั้งทางเทคนิค เช่น การเข้ารหัสข้อมูล (Encryption) และการจำกัดสิทธิ์การเข้าถึง (Access Control), และมาตรการเชิงบริหารจัดการ เช่น การจัดอบรมบุคลากรเรื่องความปลอดภัยของข้อมูล และการกำหนดนโยบายโต๊ะสะอาด (Clean Desk Policy) เพื่อป้องกันการเข้าถึงเอกสารสำคัญโดยไม่ได้รับอนุญาต

**๒.๖ หลักการจำกัดระยะเวลาการจัดเก็บ (Storage Limitation)**

ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลที่ชัดเจน และต้องมีระบบตรวจสอบเพื่อ ลบหรือทำลาย ข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาดังกล่าว หรือเมื่อข้อมูลนั้นหมดความจำเป็นตามวัตถุประสงค์ที่ได้เก็บรวบรวมมาแล้ว

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

**๒.๗ หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation)**

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและควบคุมข้อมูลของตนเอง ซึ่งรวมถึงสิทธิสำคัญหลายประการ เช่น:

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

**ตัวอย่าง:** ผู้ใช้งานแพลตฟอร์มโซเชียลมีเดียมีสิทธิขอดูข้อมูลทั้งหมดที่แพลตฟอร์มเก็บรวบรวมเกี่ยวกับตนเอง (เช่น ประวัติการโพสต์, ข้อมูลโปรไฟล์) และมีสิทธิร้องขอให้ลบบัญชีและข้อมูลที่เกี่ยวข้องทั้งหมดออกจากระบบได้

**๒.๘ หลักการความรับผิดชอบ (Accountability)**

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบในการปฏิบัติตามหลักการและมาตรการต่างๆ ที่กฎหมายกำหนดอย่างเคร่งครัด และต้องสามารถแสดงหลักฐานหรือพิสูจน์ให้เห็นถึงการปฏิบัติตามกฎหมายได้อย่างเป็นรูปธรรม หลักการนี้เป็นเครื่องยืนยันว่าการคุ้มครองข้อมูลจะเกิดขึ้นจริงในทางปฏิบัติ

**ตัวอย่าง** หากเกิดเหตุข้อมูลลูกค้ารั่วไหลออกจากระบบของบริษัท บริษัทที่เป็นผู้ควบคุมข้อมูลต้องมีหน้าที่รับผิดชอบในการแจ้งเหตุให้เจ้าของข้อมูลที่ได้รับผลกระทบและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยเร็ว พร้อมทั้งมีมาตรการตรวจสอบและเยียวยาความเสียหายที่เกิดขึ้น

การปฏิบัติตามหลักการทั้ง ๘ ประการนี้อย่างครบถ้วน จะช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีธรรมาภิบาลและสร้างความน่าเชื่อถือให้กับองค์กร

**ตารางสรุปหลักการ ๘ ประการ**

เพื่อทบทวนความเข้าใจ สามารถสรุปหัวใจสำคัญของแต่ละหลักการได้ดังตารางต่อไปนี้

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

ตารางนี้เป็นเครื่องมือช่วยจำที่ทำให้เห็นภาพรวมของกรอบการคุ้มครองข้อมูลส่วนบุคคลได้อย่างรวดเร็ว

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

**๓. ประโยชน์ที่ได้รับจากการฝึกอบรม**

**๓.๑ ต่อตนเอง** ช่วยสร้างความตระหนักรู้ (Awareness) และความเข้าใจที่ถูกต้องเกี่ยวกับสิทธิหน้าที่ตามกฎหมาย PDPA ทำให้สามารถปกป้องข้อมูลส่วนบุคคลของตนเองจากการถูกละเมิดในชีวิตประจำวันได้ นอกจากนี้ยังเป็นการเพิ่มทักษะความเชี่ยวชาญในการจัดการข้อมูลอย่างเป็นระบบ ซึ่งเป็นทักษะที่สำคัญอย่างยิ่งในยุคเศรษฐกิจดิจิทัล ทำให้มีความมั่นใจในการตัดสินใจเมื่อต้องทำหน้าที่เกี่ยวข้องกับการเก็บรวมรวมหรือส่งต่อข้อมูลส่วนบุคคล ไม่ต้องกังวลเรื่องการทำผิดกฎหมายโดยไม่ได้ตั้งใจ

**๓.๒ ต่อองค์กร** ช่วยลดความเสี่ยงจากการถูกฟ้องร้องหรือถูกลงโทษตามกฎหมาย ซึ่งมีโทษปรับที่สูงมาก การที่บุคลากรมีความรู้จะช่วยสร้างภาพลักษณ์ความน่าเชื่อถือ (Trust) ให้กับหน่วยงานว่าเป็นองค์กรที่มีมาตรฐานสากลในการจัดการข้อมูลผู้รับบริการ ช่วยให้กระบวนการทำงานภายในมีความเป็นระเบียบ ลดการเก็บข้อมูลที่ซ้ำซ้อนหรือไม่จำเป็น ซึ่งนำไปสู่การบริหารจัดการทรัพยากรสารสนเทศที่มีประสิทธิภาพมากขึ้น และสร้างความพึงพอใจให้กับผู้มีส่วนได้ส่วนเสียด้วยเช่นกัน

**๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการฝึกอบรมครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน**

**การทบทวนและปรับปรุงเอกสาร** เริ่มจากการสำรวจแบบฟอร์มการขอข้อมูลต่างๆ ในหน่วยงาน เพื่อจัดทำหรือปรับปรุง "ประกาศนโยบายความเป็นส่วนตัว" (Privacy Notice) ให้ชัดเจนตามหลักกฎหมาย โดยระบุวัตถุประสงค์และระยะเวลาการจัดเก็บที่แน่นอน

**การพัฒนาระบบการจัดเก็บข้อมูล** นำหลักการ "Privacy by Design" มาใช้ในการออกแบบระบบงานใหม่ๆ โดยจำกัดสิทธิ์การเข้าถึงข้อมูล (Access Control) ให้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น และตรวจสอบว่ามีการทำลายข้อมูลเมื่อสิ้นสุดระยะเวลาที่จำเป็น

**การถ่ายทอดองค์ความรู้** จัดกิจกรรมแบ่งปันความรู้ (Knowledge Sharing) ให้กับเพื่อนร่วมงานในแผนก เพื่อให้เกิดแนวปฏิบัติที่ตรงกันทั้งองค์กร และช่วยกันเฝ้าระวังไม่ให้เกิดเหตุการณ์ข้อมูลรั่วไหล เช่น การไม่วางเอกสารที่มีข้อมูลส่วนบุคคลทิ้งไว้บนโต๊ะทำงาน หรือการระมัดระวังการส่งข้อมูลผ่านช่องทางที่ไม่ปลอดภัย อย่าง LINE หรือ Messenger โดยไม่จำเป็น

**๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน**

**ความซับซ้อนของขั้นตอนการทำงาน** การต้องขอความยินยอมหรือแจ้งรายละเอียดที่เพิ่มขึ้น อาจทำให้ผู้รับบริการรู้สึกว่าขั้นตอนยุ่งยากขึ้น หรือทำให้เจ้าหน้าที่ต้องใช้เวลาในการอธิบายมากขึ้น ซึ่งอาจส่งผลต่อความรวดเร็วในการให้บริการในระยะแรก

**ข้อจำกัดทางเทคโนโลยี** ระบบฐานข้อมูลเดิมของหน่วยงาน (Legacy System) อาจไม่ได้ออกแบบมาเพื่อรองรับการลบข้อมูลเป็นรายบุคคล หรือการจำกัดสิทธิ์การเข้าถึงที่ละเอียดพอ ทำให้การปรับปรุงระบบต้องใช้เวลาและงบประมาณสูง

**ความเคยชินและวัฒนธรรมองค์กร** การปรับเปลี่ยนพฤติกรรมการทำงานที่เคยปฏิบัติมานาน เช่น การส่งไฟล์ข้อมูลผ่านโซเชียลมีเดียเพื่อความสะดวก อาจได้รับการต่อต้านจากบุคลากรบางส่วนที่มองว่าเป็นการเพิ่มภาระงาน หรือมองว่ากฎหมายมีความยุ่งยากเกินความจำเป็นในการปฏิบัติงานจริง

**๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล**

**ด้านนโยบายและทรัพยากร** ต้องการให้ผู้บังคับบัญชากำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้เป็นวาระสำคัญของหน่วยงาน และสนับสนุนงบประมาณในการปรับปรุงเครื่องมือ อุปกรณ์ หรือซอฟต์แวร์ที่ช่วยในการรักษาความปลอดภัยของข้อมูลให้ทันสมัย

**ด้านการบริหารจัดการ** การจัดตั้งทีมงานหรือแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ที่ชัดเจน เพื่อให้มีที่ปรึกษาเมื่อเกิดข้อสงสัยในการปฏิบัติงาน รวมถึงการสนับสนุนให้มีการอบรมทบทวนความรู้เป็นระยะๆ เนื่องจากแนวปฏิบัติทางกฎหมายอาจมีการเปลี่ยนแปลง

**การเป็นแบบอย่างที่ดี** ควรให้ความสำคัญและปฏิบัติตามหลักการ PDPA อย่างเคร่งครัด เพื่อสร้างวัฒนธรรมองค์กรที่เคารพในความเป็นส่วนตัว ซึ่งจะช่วยสร้างขวัญและกำลังใจให้พนักงานระดับปฏิบัติการกล้าที่จะเปลี่ยนแปลงกระบวนการทำงานให้ถูกต้องตามกฎหมาย

จึงเรียนมาเพื่อโปรดทราบ

(ลงชื่อ) .....

( นางสาวศจิษฐา รีรักษ์ )

ผู้เข้ารับการฝึกอบรม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

คุณศจิษฐา รีรักษ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 2 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680402579

# สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า**

## คุณศจิษฐา รีรักษ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 2 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

สำเนาถูกต้อง
ศจิษฐา รีรักษ์
...การโรงพยาบาลส่งเสริมสุขภาพตำบลท่าวังหิน

PDPC680402579

ห้ามใช้โฆษณาในทางธุรกิจ

**สรุปโครงการอบรมเชิงปฏิบัติการหลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป (e-learning)**

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

ในยุคดิจิทัลปัจจุบันที่เทคโนโลยีก้าวหน้าอย่างรวดเร็ว การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้อย่างง่ายดายและรวดเร็ว ซึ่งนำมาสู่การละเมิดสิทธิความเป็นส่วนตัวที่สร้างความเดือดร้อนรำคาญและความเสียหายให้แก่เจ้าของข้อมูลจำนวนมาก อีกทั้งยังส่งผลกระทบในเชิงลบต่อระบบเศรษฐกิจโดยรวม ด้วยเหตุนี้ การมีหลักเกณฑ์และมาตรการกำกับดูแลที่ชัดเจนจึงกลายเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อสร้างความเชื่อมั่นว่าข้อมูลส่วนบุคคลจะได้รับการจัดการอย่างถูกต้องและปลอดภัย การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้เป็นเพียงการปกป้องสิทธิขั้นพื้นฐานของบุคคลเท่านั้น แต่ยังเป็นกลไกสำคัญในการสร้างมาตรฐานและมาตรการเยียวยาที่มีประสิทธิภาพเมื่อเกิดการละเมิดสิทธิขึ้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและเป็นที่ยอมรับในระดับสากล แนวทางของ OECD (Organisation for Economic Co-operation and Development) ได้กำหนดหลักการสำคัญ ๘ ประการ ซึ่งได้กลายเป็นรากฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงเป็นหัวใจสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยด้วย

**๑. ความสำคัญ แนวคิด ขอบเขต และประเภทของข้อมูล**

แนวคิดหลักของ PDPA คือการให้ "อำนาจ" แก่เจ้าของข้อมูลในการควบคุมข้อมูลของตนเองในยุคที่ข้อมูลถูกนำไปใช้ในเชิงพาณิชย์และอาชญากรรมไซเบอร์ ข้อมูลส่วนบุคคลเปรียบเสมือนทรัพย์สินที่ต้องการการล้อมรั้วป้องกัน ขอบเขตของกฎหมายนี้ครอบคลุมทั้งหน่วยงานรัฐและเอกชน ไม่ว่าจะเป็นการเก็บข้อมูลในรูปแบบกระดาษหรือดิจิทัล หากข้อมูลนั้นสามารถระบุตัวตนบุคคลที่ยังมีชีวิตอยู่ได้ (ไม่รวมผู้ถึงแก่กรรม) ถือเป็นข้อมูลส่วนบุคคลทั้งสิ้น ประเภทข้อมูลแบ่งเป็น ๒ ระดับหลัก คือ ข้อมูลทั่วไป (ชื่อ, ที่อยู่, IP Address) และข้อมูลอ่อนไหว (Sensitive Data) ซึ่งประเภทหลังนี้มีความสำคัญมาก เพราะหากรั่วไหลอาจนำไปสู่การเลือกปฏิบัติหรือกระทบต่อศักดิ์ศรีความเป็นมนุษย์ เช่น ข้อมูลสหภาพแรงงาน รสนิยมทางเพศ หรือข้อมูลชีวภาพ (ใบหน้า, ลายนิ้วมือ) การเก็บข้อมูลประเภทนี้จึงต้องได้รับความยินยอมโดยชัดแจ้งและมีมาตรฐานความปลอดภัยที่สูงกว่าปกติ นอกจากนี้ PDPA ยังเชื่อมโยงกับกฎหมายอื่น เช่น พ.ร.บ. ไซเบอร์ฯ เพื่อสร้างโครงสร้างพื้นฐานด้านความปลอดภัยที่ครอบคลุมทั้งประเทศ

**๒. หลักการคุ้มครองข้อมูลส่วนบุคคล (Principles)**

หลักการพื้นฐานที่ผู้ควบคุมข้อมูลต้องยึดถือประกอบด้วย ๓ ส่วนสำคัญคือ

๑. การเก็บรวบรวมอย่างจำกัด (Data Minimization) คือการเก็บเท่าที่ "จำเป็น" จริง ๆ ภายใต้วัตถุประสงค์ที่แจ้งไว้ เช่น หากสมัครสมาชิกร้านอาหาร ไม่จำเป็นต้องขอเลขบัตรประชาชน

๒. ความถูกต้องของข้อมูล ผู้เก็บต้องตรวจสอบให้ข้อมูลทันสมัยและไม่ทำให้เกิดความเข้าใจผิด

๓. การจำกัดระยะเวลาการเก็บ (Storage Limitation) ต้องกำหนดชัดเจนว่าจะเก็บข้อมูลไว้นานแค่ไหน (เช่น ๑๐ ปีตามอายุความทางภาษี) และเมื่อพ้นกำหนดต้องทำลายทิ้งทันที หลักการเหล่านี้มีไว้เพื่อลดความเสี่ยง หากเกิดเหตุข้อมูลรั่วไหล ความเสียหายจะถูกจำกัดวงแคบเพราะเราไม่ได้เก็บข้อมูลที่ไม่จำเป็นไว้ตั้งแต่แรก นอกจากนี้ยังเน้นความโปร่งใสผ่าน "นโยบายความเป็นส่วนตัว" (Privacy Notice) ที่ต้องเขียนด้วยภาษาที่เข้าใจง่าย ไม่ใช้ภาษากฎหมายที่ซับซ้อนเกินไป เพื่อให้ประชาชนทราบว่าข้อมูลของตนจะถูกนำไปใช้อย่างไร ใครเป็นผู้รับข้อมูลต่อ และจะติดต่อผู้ควบคุมข้อมูลได้อย่างไร

**๓. ฐานทางกฎหมาย (Lawful Basis) ในการเก็บรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**

หลายคนเข้าใจผิดว่าต้องขอ "ความยินยอม" (Consent) ในทุกกรณี แต่ในความเป็นจริง Consent คือทางเลือกสุดท้ายหากไม่มีฐานอื่นรองรับ ฐานทางกฎหมายช่วยให้กิจกรรมทางเศรษฐกิจและสังคมดำเนินต่อไปได้ เช่น ฐานสัญญา: ธนาคารต้องเก็บที่อยู่คุณเพื่อส่งใบแจ้งหนี้โดยไม่ต้องขอความยินยอมซ้ำซ้อน

ฐานกฎหมาย นายจ้างต้องเก็บเลขผู้เสียภาษีของลูกจ้างเพื่อส่งกรมสรรพากร

ฐานประโยชน์สาธารณะ: หน่วยงานรัฐเก็บข้อมูลเพื่อสวัสดิการแห่งรัฐ

ฐานประโยชน์อันชอบธรรม: การติดกล้อง CCTV เพื่อความปลอดภัยในอาคาร (แต่ต้องติดป้ายแจ้ง)

ฐานระงับอันตรายต่อชีวิต: เช่น กรณีอุบัติเหตุฉุกเฉิน แพทย์สามารถเข้าถึงประวัติการแพ้ยาได้ทันทีโดยไม่ต้องรอขอความยินยอม

การเลือกใช้ฐานที่ถูกต้องมีความสำคัญมาก เพราะหากองค์กรอ้างฐาน Consent แล้วภายหลังเจ้าของข้อมูลถอนความยินยอม องค์กรนั้นอาจต้องหยุดกิจกรรมทันที แต่หากอ้างฐานอื่น เช่น ฐานกฎหมาย แม้เจ้าของข้อมูลจะไม่พอใจ องค์กรก็ยังมีสิทธิเก็บข้อมูลนั้นไว้ได้ตามที่กฎหมายกำหนด

**๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)**

สิทธิเหล่านี้คือเครื่องมือที่ประชาชนใช้ตรวจสอบและควบคุมข้อมูลของตนเอง เริ่มตั้งแต่

- สิทธิขอเข้าถึง (Right of Access) คุณสามารถเดินไปถามธนาคารหรือแอปพลิเคชันได้ว่า "คุณมีข้อมูลอะไรของฉันบ้าง และเอาไปให้ใครดูบ้าง?" โดยองค์กรต้องตอบกลับภายใน ๓๐ วัน

- สิทธิขอให้ลบ (Right to Erasure) หรือ "สิทธิที่จะถูกลืม" (Right to be forgotten) ใช้ได้เมื่อข้อมูลนั้นหมดความจำเป็นหรือได้มาโดยไม่ชอบ

- สิทธิขอให้โอนย้ายข้อมูล (Right to Data Portability) เช่น คุณต้องการย้ายข้อมูลประกันชีวิตจากบริษัท A ไปบริษัท B ในรูปแบบที่คอมพิวเตอร์อ่านได้ เพื่อความสะดวกในการเปรียบเทียบเบี้ยประกัน

- สิทธิคัดค้าน (Right to Object) โดยเฉพาะการนำข้อมูลไปใช้เพื่อการตลาด (Direct Marketing) คุณมีสิทธิสั่งให้เขาหยุดโทรมาขายประกันได้ทันที การใช้สิทธิเหล่านี้เป็นรากฐานของการสร้างดุลอำนาจระหว่างปัจเจกบุคคลกับองค์กรขนาดใหญ่ เพื่อไม่ให้ข้อมูลถูกนำไปใช้ในทางที่เจ้าของข้อมูลไม่ประสงค์

**๕. ความรับผิดและบทกำหนดโทษ**

PDPA มีบทลงโทษที่ครอบคลุมทุกมิติ เพื่อให้มั่นใจว่ากฎหมายจะถูกบังคับใช้จริง

- **โทษทางแพ่ง** เน้นการเยียวยาผู้เสียหาย โดยศาลสั่งให้ชดใช้ค่าสินไหมทดแทนตามจริง และอาจสั่งให้จ่าย "ค่าสินไหมเชิงลงโทษ" เพิ่มขึ้นอีกไม่เกิน ๒ ของค่าเสียหายจริง เพื่อเป็นการดัดนิสัยหน่วยงานที่ละเลย

- **โทษทางปกครอง** เป็นเงินค่าปรับที่จ่ายให้แก่รัฐ มีตั้งแต่ ๑ ล้านถึง ๕ ล้านบาท ขึ้นอยู่กับความร้ายแรง

- **โทษทางอาญา** เป็นกรณีที่ร้ายแรงที่สุด เช่น การเปิดเผยข้อมูลอ่อนไหวโดยทุจริต หรือมุ่งหวังให้ผู้อื่นได้รับความอับอาย/เสียชื่อเสียง มีโทษจำคุกสูงสุด ๑ ปี และปรับสูงสุด ๑ ล้านบาท ที่สำคัญคือ หาก

ผู้กระทำความผิดเป็นนิติบุคคล (บริษัท) "กรรมการหรือบุคคลที่รับผิดชอบ" ในการดำเนินงานของบริษัทนั้น ๆ อาจต้องรับโทษจำคุกร่วมด้วย หากพิสูจน์ได้ว่าความผิดเกิดจากการสั่งการหรือการละเว้นการสั่งการของตน

**๖. กลไกการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ**

เมื่อเจ้าของข้อมูลรู้สึกว่าถูกละเมิด หรือไม่สามารถใช้สิทธิตามข้อ ๔ ได้ (เช่น ขอเข้าถึงข้อมูลแล้วถูกปฏิเสธโดยไม่มีเหตุผล) ขั้นตอนแรกคือการร้องเรียนไปยังผู้ควบคุมข้อมูลนั้น ๆ ก่อน หากไม่ได้รับการแก้ไข จึงจะเข้าสู่กลไกการร้องเรียนต่อ คณะกรรมการผู้เชี่ยวชาญ ภายใต้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) กระบวนการนี้ถูกออกแบบมาให้เป็น "ทางลัด" ก่อนไปถึงศาล คณะกรรมการจะทำหน้าที่ตรวจสอบข้อเท็จจริง ไกล่เกลี่ยข้อพิพาท และมีอำนาจสั่งการให้ผู้ควบคุมข้อมูลดำเนินการอย่างใดอย่างหนึ่ง เช่น สั่งให้ลบข้อมูล หรือสั่งให้จ่ายค่าปรับทางปกครอง การร้องเรียนสามารถทำได้ผ่านช่องทางออนไลน์หรือมายื่นด้วยตนเอง ซึ่งเป็นกลไกที่ช่วยให้ประชาชนเข้าถึงความยุติธรรมได้ง่ายขึ้นโดยไม่ต้องเสียค่าใช้จ่ายในการจ้างทนายความ ฟ้องศาลในเบื้องต้น และคำสั่งของคณะกรรมการถือเป็นคำสั่งทางปกครองที่ต้องปฏิบัติตาม

**๗. การปฏิบัติเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Notification)**

ในโลกไซเบอร์ไม่มีระบบใดปลอดภัย ๑๐๐% กฎหมายจึงเน้นที่ "การจัดการหลังเกิดเหตุ" เมื่อเกิดเหตุข้อมูลรั่วไหล (Data Breach) องค์กรต้องรีบประเมินความเสี่ยงทันที หากพบว่ามีความเสี่ยงต่อเจ้าของข้อมูลต้องแจ้งเหตุให้ สคส. ทราบภายใน ๗๒ ชั่วโมง เพื่อให้เจ้าหน้าที่รัฐเข้ามาประคองสถานการณ์ หากประเมินแล้วพบว่ามีความเสี่ยงสูงมาก (High Risk) เช่น ข้อมูลเลขบัตรประชาชนและเลขหลังบัตรหลุดไป ซึ่งอาจนำไปสู่ การสวมรอยทำธุรกรรม องค์กรต้องแจ้ง "เจ้าของข้อมูล" ทุกคนทราบโดยเร็วที่สุด พร้อมทั้งบอกวิธีที่เจ้าของข้อมูลควรทำเพื่อป้องกันตัวเอง (เช่น แนะนำให้ไปเปลี่ยนรหัสผ่าน หรืออายัดบัตร) การซ่อนเร้นความผิดหรือ การไม่แจ้งเหตุถือเป็นความผิดร้ายแรงตามกฎหมาย การแจ้งเตือนที่รวดเร็วจะช่วยลดความเสียหายจาก การถูกนำข้อมูลไปใช้ในทางมิชอบได้มหาศาล

**๘. บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

DPO คือ "ตัวกลาง" และ "ที่ปรึกษา" ที่กฎหมายบังคับให้หน่วยงานรัฐทุกแห่ง และบริษัทเอกชนที่มีการประมวลผลข้อมูลจำนวนมากหรือข้อมูลอ่อนไหวต้องมี DPO ไม่ได้มีหน้าที่เข้าไปทำความสะอาดข้อมูลด้วยตัวเอง แต่มีบทบาทในการวางนโยบาย ให้คำแนะนำแก่พนักงานในองค์กรว่าการทำแคมเปญการตลาดแบบนี้เสี่ยง ผิดกฎหมายหรือไม่ และเป็นผู้ประสานงานหลักเมื่อมีเจ้าของข้อมูลมาใช้สิทธิ หรือเมื่อต้องติดต่อกับ สคส. กฎหมายกำหนดให้ DPO ต้องมีความเป็นอิสระในการปฏิบัติหน้าที่ (ไม่ถูกไล่ออกเพียงเพราะรายงานว่าบริษัททำผิดกฎหมาย) และผู้บริหารต้องสนับสนุนทรัพยากรให้ DPO ทำงานได้จริง การมี DPO ที่เข้มแข็งจะช่วยให้องค์กรสร้างวัฒนธรรม "Privacy by Design" หรือการคำนึงถึงความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบระบบหรือบริการใหม่ ๆ ไม่ใช่มาแก้ไขภายหลังซึ่งจะมีต้นทุนสูงกว่า

**๙. กลไกการคุ้มครองข้อมูลส่วนบุคคลของ สคส. (PDPC)**

สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) ทำหน้าที่เป็น Regulators หรือ "ตำรวจข้อมูล" ของประเทศไทย กลไกของ สคส. ไม่ได้เน้นแค่การลงโทษ แต่เน้นที่การสร้างระบบนิเวศ (Ecosystem) ของการคุ้มครองข้อมูล เช่น การออกกฎหมายลำดับรองเพื่อขยายความให้ชัดเจน (เช่น มาตรฐานความปลอดภัยขั้นต่ำที่บริษัทต้องมีคืออะไร) การสร้างมาตรฐานความร่วมมือกับหน่วยงานกำกับดูแลอื่น ๆ เช่น แบงก์ชาติ หรือ กสทช. นอกจากนี้ สคส. ยังมีหน้าที่ส่งเสริมความรู้ (Digital Literacy) ให้ประชาชนรู้เท่าทันสิทธิ์ของตนเอง และส่งเสริมให้ภาคธุรกิจมีแนวปฏิบัติที่ดี (Code of Practice) เพื่อให้การคุ้มครองข้อมูลเป็นมาตรฐานเดียวกัน ทั้งประเทศ กลไกเหล่านี้มุ่งหวังจะทำให้ประเทศไทยเป็นที่ยอมรับในระดับสากลว่ามี

มาตรฐานการคุ้มครองข้อมูลที่เพียงพอ เพื่อประโยชน์ในการไหลเวียนของข้อมูลข้ามพรมแดนและการดึงดูดการลงทุนจากต่างประเทศ

# สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอมอบประกาศนียบัตรฉบับนี้เพื่อแสดงว่า

## คุณจันทิมา จันทะบูรณ์

ได้ผ่านการอบรมหลักสูตรการเรียนรู้ออนไลน์
หลักสูตรด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับประชาชนทั่วไป

ให้ไว้ ณ วันที่ 25 ธันวาคม 2568

พันตำรวจเอก
(สุรพงศ์ เปล่งขำ)
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPC680406390