การคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับผู้ปฏิบัติงาน

นายชนภัทร วินยวัฒน์
อัยการผู้เชี่ยวชาญพิเศษ
สำนักงานที่ปรึกษากฎหมาย
สำนักงานอัยการสูงสุด

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, 2019)

- ประกาศ 24 พฤษภาคม 2562
- ประกาศให้บังคับใช้ 27 พฤษภาคม 2563 เลื่อนการบังคับใช้ 2 ครั้ง
- จะบังคับใช้เป็นการทั่วไป 1 มิถุนายน 2565
- General Data Protection Regulation: GDPR

ยุคก่อน PDPA 2019

- การคุ้มครองสิทธิความเป็นส่วนตัวตามรัฐธรรมนูญ มาตรา 32
- การคุ้มครองสิทธิของบุคคล ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420
- ความผิดอาญาฐานหมิ่นประมาท ตามประมวลกฎหมายอาญา มาตรา 326
- ความผิดอาญาฐานนำเข้าข้อมูลอันเป็นเท็จในระบบคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยความรับผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. 2544
- พ.ร.บ. สุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 7

หลักการสำคัญของ PDPA

1) ห้าม “ยุ่ง” กับ “ข้อมูลส่วนบุคคล” ของผู้อื่น เว้นแต่จะมีเหตุตามกฎหมาย
2) เมื่อต้อง “ยุ่ง” ต้องมีรูปแบบและวิธีการที่เหมาะสม
3) ถ้าฝ่าฝืน มีโทษตามกฎหมาย

- ยุ่ง = ประมวลผลข้อมูล (Processing)

เค้าโครงของการบรรยาย

- ความหมายของข้อมูลส่วนบุคคล
- หลักการ “ประมวลผล” ข้อมูลส่วนบุคคลของผู้อื่นตามกฎหมาย
- ความเสี่ยงในการจัดการข้อมูล่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
- การจัดการความเสี่ยง
- การปฏิบัติตน

ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ตัวอย่าง

- ชื่อ นามสกุล, เลขประจำตัวประชาชน, ที่อยู่
- Email address, ทะเบียนรถ, IP address,
- รูม่านตา, ลายพิมพ์นิ้วมือ, แบบพิมพ์ฟัน, การจำลองใบหน้า
- ข้อมูลทางชีวภาพอื่น เช่น กรุ๊ปเลือด, รายละเอียด DNA

กิจกรรมที่ควบคุม : การประมวลผล (Processing)

- การเก็บรวบรวม (Storage and Collection)
- การใช้หรือเปิดเผย (Usage and Disclose)

มาตรา 4 : ประเภทของกิจกรรมที่ได้รับยกเว้น

- การเก็บรวบรวม ใช้ หรือเปิดเผย เพื่อประโยชน์ส่วนรวมหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้น
- การดำเนินการของหน่วยงานของรัฐ ที่มีหน้าที่รักษาความมั่นคงของรัฐ (การคลัง) การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ ความมั่นคงปลอดภัยทางไซเบอร์
- การเก็บรวบรวมเพื่อกิจการสื่อสารมวลชน งานศิลปกรรม งานวรรณกรรม ตามจริยธรรมแห่งการประกอบวิชาชีพ หรือประโยชน์สาธารณะ
- สภาผู้แทนราษฎร วุฒิสภา รัฐสภา กรรมาธิการ ตามอำนาจหน้าที่
- การพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ การดำเนินงานตามกระบวนการยุติธรรมทางอาญา
- การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบข้อมูลเครดิต

มาตรา 4 : ประเภทของกิจกรรมที่ได้รับยกเว้น

- แม้จะได้รับยกเว้น ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

บุคคลผู้เกี่ยวข้องใน PDPA

- เจ้าของข้อมูลส่วนบุคคล (Data Subject: DS)
- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller: DC)
- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor: DP)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
- บุคคลที่สาม (Third Party: TP)

เจ้าของข้อมูลส่วนบุคคล

(Data Subject : DS)

- ไม่มีคำนิยาม
- บุคคลผู้มีชีวิตอยู่ที่ข้อมูลสามารถระบุได้ทั้งทางตรง และทางอ้อม ว่าเป็นใคร
- มีสิทธิบางอย่าง ตามที่กฎหมายกำหนด

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller : DC)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor : DP)

- บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
- *ไม่ใช่เจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล*

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

- **คนที่ได้รับมอบหมาย**เพื่อทำหน้าที่ให้คำแนะนำ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน/ องค์กร/ สถาบัน ให้เป็นไปตามกฎหมาย
- เจ้าหน้าที่ในทุกแผนก หรือทุกส่วนงาน ที่ได้รับมอบหมายให้ดำเนินการ เพื่อการประมวลผลข้อมูล

สถานะของพนักงานในหน่วยงาน/ องค์กร/ สถาบัน ว่าเป็น DC หรือ DP หรือ DPO

- ในกรณีที่มีอำนาจตัดสินใจ กระทำการในนาม DC
- ในกรณีที่ทำตามคำสั่งหรือในนามของนิติบุคคลนั้น

พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2544

- ใช้กับ ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ทั้งข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐ หรือข้อมูลข่าวสารส่วนบุคคล
- หลัก ข้อมูลข่าวสารของทางราชการต้องเปิดเผย
- ข้อยกเว้น ๑) ปกปิดในบางกรณี

  ๒) ปกปิด ข้อมูลข่าวสารส่วนบุคคล

หลักการของ PDPA

- ห้าม “ประมวลผล” “ข้อมูลส่วนบุคคล” ของคนอื่น
- หากจำเป็นต้องประมวลผล ต้อง
  - มีฐานของกฎหมาย
  - ประมวลผลตามเงื่อนไขของกฎหมาย
    - เท่าที่ควรจะทำ ไม่ใช่ เท่าที่สามารถทำได้
    - เท่าที่จำเป็น
    - เท่าที่ได้รับอนุญาต
  - มีมาตรการรักษาความปลอดภัยในข้อมูลส่วนบุคคล
  - DS ต้องมีส่วนร่วมในความเคลื่อนไหวของข้อมูลตนเอง
  - มีมาตรการเยียวยาความเสียหายในกรณีเกิดความเสียหาย
- มีองค์กรเฉพาะสำหรับดูแลในเรื่องข้อมูลส่วนบุคคล

Step 1: ข้อมูลส่วนบุคคลในความครอบครอง

- ทำความเข้าใจกับข้อมูลส่วนบุคคลในส่วนงาน
- ลักษณะของส่วนงาน เช่น งานทะเบียน, งานสอน, งานทรัพยากรบุคคล, งานบริหาร, งานจัดซื้อจัดจ้าง, งานบัญชีและงานคลัง, งานเทคโนโลยีสารสนเทศ
- ลักษณะการทำงาน (Workflow)

Step 2 : การได้มาซึ่งข้อมูลส่วนบุคคล

- ช่องทางการได้มา
- วิธีการได้มา
  - ฐานที่ชอบด้วยกฎหมาย (Legal Bases) 6 + 1
  - ประมวลผลให้น้อยที่สุด (Data Minimization) เท่าที่จำเป็น (Necessity)
  - ประมวลผลตามกรอบวัตถุประสงค์อันชอบด้วยกฎหมาย
  - ถ้ามีการเปลี่ยนวัตถุประสงค์ในการประมวลผล ต้องแจ้งให้เจ้าของข้อมูลทราบ และต้องได้รับความยินยอมจาก DS ก่อน เว้นแต่ กฎหมายบัญญัติให้กระทำได้

ฐานในการประมวลผลตาม PDPA (ม. 24)

- ความยินยอม (Consent)
- เพื่อการศึกษาวิจัย การจัดทำเอกสารประวัติศาสตร์ เพื่อประโยชน์สาธารณะ โดยมีมาตรการที่เหมาะสม (Research / Statistics)
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ (Vital Interest)
- จำเป็นเพื่อปฏิบัติตามสัญญาซึ่งมี DS เป็นคู่สัญญา หรือดำเนินการตามคำขอของ DS ก่อนเข้าทำสัญญา (Contract)
- การปฏิบัติตามภารกิจของรัฐเพื่อประโยชน์สาธารณะ หรือตามที่ DC ได้รับมอบหมาย (Public Task)
- ความจำเป็น/ความชอบด้วยกฎหมาย เพื่อประโยชน์ของผู้อื่น ซึ่งสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของ DS มีน้อยกว่า (Legitimate Interest)
- การปฏิบัติตามกฎหมายของ DC (Legal Obligation)

การขอความยินยอม

- เวลา : ก่อนหรือขณะประมวลผล
- รูปแบบ : ชัดแจ้ง และ เป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์
  ตัดสินใจได้อย่างอิสระ
- เนื้อหา : แยกส่วน อ่านง่าย ไม่เป็นการหลอกลวง
- รายการที่ต้องแจ้ง :
  - วัตถุประสงค์ในการประมวลผล
  - สิทธิของ DS
- ระยะเวลาที่จะถอนความยินยอม (ข้อจำกัดสิทธิ????)

ความยินยอมของบุคคลผู้หย่อนความสามารถ

- ผู้เยาว์ - ถ้าไม่ใช่การใด ๆ ที่อาจให้ความยินยอมได้เองโดยลำพัง (ตามมาตรา ๒๒ ๒๓ และ ๒๔ ป.พ.พ.) ผู้เยาว์ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจทำการแทนผู้เยาว์
- ผู้เยาว์อายุไม่เกิน ๑๐ ปี :ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองฯ
- คนไร้ความสามารถ : ขอความยินยอมจากผู้อนุบาล
- คนเสมือนไร้ความสามารถ : ขอความยินยอมจากผู้พิทักษ์

วิธีประมวลผล

- ประมวลผลอย่างจำกัด (Data Minimization)
  - เท่าที่ควรจะทำ ไม่ใช่ เท่าที่สามารถทำได้
  - เท่าที่จำเป็น
  - เท่าที่ได้รับอนุญาต
- ประมวลผลตามกรอบวัตถุประสงค์อันชอบด้วยกฎหมาย
  - ตามเหตุผลที่ได้ประมวลผลข้อมูลนั้น ๆ
  - ถ้าเปลี่ยนวัตถุประสงค์ในการประมวลผล ต้องแจ้งให้เจ้าของข้อมูลทราบ และต้องได้รับความยินยอมจาก DS ก่อน เว้นแต่ กฎหมายบัญญัติให้กระทำได้
- ต้องมีมาตรการรักษาความปลอดภัยในข้อมูลนั้น ๆ

การรักษาความปลอดภัยในข้อมูล

- ประกาศ DES เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (17 ก.ค. 63)
  - คุณสมบัติของข้อมูล
    - การคงไว้ซึ่งความลับ (Confidentiality)
    - สภาพพร้อมใช้งาน (Availability)
    - มีความถูกต้องครบถ้วน (Integrity)
  - เพื่อป้องกันการกระทำโดยมิชอบด้วยกฎหมาย ดังนี้
    - การสูญหาย
    - การเข้าถึง
    - การใช้
    - การเปลี่ยนแปลง
    - การแก้ไข
    - การเปิดเผย

การรักษาความปลอดภัยในข้อมูล: หลักการ

- มาตรการ
  - มาตรการป้องกันด้านบริหารจัดการ (Administrative Safeguard)
  - มาตรการป้องกันด้านเทคนิค (Technical Safeguard)
  - มาตรการด้านกายภาพ (Physical Safeguard)
- การเข้าถึง/การควบคุมการใช้งาน (ขั้นต่ำ)
  - การควบคุมการเข้าถึงอุปกรณ์จัดเก็บต้องมั่นคงปลอดภัย
  - การอนุญาต กำหนดการเข้าถึง
  - การบริหารจัดการการเข้าถึง ควบคุมเฉพาะผู้ที่ได้รับอนุญาตแล้ว
  - การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
  - มีวิธีการตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง การเปลี่ยนแปลง ลบ หรือถ่ายโอน
- Assets : แหล่งที่มา, สถานที่จัดเก็บ, สถานที่ปลายทาง

ตัวอย่างการรักษาความปลอดภัย

ภายใน

- การกำหนดนโยบายส่วนบุคคล (Privacy Policy)
- การควบคุมการเข้าถึง (Access Control)
- การกำหนดรหัส (Encryption)
- การพรางข้อมูล (Anonymization) และการแฝงข้อมูล (Pseudonymization)
- การรวมข้อมูล (Aggregation)
- การบังข้อมูล (Masking)

ภายนอก

- การทำข้อตกลง (NDA, DPA)
- การกำหนดนโยบาย

สรุปหลักการประมวลผล

- ฐานที่ชอบด้วยกฎหมาย (Legal Bases) 6 + 1
- ประมวลผลให้น้อยที่สุด (Data Minimization) เท่าที่จำเป็น (Necessity)
- ประมวลผลตามกรอบวัตถุประสงค์อันชอบด้วยกฎหมาย
- แจ้งให้ DS ทราบ
- ถ้ามีการเปลี่ยนวัตถุประสงค์ในการประมวลผล ต้องแจ้งให้เจ้าของข้อมูลทราบ และต้องได้รับความยินยอมจาก DS ก่อน เว้นแต่ กฎหมายบัญญัติให้กระทำได้
- ต้องมีมาตรการรักษาความปลอดภัย

Step 3: การจัดการข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)

- ข้อมูลส่วนบุคคลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวมหรือประมวลผล ได้แก่ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นใดในทำนองเดียวกันที่คณะกรรมการประกาศกำหนด
- กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

Sensitive Personal Data (มาตรา 26)

- หลัก : ห้ามเก็บข้อมูลส่วนบุคคลดังนี้โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล
- ข้อยกเว้น : มีเหตุอื่นตามกฎหมาย โดยมีมาตรการการคุ้มครองที่เหมาะสม เช่น
  - Vital interest : ไม่อยู่ในสภาวะให้ความยินยอมได้
  - Non-profit organization use: โดยไม่ได้เปิดเผยออกสู่สาธารณะ
  - Public Disclosure : โดยชัดแจ้ง และโดยเจ้าของข้อมูล
  - Legal Claim: กระทำเพื่อก่อตั้งสิทธิเรียกร้อง/การต่อสู้คดี
  - Legal Obligation: มีกฎหมายกำหนดให้มีหน้าที่ เช่น ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย ประโยชน์สาธารณะ

Step 4: สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิในการถอนการให้ความยินยอม (right of withdrawal consent)
- สิทธิการเข้าถึง (right of access)
- สิทธิขอรับ/ส่งข้อมูลส่วนบุคคลไปให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่น (right to data portability)
- สิทธิคัดค้าน (right to object)
- สิทธิขอให้ลบข้อมูลส่วนบุคคล (right of erasure)
- สิทธิระงับการใช้ข้อมูลส่วนบุคคล (right of processing restriction)
- สิทธิทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน (right to rectification)
- สิทธิร้องเรียน (right to complain)

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- ไม่ใช่สิทธิเด็ดขาด อาจจะถูกปฏิเสธได้
- ถ้าคำขอไม่สมเหตุสมผล กับคำขอฟุ่มเฟือย DC ปฏิเสธได้เกือบทุกกรณี ยกเว้น การเพิกถอนความยินยอม
- ถ้าเก็บรวบรวมโดยใช้ความยินยอมเพียงอย่างเดียว เจ้าของข้อมูลจะมีสิทธิทุกประการได้

Step 5: ประเมินความเสี่ยงด้านต่าง ๆ

- การจัดทำเอกสารที่เกี่ยวข้อง
- การเตรียมความพร้อม และการสร้างความตระหนัก
- ฐานกฎหมาย
- ข้อจำกัดเรื่องวัตถุประสงค์ (Purpose Limitation)
- การใช้ข้อมูลเท่าที่จำเป็น (Data Minimization)
- ความถูกต้องและพร้อมใช้ข้อมูล (Accuracy and Availability)
- รูปแบบและวิธีการเก็บรักษา (Storage Limitation)
- การใช้และการเปิดเผยข้อมูล (Use and Disclose Limitation)
- สิทธิของเจ้าของข้อมูล (Data Subject's Rights)

Step 6: ประเมินความพร้อมของผู้เกี่ยวข้อง

- DC
- DP
- DPO
- บุคคลที่สาม

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (DC)

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- ป้องกันไม่ให้บุคคลหรือนิติบุคคลอื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- จัดให้มีระบบการตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา/ที่ไม่เกี่ยวข้อง/เกินความจำเป็น/เจ้าของข้อมูลส่วนบุคคลร้องขอ/เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม
- แจ้งการละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน
- จัดทำบันทึกรายการ (Record of Processing : ROP)

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (DP)

- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- แจ้งให้ผู้ควบคุมข้อมูลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- ถ้าผู้ประมวลผลฯ ไม่ปฏิบัติตามคำสั่งของผู้ควบคุมฯ ให้ถือว่า ผู้ประมวลผลเป็นผู้ควบคุม

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

- ในกรณีที่ DC/ DP เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคล จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ
- กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 ตามคำสั่งและนโยบายของ DC
- รายงานกรณีมีการละเมิดข้อมูลส่วนบุคคลต่อ DC

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคล
- ตรวจสอบการดำเนินงานของ DC/DP เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับสำนักงาน
- รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

หน้าที่ของบุคคลที่สาม

- ปฏิบัติตามเงื่อนไขของ DC/DP/DPO กำหนด
- ไม่เป็นผู้ประมวลผลโดยไม่ชอบด้วยกฎหมาย
- ถ้าพบเหตุละเมิด ให้แจ้ง DC/DPO เพื่อดำเนินการต่อไป

ความรับผิด

- ทางแพ่ง
- ทางอาญา
- ทางปกครอง

ความรับผิดทางแพ่ง

- ค่าเสียหายตามจริง
- ค่าเสียหายเชิงลงโทษ – ค่าสินไหมสูงสุดสองเท่าของค่าเสียหายตามจริง
- อายุความ
  - 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
  - 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

ความรับผิดทางอาญา

- ใช้หรือเปิดเผย Personal Data หรือ Sensitive Data

โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

  - จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ
- เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย
  - จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ
- ยอมความได้

- ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม PDPA นำไปเปิดเผยแก่ผู้อื่น
  - จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความรับผิดทางปกครอง

- ผู้ควบคุมข้อมูลส่วนบุคคล - มาตรา 82, 83, 84
- ผู้ประมวลข้อมูลส่วนบุคคล - มาตรา 85, 86, 87
- ผู้แทนผู้ควบคุมข้อมูลส่วนบุคคล/ ผู้ประมวลข้อมูลส่วนบุคคล - มาตรา 88
- โทษ -ปรับสูงสุดไม่เกิน 5 ล้านบาท ขึ้นอยู่กับประเภทของความผิดตาม พ.ร.บ.

ข้อมูลส่วนบุคคลที่มีอยู่ขณะนี้ ทำอย่างไร????

- เก็บรวบรวมไว้ก่อนวันที่ PDPA ใช้บังคับ
  - ✓เก็บรวบรวมและใช้ได้ต่อไปตามวัตถุประสงค์เดิม
  - ✓กำหนดวิธีการยกเลิกความยินยอมโดยง่ายและเผยแพร่ประชาสัมพันธ์ให้ DS ที่ไม่ประสงค์จะให้ความยินยอมทราบ
- ถ้าวัตถุประสงค์เปลี่ยนไป?
- มาตรการที่ต้องการเพิ่มเติม?

ความสัมพันธ์กับพระราชบัญญัติข้อมูลข่าวสารทางราชการฯ

- มาตรการที่ขัดหรือแย้ง
- มาตรการเพิ่มเติม
- การร้องเรียน อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ บทลงโทษ
- อำนาจคณะกรรมการผู้เชี่ยวชาญ

Q & A