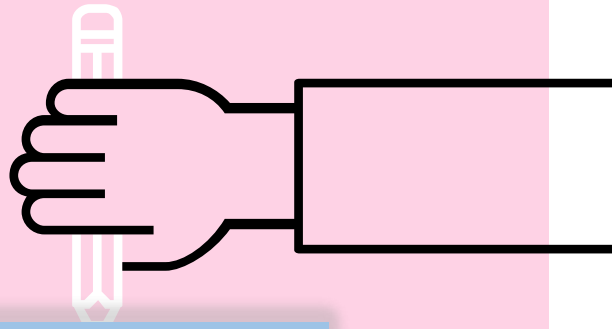
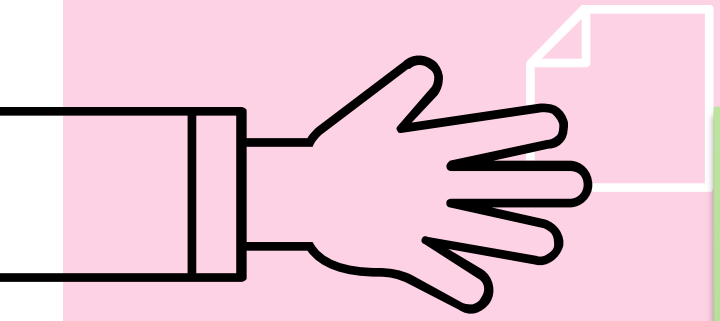


พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
Personal Data Protection Act B.E.2019



โดย ฝ่ายกฎหมาย **TCC Assets**

11 พฤษภาคม 2563

ทำไมต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล(PDPA)

1. ความมั่นใจของประชาชน ไม่ให้ใครจะเอาข้อมูลไปใช้ ข้อมูลของบุคคลจะได้รับการคุ้มครอง

2. ธรรมาภิบาลข้อมูล (Data Governance) ทุกภาคส่วนคาดหวัง มีความประสงค์ให้คนที่เก็บข้อมูลมีการจัดเก็บข้อมูลที่โปร่งใส และมีการคุ้มครองข้อมูลที่เหมาะสม

3. ประเทศไทยอยู่คนเดียวไม่ได้ กฎหมายฉบับนี้เป็นการยืนยันให้ทั่วโลกทราบว่าเรามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่พร้อมแล้ว การทำธุรกิจระหว่างประเทศก็ไม่ต้องพึ่งเครื่องมืออื่น ๆ ในการโอนข้อมูลข้ามพรมแดน ทำให้ธุรกิจคล่องตัว

กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

- **กฎหมายรัฐธรรมนูญ 2560**

  มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นละเมิด หรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าทางใดๆ จะกระทำมิได้ เว้นแต่ โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

- **พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562**

  ระยะที่ 1 ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562

  ระยะที่ 2 มีผลบังคับใช้ 28 พฤษภาคม 2563

กฎหมายคุ้มครองข้อมูลส่วนบุคคลและการบังคับใช้กฎหมาย

พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ประกาศในราชกิจจานุเบกษา วันที่ 27 พฤษภาคม 2562

28 พฤษภาคม 2563
(ครบ 1 ปี)

บริษัทจะต้องเตรียมความพร้อมให้เสร็จก่อนวันที่ 28 พฤษภาคม 2563

ระยะที่ 1
มีผลตั้งแต่วันที่
28 พฤษภาคม 2562 เป็นต้นไป

- คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ระยะที่ 2
เริ่มมีผลตั้งแต่วันที่ 28 พฤษภาคม 2563 เป็นต้นไป

- การขอความยินยอม
- การตั้ง DPO
- การร้องเรียน
- บทลงโทษ
  - ทางแพ่ง
  - ทางอาญา
  - ทางปกครอง
- เก็บ รวบรวม ใช้ ตามกฎหมาย
- การคุ้มครองข้อมูลส่วนบุคคล
- หน้าที่ผู้เกี่ยวข้อง
  1. Controller
  2. Processor
- สิทธิของเจ้าของข้อมูล
  - เข้าถึง
  - ขอรับสำเนา
  - ลบ/แก้ไข
  - คัดค้าน/ปฏิเสธ
  - ควบคุม/จำกัดการประมวลผล

ขอบเขตอำนาจการใช้บังคับ

1. เจ้าของข้อมูลส่วนบุคคลอยู่ในราชอาณาจักร
2. ผู้ประกอบการมีบริษัทหรือสาขาที่ตั้งในไทย ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้น จะเกิดขึ้นในไทยหรือไม่ก็ตาม
3. ผู้ประกอบการไม่มีบริษัทหรือสาขาที่ตั้งในไทยแต่

   3.1 เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลในไทย ไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม

   3.2 มีการติดตามและจัดเก็บพฤติกรรมของเจ้าของข้อมูลในไทย ตราบเท่าที่พฤติกรรมที่จัดเก็บนั้นเกิดขึ้นในไทย

ความจำเป็นที่องค์กรและผู้บริหารต้องให้ความสำคัญ

ทุกหน่วยงานที่มีการจัดเก็บหรือใช้ข้อมูลส่วนบุคคล เช่น

Accounting

ข้อมูลของผู้รับ-จ่ายเงิน

Procurement

ข้อมูลของคู่สัญญา/กรรมการ

HR

ข้อมูลผู้สมัครงาน ข้อมูลพนักงาน

Marketing

ข้อมูลลูกค้า

IT

Terms & Conditions ของ website

การจัดเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลขององค์กร

Com Sec

ข้อมูลผู้บริหาร ผู้ถือหุ้น

Legal: ให้คำปรึกษาและสนับสนุนการดำเนินงานให้สอดคล้องกับกฎหมาย

ข้อมูลส่วนบุคคล: ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรม

ข้อมูลส่วนบุคคลทั่วไป
Personal Data

1. ชื่อ-นามสกุล
2. ลายพิมพ์นิ้วมือ
3. เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต การเก็บสำเนาบัตรประชาชน หรือบัตรอื่นๆ ที่มีข้อมูลส่วนบุคคลที่ระบุตัวบุคคลได้ ถือเป็นข้อมูลส่วนบุคคล
4. ที่อยู่ อีเมล์ เบอร์โทรศัพท์
5. ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น **IP Address, Cookie ID**
6. ข้อมูลระบุทรัพย์สินของบุคคล เช่น โฉนดที่ดิน สมุดทะเบียนรถยนต์
7. ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงาน

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว
Sensitive Data

1. เชื้อชาติ เผ่าพันธุ์
2. ความคิดเห็นทางการเมือง
3. ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
4. พฤติกรรมทางเพศ
5. ประวัติอาชญากรรม
6. ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต
7. ข้อมูลสหภาพแรงงาน
8. ข้อมูลพันธุกรรม
9. ข้อมูลชีวภาพ
10. ข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

- เลขทะเบียนรถยนต์
- ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์หรือแฟกซ์ที่ทำงาน ที่อยู่สำนักงาน อีเมล์ที่ใช้ในการทำงาน อีเมล์ของบริษัท เช่น info@tcca.com เป็นต้น

  ข้อมูลทางธุรกิจ แต่หากระบุถึงตัวบุคคลย่อมเป็นข้อมูลส่วนบุคคล เช่น yaya.urassaya@tcca.com
- ข้อมูลนิรนาม (**Anonymous Data**) : ข้อมูลหรือชุดข้อมูลที่ผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้
- ข้อมูลแฝง (**Pseudonymous Data:** ข้อมูลที่ยังคงเป็นข้อมูลส่วนบุคคลแต่เป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลตั้งต้น
- ข้อมูลผู้ตาย

ข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคล

1. เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัว
2. การดำเนินงานของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคง
3. เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะ
4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภารวมถึงคณะกรรมมาธิการที่แต่งตั้งโดยสภาผู้แทน
5. การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนพิจารณาคดี การบังคับคดี การวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมาย

หน้าที่ขององค์กรตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- จัดเก็บเท่าที่จำเป็น (มาตรา 22)
- แจ้งวัตถุประสงค์ให้ทราบ “ก่อน” หรือ “ขณะ” เก็บข้อมูล (มาตรา 23)
- ห้ามเก็บจากแหล่งอื่น (มาตรา 25) เว้นแต่ได้แจ้งภายใน 30 วันนับแต่เก็บรวบรวม และได้รับความยินยอมจากเจ้าของข้อมูล

- ใช้ให้ตรงตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูล (มาตรา 21)
- ใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลไม่ได้ (มาตรา 27)
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูล (มาตรา 41)

- เปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลไม่ได้ (มาตรา 27)
- การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ปลายทางที่ได้รับข้อมูลจะต้องมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ (มาตรา 28-29)

- แก้ไขให้ข้อมูลถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ทำให้เข้าใจผิด (มาตรา 35-36)
- จัดให้มีมาตรการรักษาความปลอดภัย (มาตรา 37)
- ทำบันทึกให้ตรวจสอบได้ (มาตรา 39)

การเตรียมความพร้อมขององค์กรเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล

ข้อมูลที่เก็บรวมรวมไว้ก่อน 28 พฤษภาคม 2563

1. เก็บรวบรวมและใช้ได้ตามวัตถุประสงค์เดิมที่ได้แจ้งต่อเจ้าของข้อมูล โดยผู้ควบคุมข้อมูลต้องดำเนินการดังนี้
   - กำหนดวิธีการยกเลิกความยินยอม เช่น ทางเว็บไซต์ของผู้ควบคุมข้อมูล และ ควรแจ้งแนวปฏิบัติเกี่ยวกับ Privacy Policy ด้วย
   - เผยแพร่ประชาสัมพันธ์ ไม่ให้เจ้าของข้อมูลใช้สิทธิแจ้งยกเลิกความยินยอมได้โดยง่าย
2. ทุกหน่วยงานต้องตรวจสอบว่า มีการจัดเก็บและรวมรวบข้อมูลส่วนบุคคลประเภทใด และเพื่อวัตถุประสงค์ใด

ข้อมูลที่เก็บรวมรวม ตั้งแต่ 28 พฤษภาคม 2563

1. จัดเก็บและรวบรวมตามฐานสิทธิภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้แก่ ฐานสัญญา ฐานความยินยอม ฐานหน้าที่ตามกฎหมาย ฐานประโยชน์อันชอบธรรม เป็นต้น
2. หากใช้ฐานความยินยอม จะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลที่ชัดแจ้ง
   - ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้ ระยะเวลาในการจัดเก็บ สิทธิในการถอนความยินยอม และวิธีการถอนความยินยอมจะต้องง่ายและรวดเร็ว
3. หากมีข้อมูลจำนวนมาก ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

1. **Data Policy** การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล
2. **Data Discovery** การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล
3. **Data Proliferation** การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคล
4. **Data Risk Level** กำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ
5. **Data Protection** มีมาตรการคุ้มครองข้อมูลส่วนบุคคล

ฐานการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สัญญา (Contract)
ใช้กับข้อมูลส่วนบุคคลทั่วไป เท่านั้น (ข้อมูลอ่อนไหว ใช้การทำตามสัญญาไม่ได้)

จดหมายเหตุ/วิจัย/สถิติ

หน้าที่ตามกฎหมาย (Legal Obligation)

ประโยชน์สำคัญต่อชีวิต (Vital Interest)
ระงับอันตรายต่อชีวิต ร่างกาย สุขภาพ

ประโยชน์อันชอบธรรม (Legitimate Interest)
ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลอื่น

ภารกิจของรัฐ (Public Task)
ความจำเป็นเพื่อประโยชน์สาธารณะและการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

ความยินยอม (Consent)

ฐานสัญญา (Contract)

จำเป็น สำหรับสัญญา

“จำเป็น” ตามปกติของการดำเนินงานให้เป็นไปตามสัญญาไม่รวมถึงกรณีปัญญาข้อพิพาทที่เกิดขึ้นจากสัญญา

- ❌ เปิดเผยข้อมูลให้หน่วยงานภายนอกเพื่อติดตามทวงหนี้
- ❌ รวบรวมข้อมูลเพื่อฟ้องร้องต่อการไม่ปฏิบัติตามสัญญา
- ❌ เปิดเผยข้อมูลในการเปิดประมูลสินทรัพย์เพื่อชดใช้หนี้

เช่น

- ที่อยู่สำหรับจัดส่งสินค้า อีเมล์สำหรับส่งใบเสร็จ
- ข้อมูลบัตรเครดิตสำหรับจอง โรงแรม

ฐานความยินยอม (Consent)

ทางเลือก ของเจ้าของข้อมูล

- ให้ก่อนที่จะเก็บรวบรวมข้อมูล
- ไม่เป็นเงื่อนไขของการให้บริการหรือแยกส่วนออกจากการให้บริการ
- วัตถุประสงค์เฉพาะเจาะจง โดยเข้าถึงได้ เข้าใจง่าย
- มีทางเลือกให้ปฏิเสธได้ หรือ ถอนได้โดยไม่เสียประโยชน์

- ✓ ควรเป็น **Opt-in** เสมอ !
- ❌ **Pre-ticked** ใช้ไม่ได้ !
- ❗ **Opt-out** อาจใช้ได้เฉพาะบางบริบท (เช่น ลูกค้าเก่า)

เช่น

- อีเมล์สำหรับการส่งจดหมายข่าว
- ข้อมูลบัตรเครดิตที่เลือกให้เว็บไซต์ จำไว้เพื่อความสะดวกในการจ่ายเงิน ครั้งต่อไป

ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

(ผู้ควบคุมข้อมูล) ปฏิบัติตามกฎหมายที่ต้องทำอยู่แล้ว

เช่น

- บริษัทแจ้งข้อมูลการจ่ายเงินเดือน พนักงานต่อสรรพากร
- องค์กรทางการเงินส่งข้อมูลการ ทำธุรกรรมที่น่าสงสัยให้หน่วยงาน ปราบปรามการฟอกเงิน

ฐานภารกิจของรัฐ (Public Task)

(เจ้าหน้าที่) ปฏิบัติหน้าที่เพื่อบรรลุภารกิจสาธารณะ

เช่น

- สรรพากรประมวลผลข้อมูลเงินเดือน
- หน่วยงานปราบปรามการฟอกเงิน ประมวลผลข้อมูลธุรกรรมที่น่าสงสัย เพื่อนำไปตรวจสอบต่อ

ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)

ความเสี่ยงสูง ควรใช้ในกรณีที่ใช้ฐานอื่นไม่ได้ (ไม่เหมาะสม)

ใช้เท่าที่จำเป็น (ใช้ให้น้อยที่สุด)

- จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมาย (Expectation)ได้อย่างสมเหตุสมผล
- ต้องระบุให้ได้ว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับ อะไรคือความจำเป็นของการประมวลผลประกอบกับมีหน้าที่ในการปกป้องเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สมดุลกับประโยชน์อันชอบธรรมที่จะได้รับ

ตัวอย่าง : การยืนยันตัวตนลูกค้า ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย ข้อมูลเพื่อการปรับปรุงการให้บริการ การรักษาความปลอดภัยของระบบและเครือข่าย ฯลฯ

ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

- ✅ ใช้ได้เฉพาะข้อมูลที่ไม่ใช่ **sensitive data** เช่น ข้อมูลสิทธิการรักษา พยาบาล ข้อมูลการเดินทาง ไปประเทศที่มีโรคติดต่อ
- ✅ ใช้เมื่ออยู่ในสถานการณ์ที่ขอความยินยอมไม่ได้เท่านั้น หากขอความยินยอมได้ให้ใช้ความยินยอม

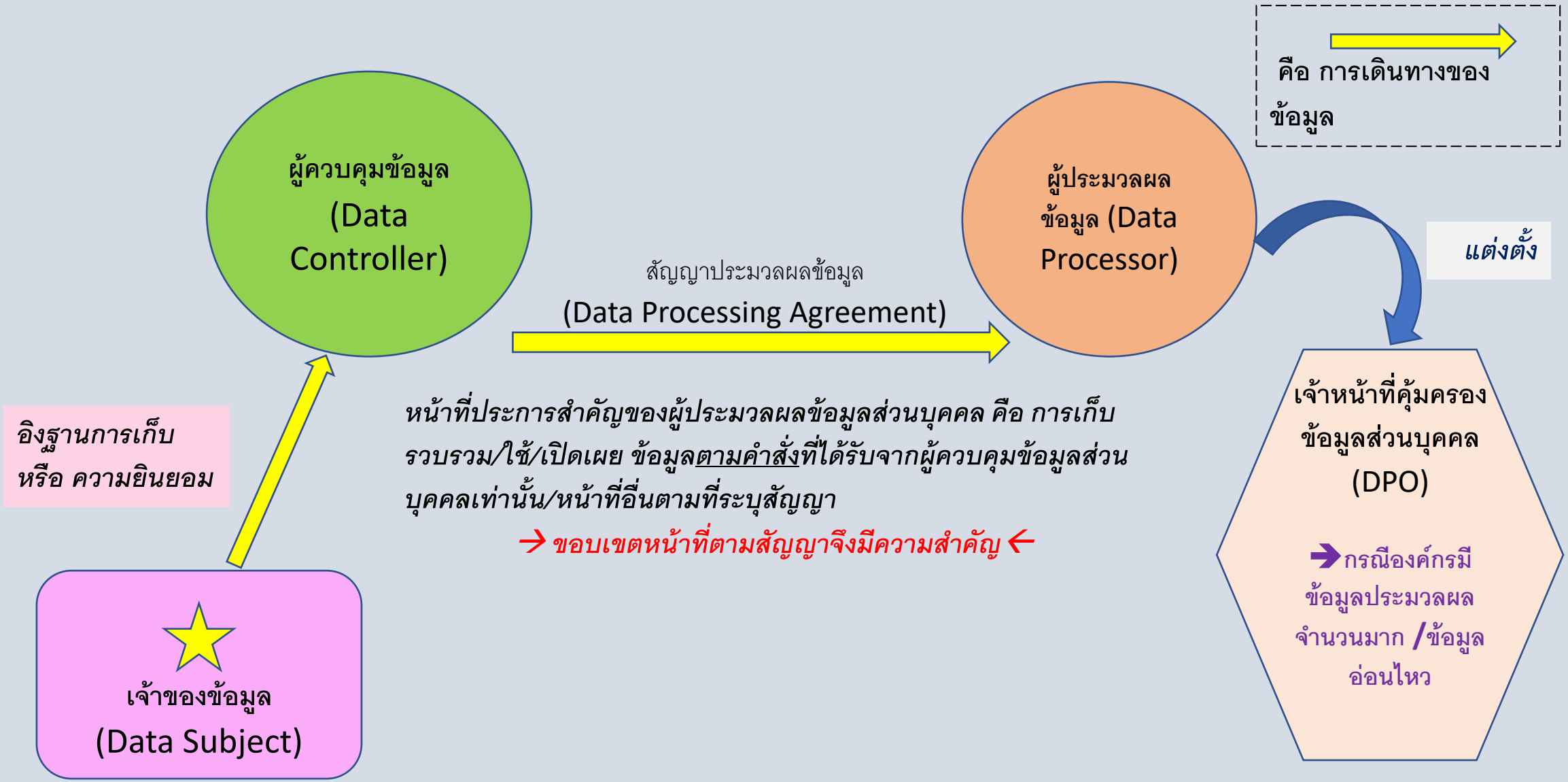
ฐานจดหมายเหตุ/วิจัย/สถิติ

- ✅ ควรเป็นไปตามมาตรฐานการวิจัย หรือมาตรฐานวิชาชีพ
- ✅ ต้องมี **Safeguard** (รอประกาศของกระทรวง)

นิยาม:ใครคือใคร?

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject):** บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller):** บุคคล/นิติบุคคลซึ่งมีอำนาจ ผู้ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือ เปิดเผย มีมาตรการดูแลความมั่นคงปลอดภัยที่เหมาะสม และทบทวนสม่ำเสมอ
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) :**บุคคล/นิติบุคคลที่เป็นคนละคนกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเก็บ ใช้ เปิดเผยตามคำสั่งของผู้ควบคุม
- **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) :** ผู้ที่ถูกแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองกรณีที่องค์กร/หน่วยงานมีข้อมูลประมวลผลจำนวนมาก/ข้อมูลที่มีความอ่อนไหว

ความสัมพันธ์ระหว่างผู้ควบคุม ผู้ประมวล และ DPO



สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. ได้รับการแจ้งให้ทราบ
2. ขอเข้าถึงข้อมูลส่วนบุคคลของตน
3. คัดค้านการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล
4. ขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
5. ขอให้ระงับการใช้ข้อมูลส่วนบุคคล
6. ขอให้แก้ไขข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล (**Data Controller**) จะต้องปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล

เว้นแต่ เป็นไปตามข้อยกเว้นที่กฎหมายกำหนด เช่น เป็นการปฏิเสธตามกฎหมาย หรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น เป็นต้น

ผู้ควบคุมข้อมูล
Data Controller

- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ
- จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา
- แจ้งเหตุละเมิดให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบอย่างไม่ชักช้า(ไม่เกิน 72 ชั่วโมง)
- กรณีการละเมิดที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล ต้องแจ้งเหตุแห่งการละเมิดพร้อมแนวทางการเยียวยาให้เจ้าของข้อมูลทราบโดยไม่ชักช้า
- หน้าที่โดยตรงที่จะต้องปฏิบัติตามการใช้สิทธิตามกฎหมายของเจ้าของข้อมูล

→ ความรับผิดสูงเพราะเป็นผู้รับผิดชอบโดยตรง

ผู้ประมวลผลข้อมูล
Data Processor

- ประมวลผลข้อมูล*ตามข้อตกลง*ระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล (ในกรณีที่ผู้ควบคุมไม่ได้ทำการประมวลผลด้วยตนเอง)
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ
- แจ้งเหตุละเมิดให้ผู้ควบคุมข้อมูลทราบ

→ ความรับผิดไม่สูงเท่าผู้ควบคุมเพราะเป็นเพียงผู้ที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามที่ผู้ควบคุมข้อมูลจ้าง

→ แต่จุดสำคัญ คือ หากกระทำการนอกเหนือขอบเขตคำสั่งการของผู้ควบคุม ผู้ประมวลผลจะถือเป็นผู้ควบคุมข้อมูลส่วนทำนอกขอบเขต = รับผิดเท่าผู้ควบคุมข้อมูล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
DPO

- องค์กรที่มีบุคลากรจำนวนมาก ต้องมีการแต่งตั้งมอบหมายเจ้าหน้าที่ให้ดูแล ประสานงาน ตรวจสอบ และให้คำแนะนำเรื่องความมั่นคงปลอดภัยของข้อมูลโดยเฉพาะ

คุณสมบัติ

จะเป็นพนักงาน/ลูกจ้าง /ผู้รับจ้างตามสัญญาให้บริการก็ได้ แต่ควรมีความรู้ด้าน PDPA เข้าใจกิจกรรมการประมวลผลและงาน IT & Security

→ ไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืน PDPA เพราะผู้ที่ต้องรับผิดชอบได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล (แล้วแต่กรณี)

→ แต่หากได้รู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่แล้วทำการเปิดเผยแก่ผู้อื่นโดยไม่มีกฎหมายรองรับ/ผิดกฎหมาย = ระวางโทษอาญา

แนวทางปฏิบัติของผู้ควบคุมข้อมูล (Data Controller)

- ❑ **มาตรการ:** ต้องมีมาตรการเชิงเทคนิค (Technical Measure) และมาตรการในเชิงบริหารจัดการ (Organizational Measure)
- ❑ **การป้องกัน:** ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลอื่น จะต้องป้องกันไม่บุคคลอื่นนั้นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ/โดยมิชอบ
- ❑ **การดำเนินการตามสิทธิเจ้าของข้อมูล:** หน้าที่โดยตรงที่จะดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามที่เจ้าของข้อมูลร้องขอ
- ❑ **การแจ้ง:** ต้องแจ้งเจ้าของข้อมูลเกี่ยวกับการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล เช่น วัตถุประสงค์ ระยะเวลาในการจัดเก็บ (และ นโยบายความเป็นส่วนตัว รายละเอียดการติดต่อของบริษัท ตัวแทนบริษัท หรือ DPO หากมี)
- ❑ **ระยะเวลาในการแจ้ง:**

การเก็บรวบรวม - ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูล กรณีทำการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลโดยตรง
- ต้องแจ้งภายในระยะเวลาตามสมควรแต่ไม่เกิน 30 วันนับแต่วันเก็บรวบรวมข้อมูล กรณีรับข้อมูลส่วนบุคคลจากแหล่งอื่น

การใช้ - ต้องแจ้งเจ้าของข้อมูลอย่างช้าเมื่อมีการติดต่อสื่อสารกันครั้งแรก กรณีการใช้ข้อมูลเพื่อการสื่อสารกับเจ้าของข้อมูล

การเปิดเผย - จะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก กรณีคาดหมายได้ว่า จะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม

การเปลี่ยนแปลง - ควรต้องแจ้งก่อนการมีผลของการเปลี่ยนแปลงของข้อมูลนั้นๆ หรือโดยเร็วที่สุด เมื่อมีการเปลี่ยนแปลงของข้อมูลที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลที่เคยแจ้งให้เจ้าของข้อมูลทราบ

➔ **ข้อยกเว้นให้ไม่ต้องแจ้ง:**

1. เจ้าของข้อมูลมีข้อมูลทราบวัตถุประสงค์หรือรายละเอียดนั้นอยู่แล้ว
2. ผู้ควบคุมข้อมูลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือข้อมูลดังกล่าวไม่สามารถกระทำได้
3. จำเป็นต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งก็ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูล
4. ผู้ควบคุมข้อมูลล่วงรู้หรือได้มาซึ่งข้อมูลจากหน้าที่/การประกอบอาชีพและต้องรักษารายละเอียดไว้เป็นความลับตามที่กฎหมายกำหนด

แนวทางปฏิบัติของผู้ประมวลผลข้อมูล (Data Processor)

- **มาตรการ:** - ต้องมีมาตรการเชิงเทคนิค (Technical Measure) และเชิงบริหารจัดการ(Organizational Measure) เพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การประมวลผลโดยปราศจากอำนาจหรือโดยมิชอบ
  - ต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่งปฏิบัติงานภายใต้อำนาจของผู้ประมวลผลข้อมูลและเข้าถึงข้อมูลได้ ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ประมวลผลข้อมูล
  - แม้ไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลเมื่อเจ้าของข้อมูลร้องขอให้ดาเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูล แต่ต้องจัดให้มีมาตรการต่างๆ ที่เพียงพอสำหรับการรองรับให้ผู้ควบคุมข้อมูลปฏิบัติหน้าที่เมื่อเจ้าของข้อมูลร้องขอ
- **การแจ้ง:** - แจ้งเสนอทางเลือกให้แก่ผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า
  - แจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล
- **ระยะเวลาในการแจ้ง:** กรณีข้อมูลส่วนบุคคลรั่วไหล แจ้งผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากได้ทราบ
- บันทึกรายการประมวลผลข้อมูลที่จัดให้มีจะต้องทำเป็นลายลักษณ์อักษรและมีรายละเอียดที่ประกอบไปด้วย
  1. ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูลที่ผู้ประมวลผลข้อมูลทำการแทน
  2. ประเภทของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล
  3. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

➔ **ข้อยกเว้น:**

1. กรณีข้อมูลส่วนบุคคลรั่วไหล ผู้ประมวลผลข้อมูลไม่มีหน้าที่แจ้งเจ้าของข้อมูล เว้นแต่ผู้ควบคุมข้อมูลมอบหมายให้ทำโดยอาศัยสัญญาระหว่างผู้ควบคุมและผู้ประมวลผล
2. กิจการขนาดเล็กอาจได้รับยกเว้นไม่ต้องจัดทำบันทึกประมวลผลข้อมูล ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด <u>แต่หากมีการ</u>เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เสี่ยงกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหรือดำเนินการเกี่ยวกับกับข้อมูลอ่อนไหว จะไม่ได้รับยกเว้น

แนวทางปฏิบัติที่เกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

❑ **การแต่งตั้ง:** กรณีที่องค์กรหรือหน่วยงานมีข้อมูลประมวลผลจำนวนมาก หรือข้อมูลอ่อนไหว จำเป็นต้องแต่งตั้งเจ้าหน้าที่ DPO เข้ามาทำหน้าที่ในการประสานงาน ตรวจสอบ ให้คำแนะนำ และ ดูแลด้านความมั่นคงปลอดภัยของข้อมูลโดยเฉพาะ โดยมีหลักปฏิบัติในการแต่งตั้ง คือ

ผู้แต่งตั้ง - ผู้ประมวลผลข้อมูล หรือ หน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด หรือ ผู้ที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลที่มีความอ่อนไหว

แต่งตั้งร่วม - หากหลายหน่วยงานรัฐหรือบริษัทในเครือแต่งตั้งร่วมกัน จะต้องทำการติดต่อได้โดยง่าย

❑ **การปฏิบัติหน้าที่:** 1. ควรมีมาตรการเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ หากปฏิบัติภารกิจอื่นด้วยในองค์กร ก็ต้องไม่มีความขัดแย้ง (Conflict of Interest) คือ จะเป็นบุคคลคนเดียวกับผู้บริหารองค์กรในระดับสูงอย่างประธานเจ้าหน้าที่บริหาร (CEO) ผู้จัดการฝ่ายการตลาด หรือหัวหน้าฝ่ายบุคคลไม่ได้

2. ต้องสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรได้ แม้ในกรณีที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังกล่าวจะเป็นพนักงาน หรือลูกจ้างของบริษัท ซึ่งได้รับการแต่งตั้ง
3. ต้องทำการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
4. ต้องรักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่
5. บริษัทผู้ประมวลผลและผู้ควบคุมข้อมูลต้องให้การสนับสนุนการทำงานและได้รับการอำนวยความสะดวกอย่างเพียงพอ เช่น ให้เวลาและจัดหาทรัพยากรให้เพียงพอในการทำงาน และมีการฝึกอบรมอย่างต่อเนื่อง

➔ ใบรับรอง: ปัจจุบันยังไม่มีกำหนดว่าต้องมีใบรับรอง สามารถเป็นบุคลากรในองค์กร แต่ควรจะให้มีแนวปฏิบัติที่อธิบายข้างต้น

ความรับผิดและโทษทางแพ่งและทางอาญา

ทางแพ่ง

ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และทำให้เกิดความเสียหายต้องรับผิดต่อเจ้าของข้อมูลส่วนบุคคล

- ชดใช้ค่าสินไหมทดแทนที่แท้จริง
- ชดใช้ค่าสินไหมทดแทนเพื่อการลงโทษ ไม่เกิน **2** เท่าของค่าสินไหมทดแทนที่แท้จริง

อายุความ

3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิด

10 ปี นับแต่วันที่มีการละเมิดข้อมูล

ทางอาญา

ผู้ต้องรับโทษ : การกระทำผิดของนิติบุคคลที่เกิดจากการสั่งการ/ละเว้นไม่สั่งการ/ไม่กระทำการของกรรมการ/ผู้จัดการ บุคคลนั้นต้องรับโทษ

- ใช้หรือเปิดเผยข้อมูลที่ได้รับนอกวัตถุประสงค์
- ใช้หรือเปิดเผยข้อมูลอ่อนไหว โดยไม่ได้รับความยินยอม
- ส่ง/โอนข้อมูลส่วนบุคคลที่อ่อนไหวไปยังต่างประเทศโดยไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. จำคุกไม่เกิน **6** เดือน หรือปรับ **500,000** บาท หรือทั้งจำทั้งปรับ
2. หากทำเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น

จำคุกไม่เกิน **1** ปี หรือปรับ **1,000,000** บาท หรือทั้งจำทั้งปรับ

โทษทางปกครอง

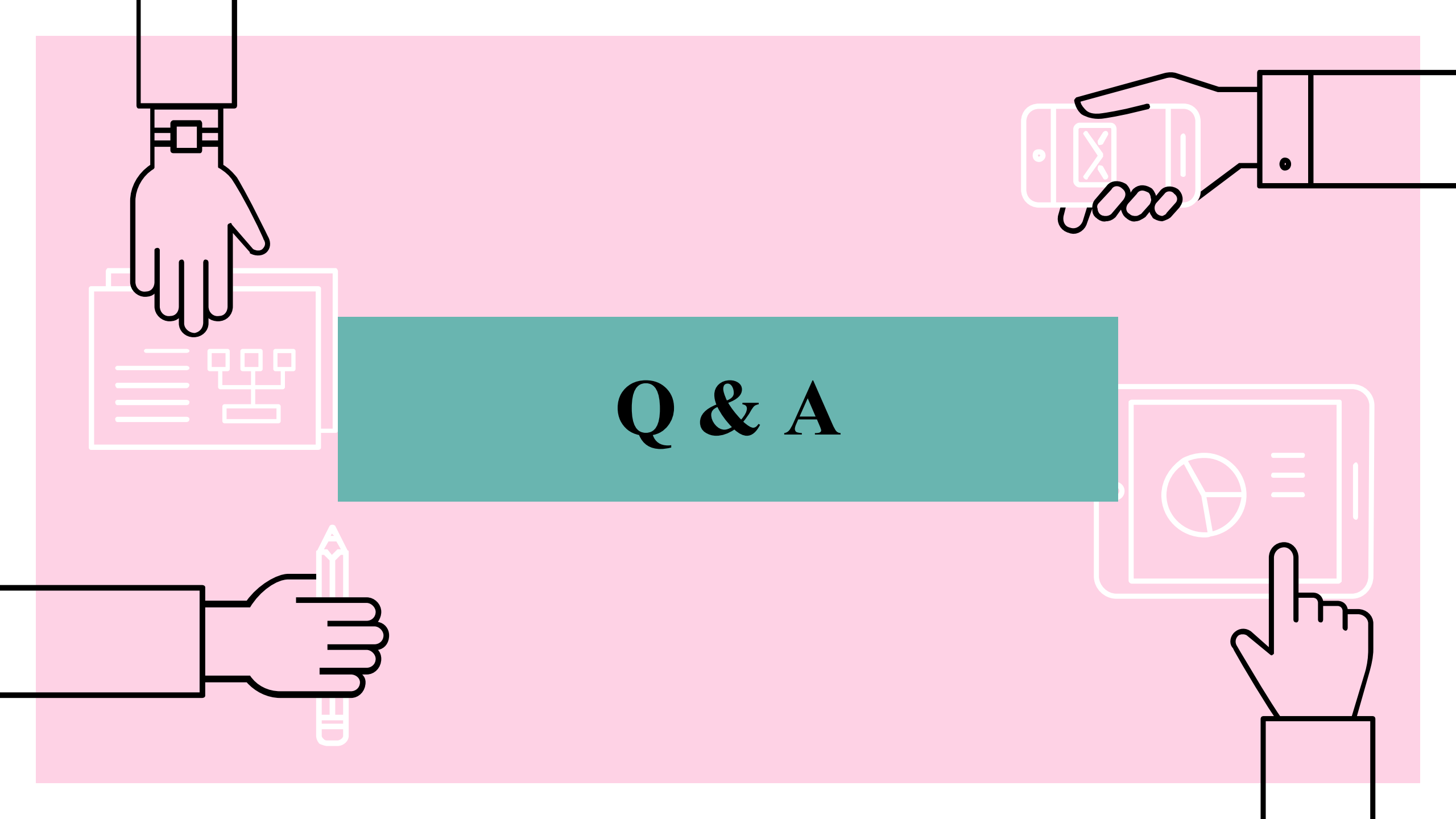
ผู้ควบคุมข้อมูลส่วนบุคคล : ปรับสูงสุดไม่เกิน 5 ล้านบาท

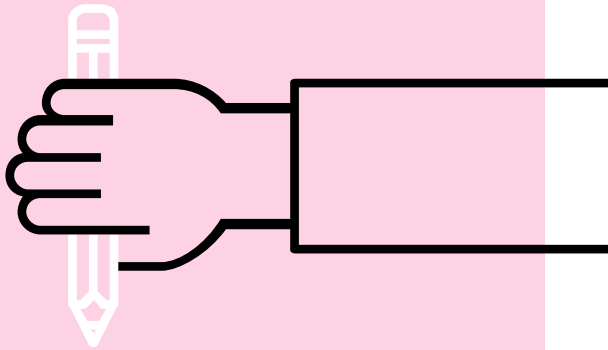
ผู้ประมวลผลข้อมูลส่วนบุคคล: ปรับสูงสุดไม่เกิน 5 ล้านบาท

ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล/ตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคล: ปรับสูงสุดไม่เกิน 1 ล้านบาท

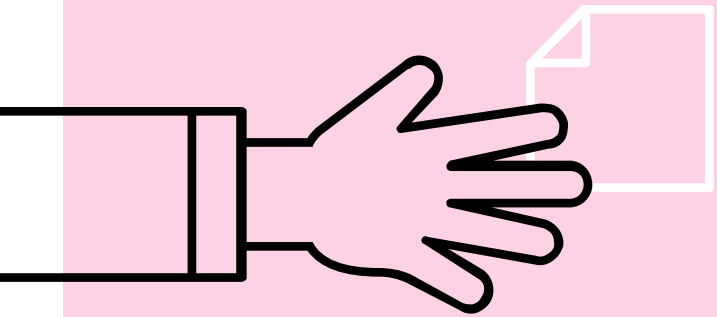
การเตรียมความพร้อมของหน่วยงานภายใน

1. นัดประชุมผู้ที่เกี่ยวข้อง
2. ทุกหน่วยงานสำรวจ รวบรวม การเก็บข้อมูล เพื่อเตรียมความพร้อม ดำเนินงานให้สอดคล้องกับ PDPA โดยทำ Data Mapping
   - ที่มาของข้อมูล
   - ประเภทของข้อมูล
   - รูปแบบการได้มาของข้อมูลส่วนบุคคล
   - ฐานทางกฎหมาย
   - รูปแบบการใช้ รวบรวม เปิดเผย ข้อมูลส่วนบุคคล
   - แหล่งที่จะมีการโอนย้ายถ่ายข้อมูล


Q & A



เอกสารนี้เป็นเอกสารภายใน
ใช้เพื่อประกอบความรู้และความเข้าใจ
ของ บริษัท ทีซีซี แอสเซ็ทส์ (ประเทศไทย) จำกัด
และ
กลุ่มบริษัทในเครือเท่านั้น



ห้ามนำไปใช้นอกกลุ่มบริษัท