การประชุมทำความเข้าใจและรับรู้

Personal Data Protection Act

การคุ้มครองข้อมูลส่วนบุคคล

PDPA

30 พ.ค.2565

โดย กลุ่มเทคโนโลยีสารสนเทศ
กรมสนับสนุนบริการสุขภาพ

4 ขั้นตอนก้าวเข้าสู่ PDPA

1

เรียนรู้ก่อนว่า PDPA คืออะไร

2

การวางแผนเชิงนโยบาย

3

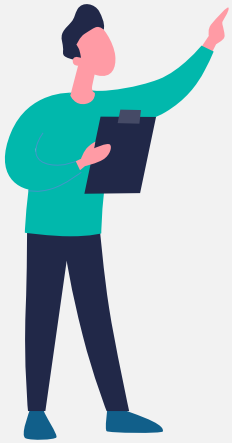
การร่าง/เขียนแนวทางปฏิบัติ

4

การควบคุม กำกับดูแล ติดตาม และประเมินผล

เนื้อหาในการประชุมฯ

1. อะไรคือข้อมูลส่วนบุคคล
2. ความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคล
3. ขอบเขตการบังคับใช้ PDPA
4. หลักการคุ้มครองข้อมูลส่วนบุคคล
5. หน้าที่ของ Data Controller
6. ฐานการประมวลผลข้อมูลส่วนบุคคล



7. หน้าที่ของ Data Processor และใครคือ DPO
8. การโอนข้อมูลส่วนบุคคลข้ามพรมแดน
9. สิทธิของเจ้าของข้อมูลส่วนบุคคล
10. องค์กรอิสระในการกำกับดูแลเรื่องข้อมูลส่วนบุคคล
11. กระบวนการร้องเรียนและบทลงโทษ
12. แนวทางการดำเนินการให้สอดคล้องกับ PDPA ในเบื้องต้น

อะไรคือข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)

ข้อมูลที่ทำให้สามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าโดยตรงหรือโดยอ้อม (สำหรับบุคคลที่ยังมีชีวิตอยู่) เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ บัตรประจำตัวประชาชน email ฯลฯ

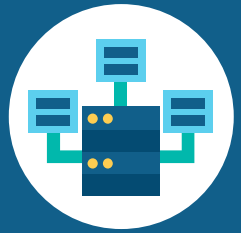
ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

+ เป็นข้อมูลที่จะต้องให้ความระมัดระวังเป็นพิเศษในการเก็บรวบรวม/ประมวลผล เช่น ข้อมูลที่บอกชาติพันธุ์ เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา ข้อมูลพันธุกรรม รสนิยมทางเพศ ข้อมูลชีวภาพ

+ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป

ความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคล

สาเหตุที่ต้องออก PDPA



สร้างความเชื่อมั่น (Trust)

ให้บุคคลทั่วไปมีความเชื่อมั่นที่จะให้ข้อมูลส่วนบุคคลกับองค์กร ไม่ว่าจะเป็นการเข้ารับบริการกับองค์กรใดๆ องค์กรนั้นจะเก็บรักษาข้อมูลส่วนบุคคลนั้นได้อย่างโปร่งใสและเป็นระบบ

ยกระดับการธรรมาภิบาลข้อมูล (Better data governance)

ทุกองค์กร (รัฐ/เอกชน) สามารถกำกับดูแลข้อมูลที่ดี ยิ่งดีเท่าไหร่ก็ยิ่งมีแนวโน้มว่าพวกเขาจะได้รับความไว้วางใจจากผู้ใช้และผู้บริโภคมากขึ้นเท่านั้น

ยกระดับสู่มาตรฐานสากล (Connecting with global standards)

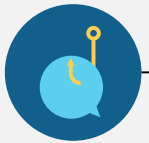
การถ่ายโอนข้อมูลทั่วโลกจำเป็นต้องเชื่อมต่อกับมาตรฐานการป้องกันระดับโลกเพื่อส่งเสริมการไหลเวียนของข้อมูลอย่างอิสระ

หลักการของ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3. สิทธิของเจ้าของข้อมูลส่วนบุคคล

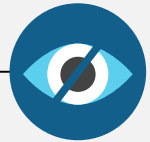
4. มีองค์กรกำกับดูแลเรื่องข้อมูลส่วนบุคคล

2. หลักการคุ้มครอง



5. การร้องเรียน

1. บังคับใช้กับใคร



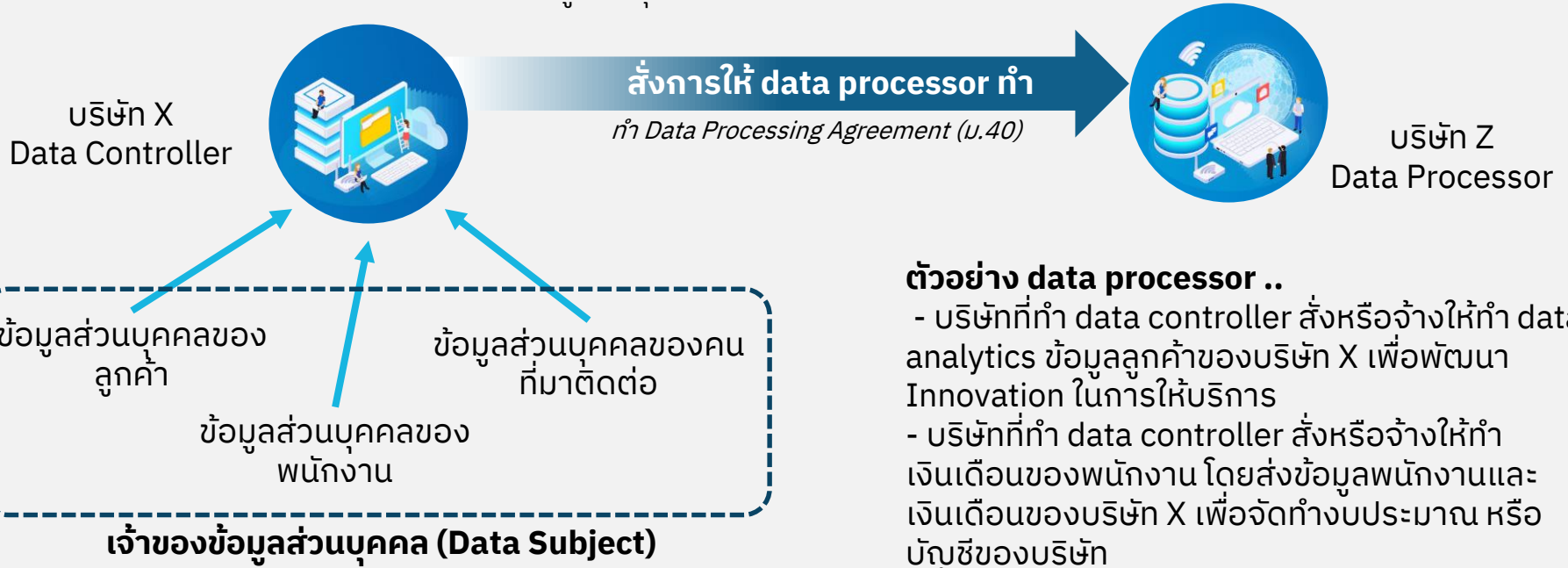
6. การลงโทษผู้ที่ไม่ปฏิบัติตามกฎหมาย

ขอบเขตการบังคับใช้ PDPA

ใครคือผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลธรรมดาหรือนิติบุคคลที่มีอำนาจสั่งการในการสั่งการหรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เจ้าของร้านถ่ายเอกสาร, บริษัทที่เก็บ-รวบรวม-ใช้-ประมวลผล-เปิดเผยข้อมูลส่วนบุคคลไว้

ใครคือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

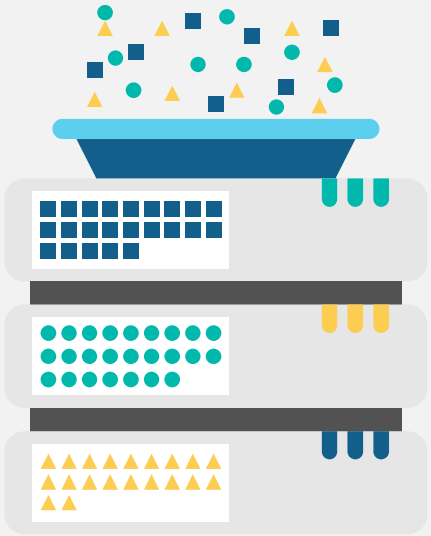


ตัวอย่าง data processor ..

- บริษัทที่ทำ data controller สั่งหรือจ้างให้ทำ data analytics ข้อมูลลูกค้าของบริษัท X เพื่อพัฒนา Innovation ในการให้บริการ
- บริษัทที่ทำ data controller สั่งหรือจ้างให้ทำเงินเดือนของพนักงาน โดยส่งข้อมูลพนักงานและเงินเดือนของบริษัท X เพื่อจัดทำงบประมาณ หรือบัญชีของบริษัท

ขอบเขตการใช้บังคับ (ม.5)

PDPA บังคับใช้กับ:



1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่ง**อยู่ในประเทศไทย** ไม่ว่ากิจกรรมการประมวลผลนั้นจะอยู่ในประเทศหรือนอกประเทศ

2. กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่**นอกประเทศไทย** PDPA จะบังคับใช้หากการดำเนินการนั้นเป็นการประมวลผลข้อมูลข้อมูลส่วนบุคคลของคนซึ่ง **อยู่ในประเทศไทย** เมื่อเป็นกิจกรรม:

   - เสนอขายสินค้าหรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศ
   - การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลเกิดขึ้นในประเทศ

Data controller หรือ Data processor ตามกรณีนี้ต้องตั้งตัวแทนในประเทศ (ม.37(5))

หลักการคุ้มครองข้อมูลส่วนบุคคล

หลักการในการเก็บ รวบรวม ประมวลผลข้อมูลส่วนบุคคลจะต้อง..

1. **Purpose limitation:** เก็บหรือใช้เท่าที่จำเป็นตามวัตถุประสงค์ที่แจ้งไว้ให้กับเจ้าของข้อมูลส่วนบุคคล

2. **Transparency:** ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล (Privacy notice) ก่อนที่บริษัทจะนำข้อมูลส่วนบุคคลมาใช้ (Inform)

3. **Security:** ให้ความมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล

มาตรการขององค์กรต้องสอดคล้องกับหลักการที่กล่าวมาด้วย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บริษัท X
Data Controller

เก็บ+ใช้+เปิดเผย
ข้อมูลส่วนบุคคลของ..

- ลูกค้า
- พนักงาน
- Vender หรือผู้มาติดต่อ

ทำสัญญา
Processing
Agreement

บริษัท Z
Data processor

บริษัท X สั่งหรือจ้างบริษัท Z ให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

ฐานกฎหมายที่ให้ใช้ข้อมูลได้ (Lawful basic) (ความชอบธรรมในการใช้ข้อมูลฯ ขององค์กร)

- **Consent:** เจ้าของข้อมูลส่วนบุคคลยินยอม
- **Contract:** เป็นความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่าง data controller และเจ้าของข้อมูลส่วนบุคคล (หากเจ้าของข้อมูลไม่เปิดเผยข้อมูลออกมาจะปฏิบัติตามสัญญาไม่ได้)
- **Legitimate interest:** เป็นผลประโยชน์อันชอบด้วยกฎหมายของ Data controller หรือบุคคลภายนอก (นำข้อมูลในบริษัทเองมาวิเคราะห์สถิติเพื่อส่งเสริมการขาย แต่ต้องไม่รุกล้ำความเป็นส่วนตัว)
- **ฐานอื่นๆ:** เช่น ใช้ข้อมูลส่วนบุคคลเพื่อการวิจัย หรือการปฏิบัติตามกฎหมาย ฯลฯ (กฎหมายสั่งให้ท่านเปิดเผยข้อมูลดังกล่าว)

หน้าที่ของ Data controller

+ Notice: (ม.23)
แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล

+ Appropriate Security: (ม.37 (1))
จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

+ Preventing unlawful disclosure: (ม.37(2)) ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

+ Data Chock and Data Subject Rights Management: (ม.37(3)) มีระบบตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็น และจัดการเรื่องการร้องขอของเจ้าของข้อมูลส่วนบุคคล

+ Breach Notification: (ม.37 (4)) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบ

+ Records of Processing Activity (ROPA): (ม.39) ทำบันทึกรายการกิจกรรมที่ใช้ข้อมูลส่วนบุคคล (เช่น ตารางนั้น เก็บข้อมูลอะไร, ประเภทไหน, เปิดเผยให้ใครบ้าง, มี Security อะไรบ้าง, ใครเข้าถึงได้บ้าง)

หลักฐานการใช้ Lawful Basis ที่สำคัญ

Lawful Basis	หลักการตามกฎหมาย PDPA 2562	หลักการใช้
1. Consent	เจ้าของข้อมูลยินยอมให้ใช้ข้อมูลส่วนบุคคล (ไม่ว่าจะเก็บ รวบรวม ใช้หรือเปิดเผย) (ม. 24 และ ม.26)	**PDPA ม. 19** กำหนดให้ . การขอความยินยอมต้องแจ้งให้**ชัดเจน**ว่าขอไปเพื่ออะไร . การขอความยินยอมต้องให้**อิสระ**กับเจ้าของข้อมูลในการให้หรือไม่ให้ความยินยอม . การขอความยินยอม ต้อง**แยกส่วนการขอความยินยอม**จากส่วนอื่นโดยชัดเจน . ถ้าการถอนความยินยอมกระทบการใช้งานในเรื่องใด **ให้แจ้งผลกระทบ**นั้นกับเจ้าของข้อมูลส่วนบุคคลด้วย
2. Contract	เป็นการปฏิบัติตาม**สัญญา**ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (ม. 24 (3) และ ม.26 (5)(ก))	รวมทั้งสัญญาที่เป็นลายลักษณ์อักษร และสัญญาที่ไม่เป็นลายลักษณ์อักษร
3. Legitimate interest	เป็นความ**จำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมาย** (Legitimate Interest) ของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอก (ม.24 (5) เช่น ประเมินการขึ้นเงินเดือนพนักงาน หรือรวบรวมสถิติโดยไม่ใช้ข้อมูลที่บ่งชี้ตัวตนของเจ้าของข้อมูล	. ประโยชน์ Legitimate interest จะต้องไม่ทำให้เกิดการลดทอนสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล . ถ้าไม่เกินความคาดหมายของเจ้าของข้อมูลส่วนบุคคล การดำเนินการนั้นน่าจะอ้างฐาน Legitimate Interest ได้
4. Legal obligation	เป็นการปฏิบัติตามกฎหมายที่ data controller ต้องปฏิบัติตาม เช่น ตำรวจร้องขอ หรือหน่วยงานรัฐร้องขอข้อมูล	

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บริษัท Z
Data Processor

สั่งการให้ data processor ทำ

บริษัท X
Data Controller

ตัวอย่าง data processor ..
- บริษัทที่ทำ data controller สั่งหรือจ้างให้ทำ data analytics ข้อมูลลูกค้าของบริษัท X เพื่อพัฒนา Innovation ในการให้บริการ
- บริษัทที่ทำ data controller สั่งหรือจ้างให้ทำเงินเดือนของพนักงาน โดยส่งข้อมูลพนักงานและเงินเดือนของบริษัท X เพื่อจัดทำงบประมาณ หรือบัญชีของบริษัท

ข้อมูลส่วนบุคคลของลูกค้า

ข้อมูลส่วนบุคคลของคนที่มาติดต่อ

ข้อมูลส่วนบุคคลของพนักงาน

หน้าที่ของ Data Processor

+ ดำเนินการ**ตามคำสั่ง**ที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล

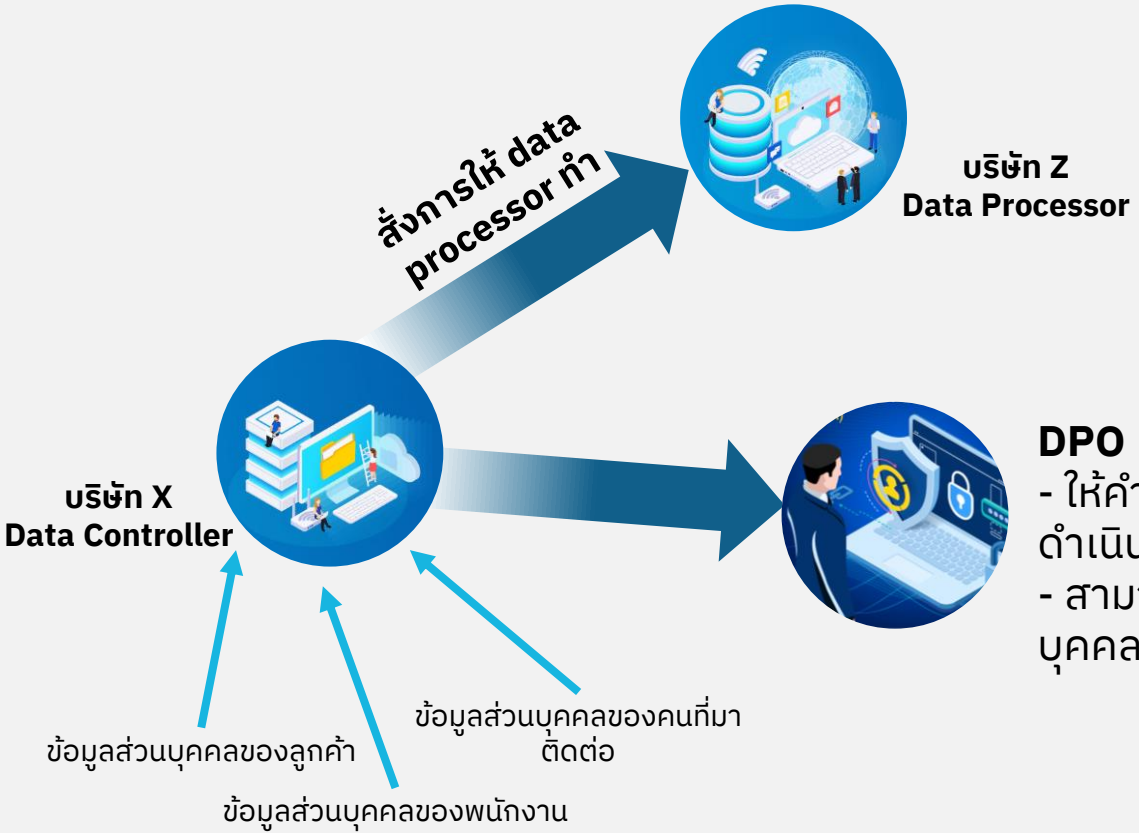
+ จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัย**ที่เหมาะสม

+ **แจ้งเหตุละเมิดข้อมูลส่วนบุคคล**ให้ data controller ทราบ

+ ทำ**บันทึกรายการ**การประมวลผลข้อมูล

ระหว่าง Data Controller และ Data Processor ต้องมีสัญญาระหว่างกันเพื่อระบุหน้าที่ที่ต้องทำ หากไม่ทำนอกคำสั่ง, ไม่มีมาตรฐานความมั่นคง, ไม่แจ้งเหตุละเมิดข้อมูลให้ Controller ทราบ (หากมีเหตุเกิดขึ้น), และไม่ทำ ROPA (Record of Processing Activity) – Data Processor ต้องเป็นฝ่ายรับผิด

ใครคือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)



DPO
- ให้คำปรึกษา Data controller เพื่อให้การดำเนินการเป็นไปตาม พ.ร.บ.
- สามารถเป็นแผนกในองค์กร หรือจ้างบุคคลภายนอกได้

หน่วยงานใดต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และหน้าที่ของ DPO

หน่วยงานใดต้องจัดให้มี DPO

1. หน่วยงานของรัฐ ตามที่ประกาศกำหนด

2. หน่วยงานที่การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด

3. หน่วยงานที่มีกิจกรรมหลักเป็นการเก็บรวบรวมใช้ หรือเปิดเผย Sensitive Personal Data (เช่น โรงพยาบาล)

(ข้อ 1., 2. รอกฎหมายลูก-ประกาศคณะกรรมการ)

หน้าที่ของ DPO

1. ให้คำแนะนำ Data controller

2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวมการใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

3. ประสานงานและให้ความร่วมมือกับสำนักงานฯ

4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

คณะกรรมการ DPO ในองค์กรควรประกอบไปด้วย ฝ่ายกฎหมาย ฝ่ายไอที ฝ่ายบริหารกิจการ/สำนักงาน และมีอำนาจในการสั่งการในองค์กรได้

การโอนข้อมูลส่วนบุคคลข้ามพรมแดน

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศ ที่รับข้อมูลส่วนบุคคล**ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ** (ตามประกาศคณะกรรมการ- รอกฎหมายลูก)

. เว้นแต่ (ม.28)..

.. เป็นการ**ปฏิบัติตามกฎหมาย**
.. ได้รับความยินยอมจากเจ้าของข้อมูล (ต้องแจ้งหากปลายทางยังไม่มี PDPA เจ้าของต้องทราบ)
.. การปฏิบัติตามสัญญาซึ่ง **data subject เป็นคู่สัญญา** หรือดำเนินการตาม**คำขอของ data subject** ก่อนเข้าทำสัญญา
.. ทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับบุคคลหรือนิติบุคคลอื่น **เพื่อประโยชน์ของ data subject**
.. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ
.. ประโยชน์สาธารณะที่สำคัญ

การโอนข้อมูลส่วนบุคคลข้ามพรมแดน

Binding Corporate Rules (BCR)
(เป็นข้อยกเว้นอีกกรณีหนึ่ง-บังคับตามบริษัทแม่ที่อยู่ในประเทศไทย)

กำหนดหลักการเกี่ยวกับกฎเกณฑ์การให้**ความคุ้มครองข้อมูลส่วนบุคคลไปยังต่างประเทศและ อยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกัน**เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากมีนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สามารถโอนข้อมูลไปยังต่างประเทศได้

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

1. สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access)
2. สิทธิ์ในการขอให้โอนข้อมูลส่วนบุคคลไปยัง data controller อื่น (Right to data portability)
3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
4. สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restrict processing)
5. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure)

Data Controller มี**สิทธิ์ที่จะปฏิเสธคำขอสิทธิ์นั้นได้** หรือไม่สามารถจะทำให้ได้ หรือยังมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลดังกล่าวนั้น เพื่อปฏิบัติตามสัญญาอยู่

องค์กรอิสระในการกำกับดูแลเรื่องข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

ให้เป็นองค์กรอิสระในการกำกับดูแลเพื่อ:

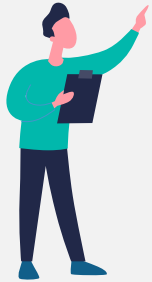
. ส่งเสริมมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
. สนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคล
. ส่งเสริมและสนับสนุนงานวิจัย
. ประสานงานกับหน่วยงานในประเทศและต่างประเทศ
. ให้คำปรึกษา และเป็นศูนย์กลางในการบริการวิชาการ
. กำหนดหลักสูตรและการฝึกอบรม
. ติดตามประเมินผลการดำเนินงานตาม พ.ร.บ.

กระบวนการร้องเรียนโดยเจ้าของข้อมูลส่วนบุคคลใน PDPA

1

Complaints

เจ้าของข้อมูลส่วนบุคคลร้องเรียนต่อ สคส. และคณะกรรมการผู้เชี่ยวชาญของ สคส. พิจารณาเรื่องร้องเรียน



2

Settlement process

คู่กรณีไกล่เกลี่ยข้อพิพาท

(ถ้าไกล่เกลี่ยได้ ข้อพิพาทยุติ)

(ถ้าไกล่เกลี่ยไม่ได้)

3

Soft-enforcement

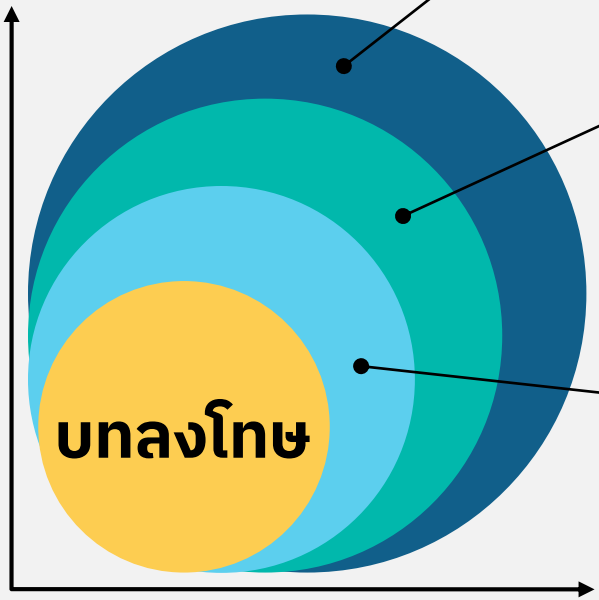
สคส. มีคำสั่งให้ดำเนินการแก้ไขการกระทำ/สั่งห้ามกระทำการเพื่อระงับความเสียหาย

(ถ้ายังไม่เป็นผล)

4

Hard sanction

สคส. สั่งปรับทางปกครอง



1. ความรับผิดทางแพ่ง

(เมื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น) ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

2. โทษทางอาญา

(โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท)

(เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดทำให้เกิดการเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย สามารถยอมความได้

3. การปรับทางปกครอง

(1-5 ล้านบาท)

คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้ โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม. 90) เช่น ไม่ทำ ROPA หรือทำแต่ไม่สมบูรณ์

เปรียบเทียบบทลงโทษของประเทศไทยกับประเทศอื่น

EU's GDPR
(General Data Protection Regulation)

for severe violations up to **€Million 20** or **4% of annual global turnover**, whichever is higher

Singapore's PDPA

up to 1 million SG dollars ~ 22 million THB

Thailand's PDPA

up to 5 million THB

Malaysia's PDPA

up to 500,000 RM ~ 4 million THB

GDPR and UK cases

Featured cases of fines imposed by Data Protection Agencies

H&M fined by DPA Humburg  (10/2020) **£Million 35.2**
Insufficient legal basis for data processing
บริษัทได้ทำการเก็บรวบรวมและสัมภาษณ์ข้อมูลส่วนตัวของพนักงาน เช่น ปัญหาชีวิตส่วนตัว, ภาวะการเจ็บป่วย, ปัญหาครอบครัว, ความคิดเห็นทางศาสนา, ความคิดเห็นทางการเมือง เก็บไว้ในไดร์ฟที่แชร์ให้กับผู้จัดการถึง 50 คนทราบ และไม่ได้ขอความยินยอมจากเจ้าของ
British Airways fined by ICO  (07/2019) **£Million** 204
Basis: inadequate security measures to prevent large scale of user data's harvesting
British airways โดนปรับ 204,600,000 euro เนื่องจากข้อมูลลูกค้าที่ลงทะเบียนใน website ของ British airways ถูก divert ไป website ปลอมที่ hacker สร้างขึ้นเพื่อเก็บเกี่ยวข้อมูลของลูกค้า โดยรวมแล้วลูกค้าประมาณ 500,000 คน ถูกล้วงข้อมูลไป ผู้กำกับดูแลพบว่าบริษัท British airways มีการจัดการด้าน security ในระดับต่ำ ทำให้เกิดเหตุการณ์นี้ขึ้น
Google fined by CNIL  **£Million** 50
Basis: Forced consent and lack of transparency
Google โดนปรับ 50,000,000 euro เนื่องจากการตั้งค่าในโทรศัพท์ระบบ Android มีการให้ผู้ใช้ต้องสร้างบัญชี Google ขึ้นมา แต่การที่ Google สามารถนำข้อมูลผู้ใช้ไปทำอะไรได้บ้าง Google ไม่ได้บอกผู้ใช้ให้กระจ่าง และการขอความยินยอมก็ใช้ภาษาคลุมเครือ ไม่ได้บอกอย่างชัดเจนว่าจะนำข้อมูลผู้ใช้ไปทำอะไร จึงขัดกับข้อกฎหมายของ GDPR ว่าการขอความยินยอมต้องอธิบายเจ้าของข้อมูลอย่างชัดแจ้งว่าจะนำข้อมูลไปทำอะไร

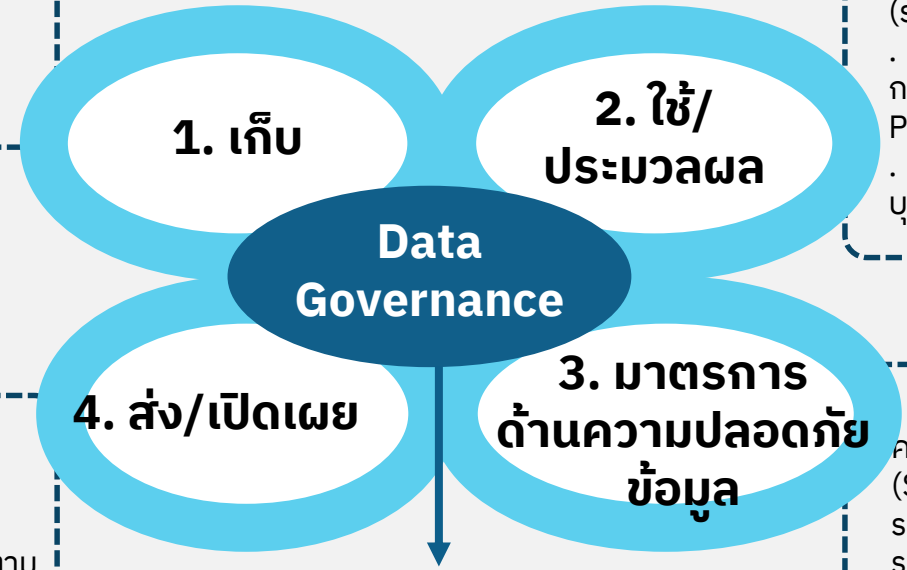
ตัวอย่างการลงโทษบริษัทในยุโรปตามกฎหมาย GDPR

1. สำนักงานทะเบียนที่ดิน (Government Office Managing the Real Estate Register) โดนปรับ 1,715 euro เนื่องจาก สนง. ได้ส่งเอกสารคำตัดสินเรื่องการเปลี่ยนแปลงผู้เช่าอสังหาริมทรัพย์ไปให้ผู้ให้เช่า และในคำตัดสินนั้นมีการเปิดเผยข้อมูลส่วนบุคคลของผู้เป็นเจ้าของอสังหาริมทรัพย์ทุกคนที่เคยได้ทำสัญญากับผู้เช่าในอดีต
Government Office Managing the Real Estate Register - **HUNGARY** 2019-08-08
2. เทศบาลเมือง Horsholm Municipality โดนปรับ 7,000 euro เนื่องจากมีเจ้าหน้าที่เทศบาลทำคอมพิวเตอร์ของสำนักงานหาย และคอมพิวเตอร์นั้นมีข้อมูลส่วนบุคคลของพนักงานของเทศบาลมากกว่า 1,600 คน ประกอบไปด้วยข้อมูลส่วนบุคคลที่อ่อนไหวและหมายเลขประกันสังคม
Horsholm Municipality - **DENMARK** 2020-03-10
3. โรงเรียนในสวีเดนโดนปรับ 18,630 euro เนื่องจากใช้เทคโนโลยีแสกนใบหน้าของนักเรียน (Facial recognition) ในการตรวจสอบการเข้าเรียน (Attendance) โดยที่ไม่มีการประเมินความเสี่ยง (DPIA: Data Protection Impact Assessment) ก่อน ผู้กำกับดูแลเห็นว่าการดำเนินการแบบนี้เกินความจำเป็น และโรงเรียนไม่ได้ดำเนินการประเมินความเสี่ยงก่อนที่จะใช้เทคโนโลยีนี้
Swedish school - **SWEDEN** 2019-08-20
4.โรงพยาบาลในประเทศโปรตุเกสโดนปรับ 400,000 euro เนื่องจากพบว่ามีการใช้โปรไฟล์ปลอมในการเข้าถึงข้อมูลคนไข้ (ซึ่งเป็นข้อมูลอ่อนไหว) และพบว่าระบบ IT security ของโรงพยาบาลไม่มีความปลอดภัยเพียงพอ นอกจากนี้พบว่ามีโปรไฟล์ของคนที่เป็นแพทย์ในระบบถึง 985 คน ทั้งๆ ที่แพทย์ในโรงพยาบาลมีแค่ 296 คน
Portugal hospital - **PORTUGAL** 2018-07-17

Conclude

. แจ้งเจ้าของข้อมูลส่วนบุคคลว่าวัตถุประสงค์ในการเก็บ/ใช้คืออะไร โดยแจ้งผ่านเอกสารการแจ้งการประมวลผล (Privacy Notice)

. กำหนดแนวทาง/นโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (standard operating procedure)
. บันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บ/ใช้ (Records of Processing. Activity: ROPA)
. ห้ามเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่ไม่มีความรับผิดชอบโดยตรง



. ทำสัญญา/ข้อตกลงกับบุคคลภายนอก หรือทำ data processing agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมาย
. ในกรณีโอนข้อมูลไปต่างประเทศ มีสัญญากับบริษัทปลายทางเพื่อคุ้มครองข้อมูลตามมาตรฐาน PDPA

. กำหนดแนวทางด้านมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Security) เช่น access control, security assessment, security policy
. กำหนดนโยบายระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล

. มีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล (data subject right)
. มีกระบวนการ Brach notification protocol
. Data protection officer (DPO) ที่ให้คำปรึกษากับองค์กร และดูแลการดำเนินการให้เป็นไปตามกฎหมาย
. อบรม (Training) ให้พนักงานมีความเข้าใจ

แนวทางปฏิบัติของกรมสนับสนุนบริการสุขภาพ

1

ทำความเข้าใจ

1. ประชุมทำความเข้าใจ และ รับรู้
2. แต่งตั้ง กก.คุ้มครองข้อมูลฯ + คณะอนุกรรมการดำเนินงานคุ้มครองข้อมูลฯ
3. จัดทำร่างแนวทางปฏิบัติฯ

2

ร่างนโยบายฯ

นโยบาย แนวทางปฏิบัติ และ แต่งตั้ง DPO , DC , DP

3

กำหนดขอบเขต

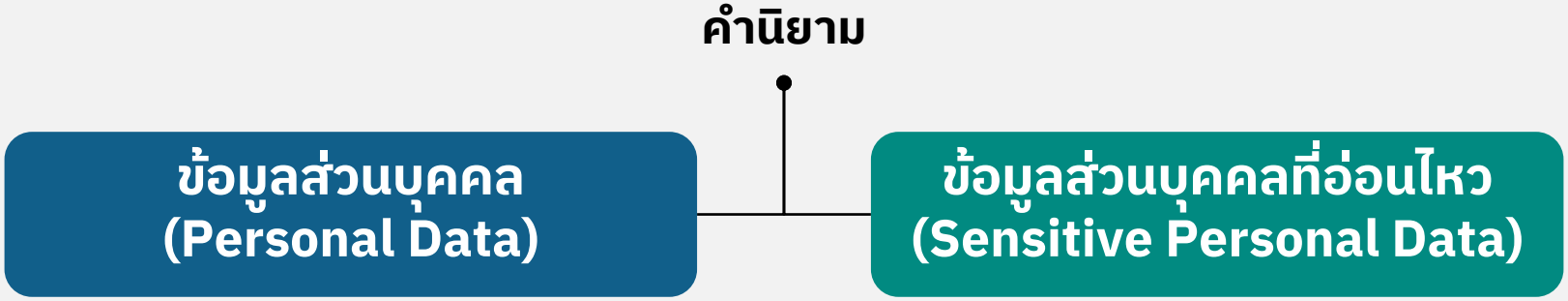
ให้หน่วยงานสามารถปฏิบัติในแนวทางเดียวกัน และ ร่วมรับผิดชอบ

4

ติดตาม ประเมินผล

ให้ความช่วยเหลือ สนับสนุน แนะนำ การปฏิบัติให้กับหน่วยงานต่างๆ ในกรม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเก็บบนกระดาษในสำนักงาน

ข้อมูลอิเล็กทรอนิกส์บนเครื่องส่วนตัว

ข้อมูลอิเล็กทรอนิกส์บนระบบ Server/Cloud

ข้อมูล (Data)

คือ ข้อเท็จจริงเกี่ยวกับสิ่งต่าง ๆ ซึ่งอาจเป็นคน สัตว์ สิ่งของ หรือเหตุการณ์ต่าง ๆ ที่ยังไม่ผ่านการประมวลผล โดยที่ข้อมูลอาจอยู่ในรูปของตัวเลข ตัวอักษร ข้อความ หรือ Multimedia ก็ได้

เนื่องจากข้อมูลเป็นส่วนประกอบที่สำคัญของระบบสารสนเทศรวมทั้งระบบสนับสนุนการตัดสินใจ จึงต้องเป็นข้อเท็จจริงที่ถูกต้อง ครบถ้วน สมบูรณ์ และน่าเชื่อถือ

- Name
- Physical attributes
- Online identifiers (including an IP address)
- Economic, cultural or social identity of a person
- Location data
- Health information
- An identification number

ข้อมูลส่วนบุคคลมีความเสี่ยงอะไรบ้าง

การถูกขโมยตัวตน

Identity theft

ถือเป็นภัยคุกคามที่น่ากลัวมากในปัจจุบัน หรือเรียกได้ว่าเป็นการขโมยข้อมูลส่วนบุคคลนั่นเอง ยกตัวอย่างเช่น ข้อมูลที่ใช้ในการติดต่อสื่อสาร หรือข้อมูลที่สามารถใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวตนได้

การประมวลผลข้อมูล

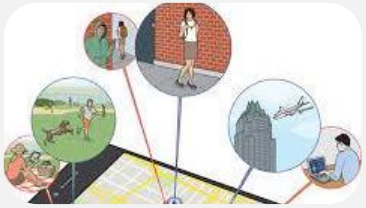
Profiling

การนำข้อมูลส่วนบุคคลไปประมลผลเพื่อกำหนด Profile ในการแสวงหาผลประโยชน์และการตลาด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

การขายข้อมูล

Misuse

การนำข้อมูลส่วนบุคคลไปขายให้กับบุคคลที่ 3 เพื่อประโยชน์ทางการตลาด



การติดตามสอดแนม

Tracking/ Stalking

การรั่วไหลของข้อมูลส่วนบุคคลบางอย่าง อาจนำไปสู่การติดตามหรือสอดแนมได้ เช่น ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลบัตรเครดิต เป็นต้น

สแปม

Spam

ในปัจจุบัน มีการสแปมหรือการส่งอีเมล/ข้อความโฆษณาหรือจดหมายลูกโซ่ไปให้โดยไม่ได้รับอนุญาตเป็นจำนวนมาก ซึ่งก่อให้เกิดความรำคาญใจต่อผู้รับและต้องเสียเวลาในการกำจัดข้อความเหล่านี้

บทบาทของผู้เกี่ยวข้องและการบังคับใช้

เจ้าของข้อมูล (Data Subjects)

เจ้าของข้อมูล - บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุถึง (บุคคลหมายถึงคนธรรมดาที่มีชีวิตอยู่ ไม่รวมถึงนิติบุคคล)

ผู้ควบคุมข้อมูล (Controllers)

ผู้ควบคุมข้อมูลส่วนบุคคล - บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล (ม 6 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

ผู้ประมวลผล (Processors)

ผู้ประมวลผลข้อมูลส่วนบุคคล - บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (ม 6 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

บุคคลภายนอก (Third Parties)

*เช่น บุคคล นิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผย (ม 27 วรรคสอง 37 พรบ ข้อมูลส่วนบุคคล พ.ศ. 2562)

*ความยินยอม
*ต้องเก็บจากเจ้าของข้อมูล
*ห้ามเก็บ Sensitive Data
*ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเจ้าของข้อมูล เช่น วัตถุประสงค์, อำนาจตามกฎหมายหรือสัญญา, ข้อมูลฯ ที่จะเก็บ, ระยะเวลาที่เก็บ , อาจจะเปิดเผยข้อมูลให้ใคร, สถานที่ วิธีการติดต่อ สิทธิของเจ้าของข้อมูล (ม 22,23 พรบใ ข้อมูลส่วนบุคคล พ.ศ. 2562)

การเก็บรวบรวม

การเปิดเผย

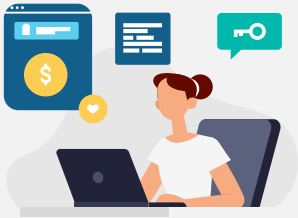
*ความยินยอม
*การโอนข้อมูลไปต่างประเทศ ปลายทางต้องมีมาตรฐานที่เพียงพอ
(ม 28,29 พรบ ข่อมูลส่วนบุคคล พ.ศ. 2562)

การใช้

การเก็บรวบรวมข้อมูลส่วนบุคคล - มาตรา 24

1. ได้รับความยินยอมจากเจ้าของข้อมูล (Consent)
2. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
3. เพื่อป้องกันหรือระงับอัตราต่อชีวิต (Vital Interest)
4. มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
5. มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public Task)
6. มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
7. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

การเก็บรวบรวม

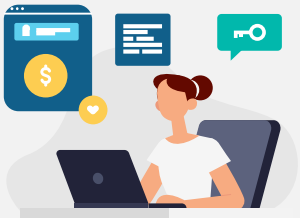


การบังคับใช้กฎหมาย

การเก็บรวบรวบข้อมูลส่วนบุคคลที่เป็น Sensitive Data - มาตรา 26

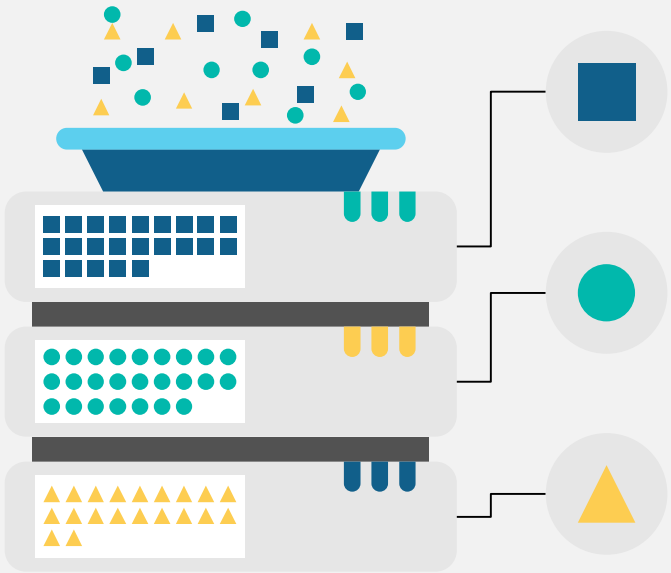
1. ได้รับความยินยอมโดยชัดแจ้ง (Consent)
2. ป้องกันหรือระงับอันตรายต่อชีวิต (Vital interest)
3. การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน
4. ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
5. การก่อตั้งสิทธิเรียบร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
6. จำเป็นในการปฏิบัติตามกฎหมายที่เกี่ยวข้องตามที่กำหนด

การเก็บรวบรวม



การบังคับใช้กฎหมาย

การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล



การบังคับใช้กฎหมาย

จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล สำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศที่รับข้อมูลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่...

1. การปฏิบัติตามกฎหมาย
2. ได้รับความยินยอมจากเจ้าของข้อมูล
3. การปฏิบัติตามสัญญา
4. การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
6. เพื่อประโยชน์สาธารณะที่สำคัญ

สิทธิของเจ้าของข้อมูลส่วนบุคคล

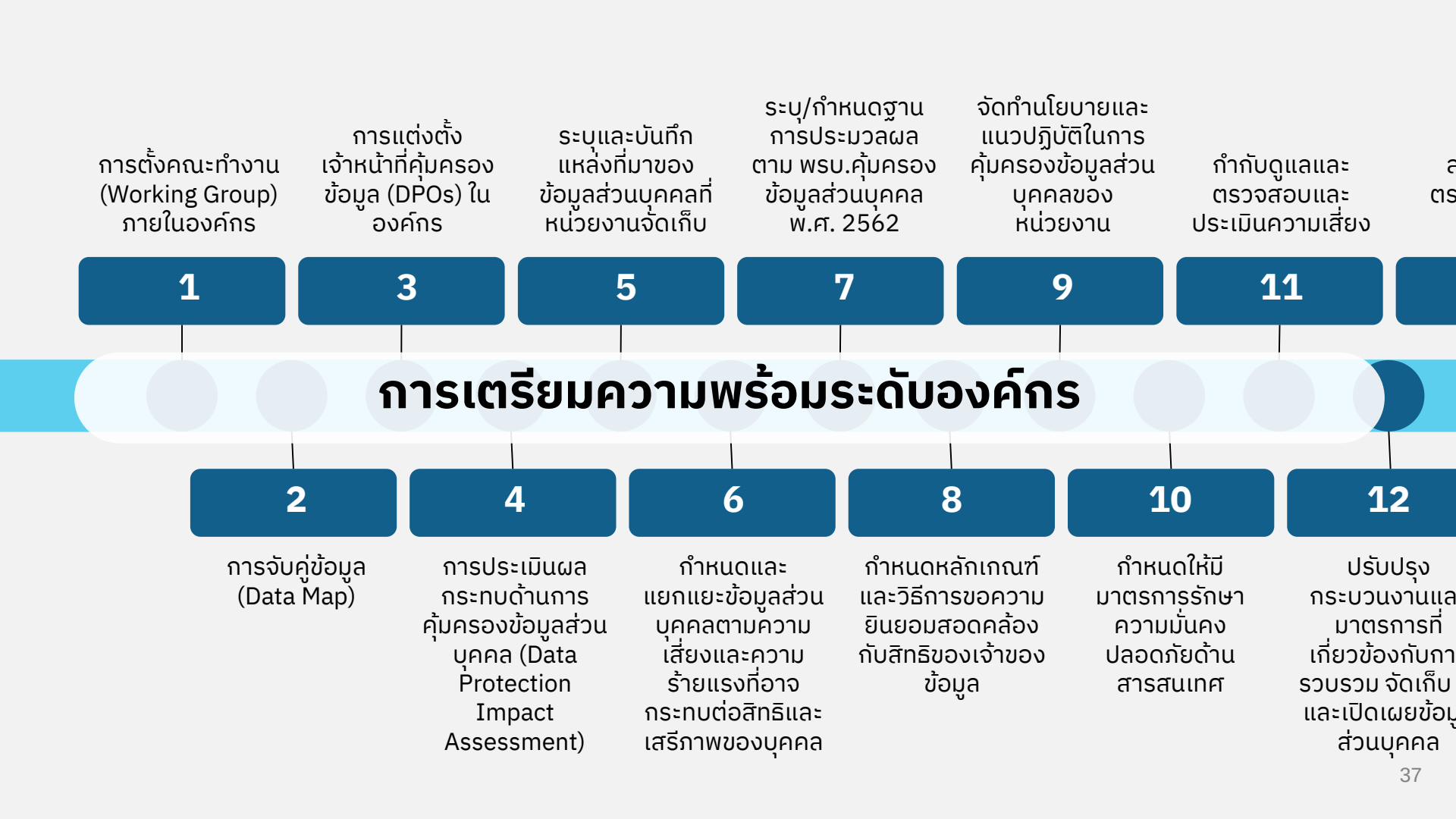
1. สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
3. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
4. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
5. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure)

หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
2. ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
3. ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
4. แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
5. แต่งตั้งตัวแทนภายในราชอาณาจักร
6. จัดทำบันทึกรายการ

หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล

1. ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
3. จัดทำและเก็บรักษารายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
4. แต่งตั้งตัวแทนภายในราชอาณาจักร
5. ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลให้ถือว่า ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล


การตั้งคณะทำงาน (Working Group) ภายในองค์กร
1
การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPOs) ในองค์กร
3
ระบุและบันทึกแหล่งที่มาของข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ
5
ระบุ/กำหนดฐานการประมวลผลตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7
จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน
9
กำกับดูแลและตรวจสอบและประเมินความเสี่ยง
11
การเตรียมความพร้อมระดับองค์กร
2
การจับคู่ข้อมูล (Data Map)
4
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)
6
กำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล
8
กำหนดหลักเกณฑ์และวิธีการขอความยินยอมสอดคล้องกับสิทธิของเจ้าของข้อมูล
10
กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
12

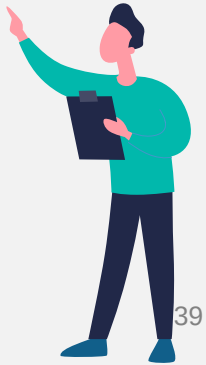

ระบุ/กำหนดฐานการประมวลผลตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน
กำกับดูแลและตรวจสอบและประเมินความเสี่ยง
สร้างความตระหนักรู้ และฝึกอบรม
การออกแบบและพัฒนาระบบโดยคำนึงถึงความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล
กำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน
7
9
11
13
15
17
การเตรียมความพร้อมระดับองค์กร
8
10
12
14
16
18
ดและ
อมูลส่วน
มความ
ะความ
ที่อาจ
สิทธิและ
องบุคคล
กำหนดหลักเกณฑ์และวิธีการขอความยินยอมสอดคล้องกับสิทธิของเจ้าของข้อมูล
กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ปรับปรุงกระบวนงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล
กำหนดมาตรการที่เหมาะสมด้านการรั่วไหลของข้อมูล (Data Breaches)
กำหนดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลทางด้านกายภาพ (Physical Security)
กำหนดมาตรการหรือแนวปฏิบัติที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เพียงพอ

1. การตั้งคณะทำงาน (Working Group) ภายในองค์กร

การตั้งคณะทำงานภายในองค์กร
ควรประกอบไปด้วยกลุ่มคนต่อไปนี้

- ฝ่ายกำหนดนโยบายและยุทธศาสตร์ขององค์กร
- ฝ่ายกฎหมาย
- ฝ่ายเทคโนโลยีสารสนเทศ
- ฝ่ายบุคคล หรือฝ่ายที่เกี่ยวข้องกับขบวนการทางธุรกิจขององค์กร

เพื่อศึกษาและทำความเข้าใจบริบทของกฎหมาย และเตรียมความพร้อมในการตรวจสอบ และปรับปรุงการดำเนินขององค์กรให้สอดคล้องตามข้อกำหนดของกฎหมาย



2. การจับคู่ข้อมูล (Data Map)

ตรวจสอบกระบวนการที่เกี่ยวข้องกับการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กร

หน่วยงานต้องตรวจสอบข้อมูลส่วนบุคคลที่มีอยู่ในองค์กร ตามกระบวนการไหลของข้อมูล (Data flows) เพื่อให้ทราบว่า **ข้อมูลส่วนบุคคลที่องค์กรนำมาใช้ในการประมวลผลมีที่มาจากแหล่งใด ข้อมูลที่จัดเป็นข้อมูลในลักษณะใด** (แบบทั่วไป หรือ ข้อมูลอ่อนไหว) ถูกจัดเก็บไว้ที่ใด จัดเก็บด้วยเหตุผลใด และถูกควบคุมโดยใคร โดยใช้วิธีการทำ Data Map เป็นต้น

3. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPOs) ในองค์กร

1

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลฯ ผู้ประมวลผลข้อมูลฯ ลูกจ้าง ผู้รับจ้างของผู้ควบคุมข้อมูลฯ หรือที่เกี่ยวข้องกับพ.ร.บ. นี้

กรณีที่หน่วยงานเข้าข่ายตามข้อกำหนดของกฎหมาย จะต้องดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office) เพื่อทำหน้าที่...

2

ตรวจสอบการการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

3

ประสานงานและให้ความร่วมมือกับสำนักงานฯ กรณีเกิดปัญหา

4

รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่ตามกฎหมายนี้

4. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

1. เพื่ออธิบายขอบเขตและวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล (จัดเก็บ ใช้ เปิดเผย)
2. เพื่อประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล
3. เพื่อจัดความเสี่ยงที่จะมีผลกระทบต่อเสรีภาพของบุคคล
4. เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานที่มีความเหมาะสม

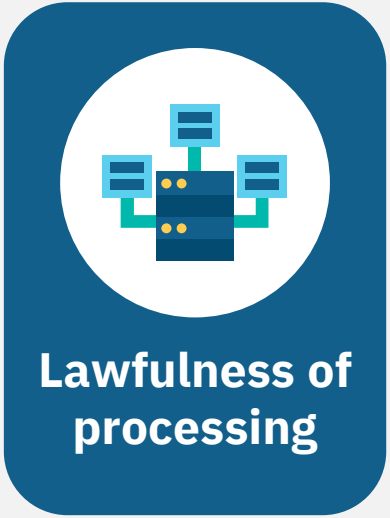
5. ระบุและบันทึกแหล่งที่มาของข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ

หน่วยงานต้อง**ให้ความสำคัญกับแหล่งที่มาของข้อมูลส่วนบุคคล**ที่หน่วยงานจัดเก็บ รวมทั้ง**ต้องบันทึกกิจกรรมที่เกิดขึ้นตลอดวงจรชีวิตของข้อมูล** (รวบรวม จัดเก็บ ใช้ เปิดเผย และการทำลาย) เพื่อการบริการจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับข้อกำหนดของกฎหมาย

หน่วยงานต้อง**จำแนกหรือแยกแยะข้อมูลให้เป็นหมวดหมู่**ข้อมูลส่วนบุคคล เพื่อระบุและ**จัดการข้อมูลบนพื้นฐานความเสี่ยง** รวมถึงกำหนดฐานการประมวลผลข้อมูลผลข้อมูลส่วนบุคคลที่เหมาะสม

6. กำหนดและแยกแยะข้อมูลส่วนบุคคลตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคล

7. ระบุ/กำหนดฐานการประมวลผลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



หน่วยงาน**จะต้องประมวลผลข้อมูลส่วนบุคคลบนฐานการประมวลผลที่ชอบกฎหมาย** (Lawfulness of processing) ทั้งในส่วนของข้อมูลส่วนบุคคลแบบทั่วไป (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 24 และมาตรา 26 โดยลำดับ

8. กำหนดหลักเกณฑ์และวิธีการขอความยินยอมสอดคล้องกับสิทธิของเจ้าของข้อมูล

การ**พัฒนากระบวนงาน และระบบงานที่เกี่ยวข้องเพื่อรองรับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย** เช่น การขอความยินยอมที่ชัดแจ้ง ข้อความเข้าใจง่าย

การใช้**สิทธิขอถอนความยินยอมของเจ้าของ**ข้อมูลส่วนบุคคล

การ**ขอเข้าถึง และปรับปรุงข้อมูลให้เป็นปัจจุบัน** เป็นต้น

9. จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน

หน่วยงานควรพิจารณาจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ที่มีเนื้อหาครอบคลุมตามหลักการอย่างน้อย ดังนี้

Collection Limitation
หลักการการรวบรวม จัดเก็บ ข้อมูลส่วนบุคคลเท่าที่จำเป็น

Use Limitation
หลักการใช้ และเปิดเผยข้อมูลอย่างจำกัด

Security Safeguards
หลักการรักษาความมั่นคงปลอดภัยข้อมูล

Purpose Specification
หลักการการกำหนดวัตถุประสงค์ที่ชัดเจน

Data Quality
หลักการคุณภาพของข้อมูลส่วนบุคคล

Individual Participation
หลักการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

Openness
หลักการเปิดเผยข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย

Accountability
หลักความรับผิดชอบของบุคคลที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคล/ประมวลผลข้อมูลส่วนบุคคล

10. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงานต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ถูกจัดเก็บ ใช้และเปิดเผย โดย**ต้องกำหนดให้มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่สอดคล้องกับมาตรฐานสากล** เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย

11. กำกับดูแลและตรวจสอบและประเมินความเสี่ยง

หน่วยงานจะต้องมีการ**กำกับดูแล และตรวจสอบการดำเนินงานบุคคลากร และผู้เกี่ยวเกี่ยวเพื่อให้เกิดการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้** เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่หน่วยงานทำการรวบรวมจัดเก็บ และเผยแพร่ถูกควบคุมภายใต้มาตรการที่กำหนดไว้ รวมถึงต้องมีการตรวจสอบและประเมินความเสี่ยงเป็นประจำอย่างสม่ำเสมอ

12. ทบทวนหรือปรับปรุงกระบวนงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล

หน่วยงานต้องทบทวนหรือปรับปรุงกระบวนงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล **เมื่อพบว่ามีความเสี่ยง หรือพบว่ามีกระบวนงานที่ไม่สอดคล้องกับข้อกำหนดของกฎหมาย โดยทบทวนตามวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้ เปิดเผย ลบหรือทำลายข้อมูล**

13. สร้างความตระหนักรู้ และฝึกอบรม

หน่วยงานต้อง**สร้างความตระหนักรู้ สำนึกรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล และหน้าที่ความรับผิดชอบของหน่วยงาน** รวมถึงการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และผลกระทบที่เกิดขึ้นจากการละเมิดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ให้แก่บุคลากรของหน่วยงาน **โดยการเผยแพร่ข้อมูลข่าวสาร และการฝึกอบรมให้ความรู้ที่เกี่ยวข้องเป็นประจำสม่ำเสมอ**

14. กำหนดมาตรการที่เหมาะสมด้านการรั่วไหลของข้อมูล (Data Breaches)

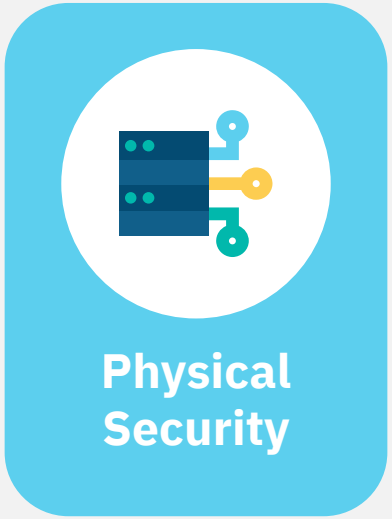
หน่วยงานต้องกำหนดมาตรการที่เหมาะสมเพื่อป้องกันการละเมิด และตรวจสอบ รวมถึงการรายงานผลการละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้น และต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

15. การออกแบบและพัฒนาระบบโดยคำนึงถึงความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล (Security and Privacy by Design)

หน่วยงานต้องให้ความสำคัญและ**ต้องใช้มาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอ ตั้งแต่ขั้นตอนการออกแบบไปจนถึงขั้นตอนพัฒนาระบบงาน** ตลอดจนบริการ ผลิตภัณฑ์ หรือการดำเนินการ ในลักษณะที่คุ้มครองสิทธิ์ส่วนบุคคลและข้อมูลส่วนบุคคล ตัวอย่าง Data protection by design เช่น การใช้นามแฝง และ การเข้ารหัส (Encoding)

16. กำหนดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลทางด้านกายภาพ (Physical Security)

หน่วยงานต้องกำหนดให้มีมาตรการในการ**รักษาความมั่นคงปลอดภัยทางด้านกายภาพของอุปกรณ์ประมวลผลและอุปกรณ์ที่เกี่ยวข้องที่ถูกนำมาใช้ในองค์ทั้งจากบุคคลภายนอกและภายในองค์กร** เช่น กำหนดนโยบายของศูนย์ข้อมูล เครือข่ายและระบบสื่อสาร รวมถึงการจัดสารสื่อบันทึกข้อมูล เป็นต้น

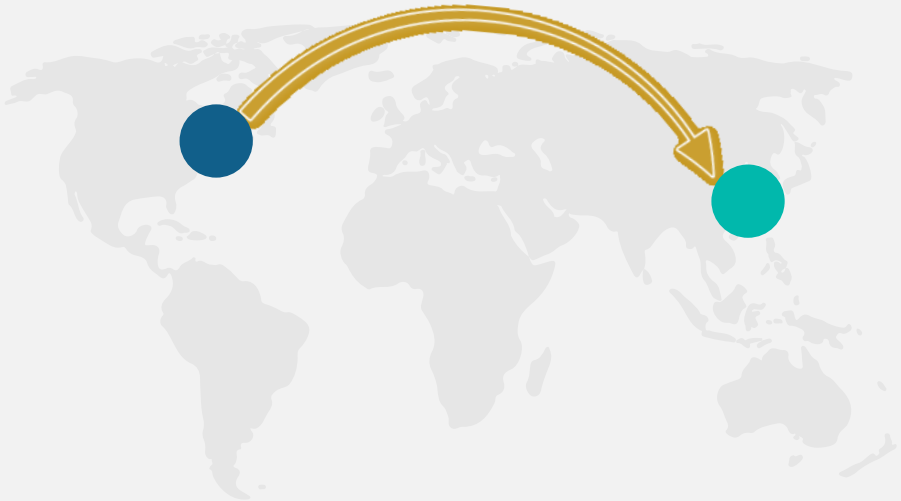


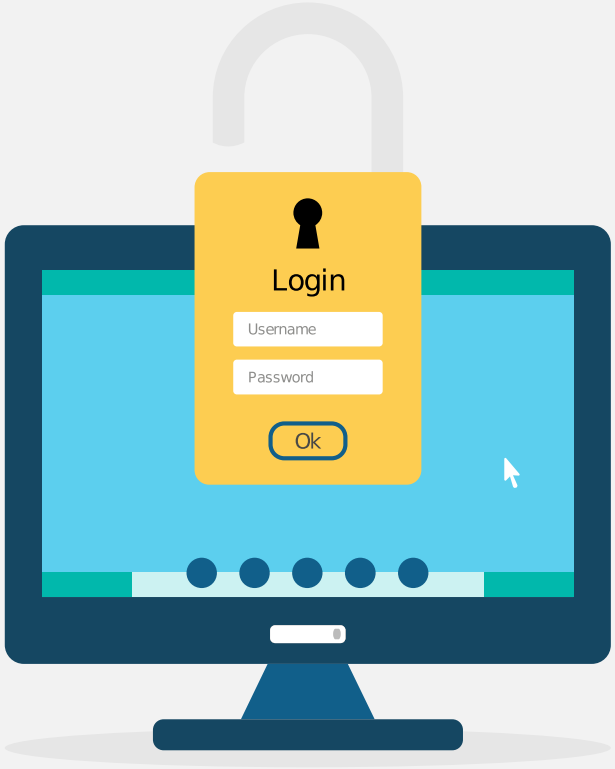
17. กำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน

หน่วยงานต้อง**กำหนดหน้าที่ความรับผิดชอบของบุคลากร**ที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคลไว้อย่างชัดเจน **และสิทธิการเข้าถึงได้เฉพาะผู้ที่มีสิทธิและมีหน้าที่รับผิดชอบเกี่ยวกับการดำเนินการขององค์กร**

18. กำหนดมาตรการหรือแนวปฏิบัติที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เพียงพอ (Cross-Border Data Transfer)

หากหน่วยงานมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางหรือองค์การระหว่างประเทศ **จะต้องคำนึงถึงว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่** เว้นแต่ดำเนินการเป็นตามข้อยกเว้นตามที่กฎหมายกำหนดในมาตรา 28





Thank