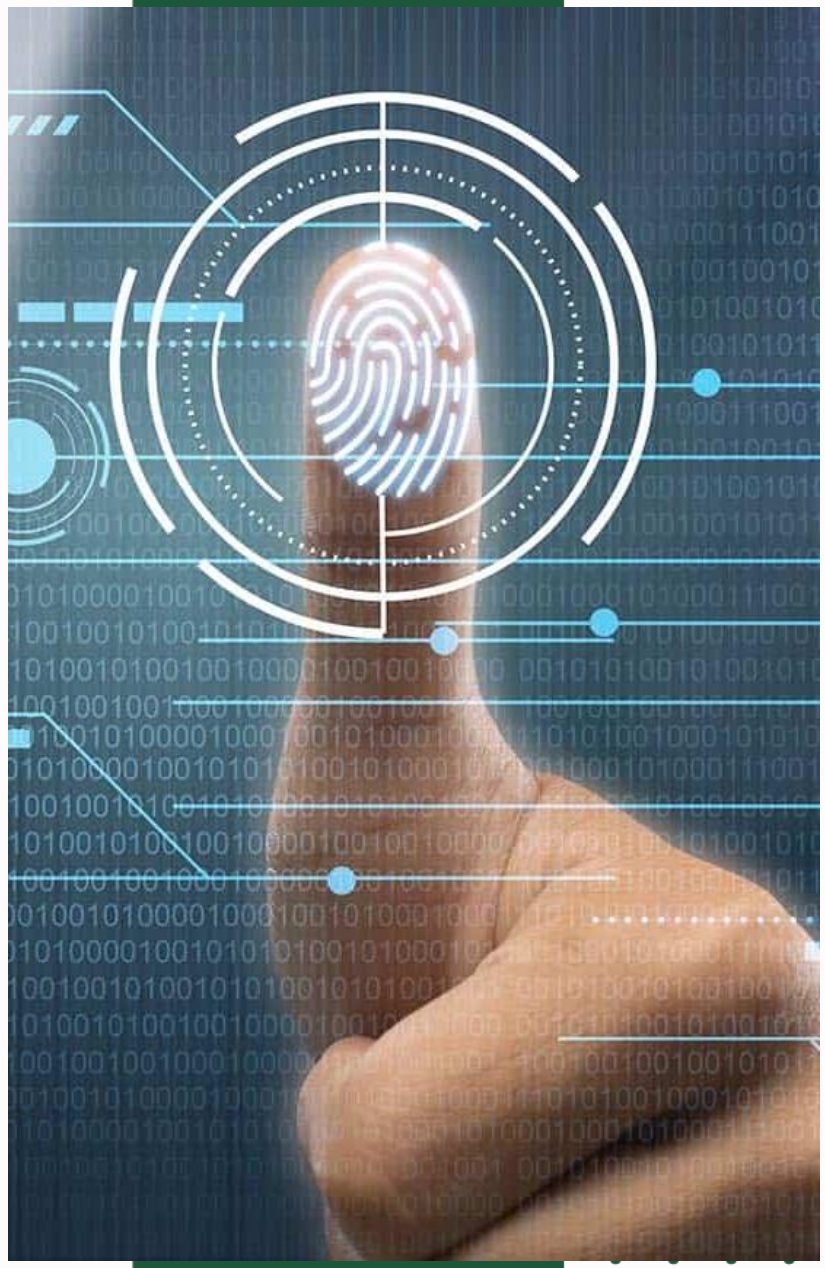
หลักสูตร

“กฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับเจ้าหน้าที่ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์”



12 กรกฎาคม พ.ศ. 2567

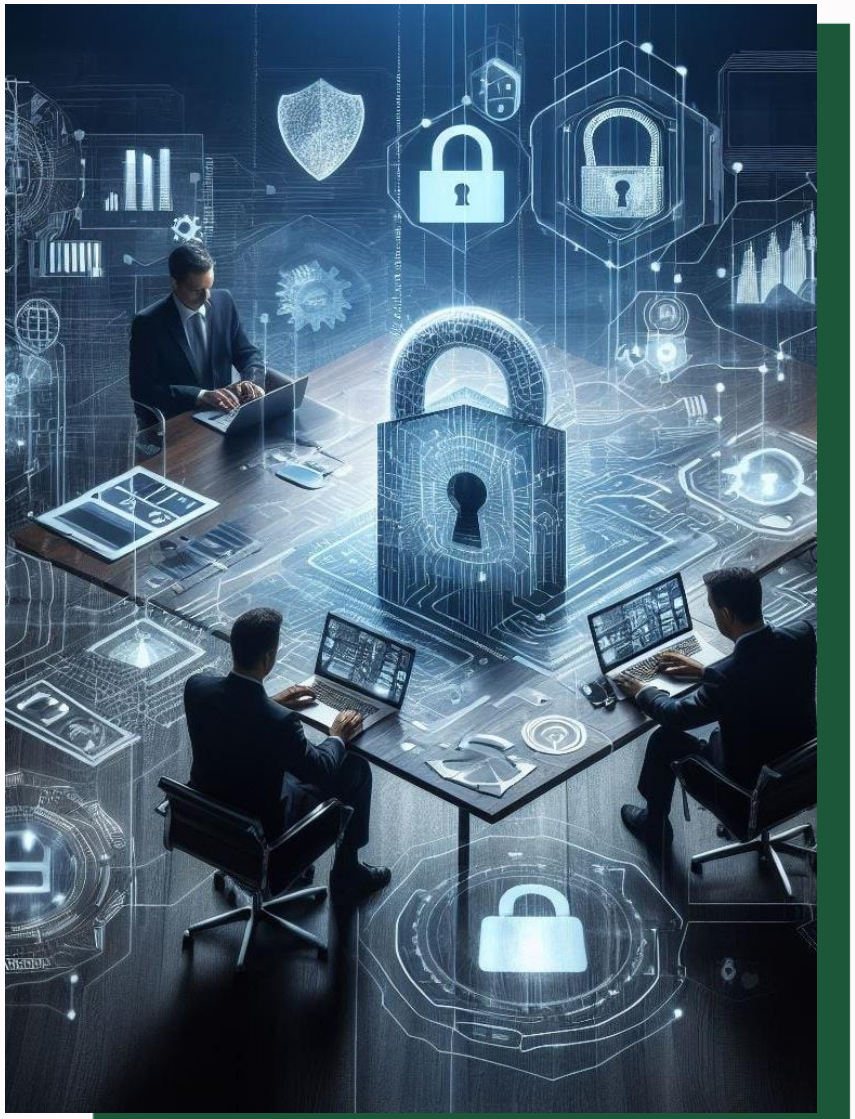
โดย อ.ศันศนีย์ หิรัญจันทร์ และ อ.ภัทรพล สุเมธลักษณ์

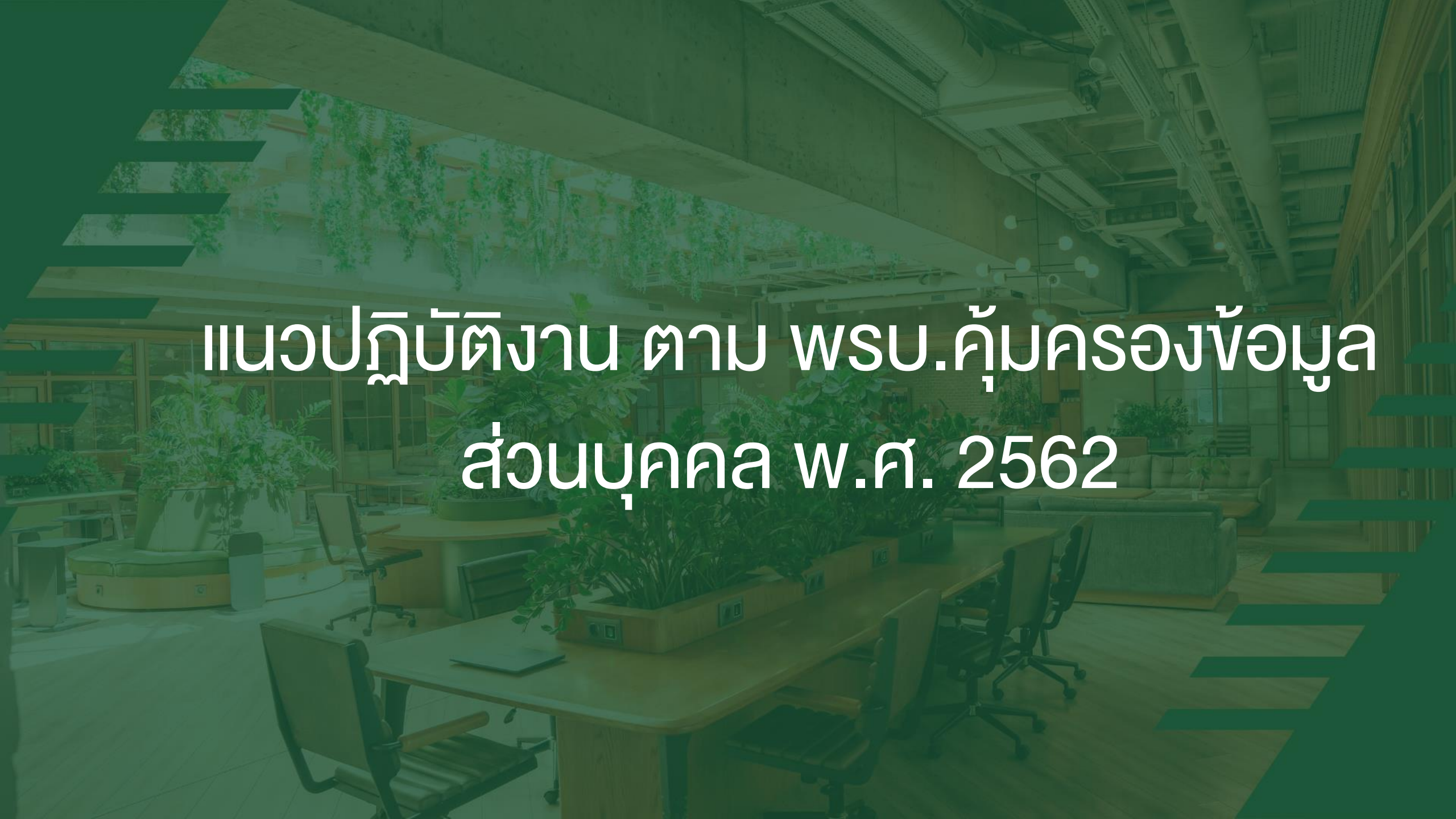
ศูนย์บริหารการจัดการองค์กรสากล

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

Content

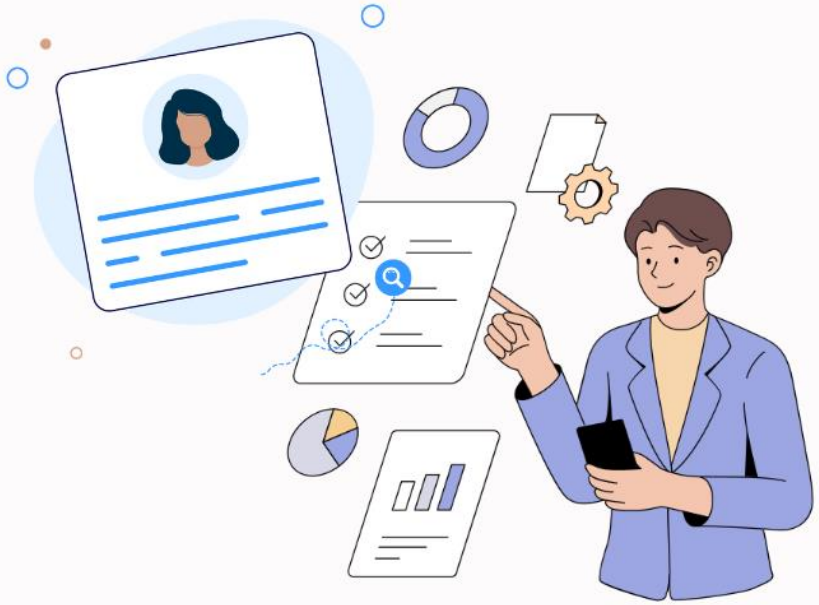
1. แนวปฏิบัติงาน ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. แนวปฏิบัติเมื่อเกิดการละเมิดความเป็นส่วนบุคคล (Data Breach)
3. การจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล (ROPA)
4. สาธิตการจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล (ROPA)





แนวปฏิบัติงาน ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พฤติกรรมเจ้าของข้อมูลส่วนบุคคล ต่อกลไกคุ้มครองข้อมูลส่วนบุคคล



หน่วยงานที่ผู้ตอบแบบสอบถามมั่นใจว่าข้อมูลส่วนบุคคลอยู่ในหน่วยงานเหล่านี้จะได้รับการดูแล คุ้มครอง และปฏิบัติตามนโยบายที่ได้ประกาศไว้ จากมากไปหาน้อย

1. ธุรกิจด้านการแพทย์ สาธารณสุข รวมถึงธุรกิจที่เกี่ยวเนื่อง (โรงพยาบาลและคลีนิกต่างๆ)
2. ธุรกิจด้านการเงิน สินเชื่อ การธนาคาร ประกันชีวิตและการประกันภัยรวมถึงธุรกิจที่เกี่ยวเนื่อง
3. ธุรกิจด้านการศึกษา (โรงเรียน มหาวิทยาลัย โรงเรียนกวดวิชา ฝึกอบรม สัมมนา) รวมถึงธุรกิจที่เกี่ยวเนื่อง
4. หน่วยงานของรัฐ
5. ธุรกิจด้านความปลอดภัย รวมถึงธุรกิจที่เกี่ยวเนื่อง
6. ธุรกิจด้านอสังหาริมทรัพย์ บ้านจัดสรร คอนโด รับสร้างบ้าน รวมถึงธุรกิจที่เกี่ยวเนื่อง
7. ธุรกิจด้านพาณิชยกรรม การขายปลีก การขายส่งและธุรกิจ E-commerce รวมถึงธุรกิจที่เกี่ยวเนื่อง
8. ธุรกิจด้านการคมนาคม ขนส่ง และการเก็บสินค้า รวมถึงธุรกิจที่เกี่ยวเนื่อง
9. มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร
10. ธุรกิจด้านการสื่อสาร โทรคมนาคม การติดต่อผ่านคอมพิวเตอร์ การติดต่อผ่านอุปกรณ์ดิจิทัล Social Media รวมถึงธุรกิจที่เกี่ยวข้อง
11. ธุรกิจด้านการท่องเที่ยวและการพักผ่อน รวมถึงธุรกิจที่เกี่ยวเนื่อง
12. ธุรกิจด้านความบันเทิง นันทนาการ (คอนเสิร์ต แข่งขันกีฬา) ธุรกิจข้อมูลข่าวสาร สื่อมวลชน สื่อบันเทิงดิจิทัล รวมถึงธุรกิจที่เกี่ยวเนื่อง
13. ธุรกิจเสริมความงาม รวมถึงธุรกิจที่เกี่ยวเนื่อง

หากมีเหตุการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคลที่อยู่ในการดูแลของกิจการต่อไปนี้ ผู้ตอบแบบสอบถามมีแนวโน้มที่จะดำเนินการขอใช้สิทธิลบข้อมูลส่วนบุคคล ยกเลิกบริการ และดำเนินการเรียกร้องค่าเสียหาย เรียงลำดับจากมากไปน้อย

1. ธุรกิจด้านการเงิน สินเชื่อ การธนาคาร ประกันชีวิตและการประกันภัยรวมถึงธุรกิจที่เกี่ยวเนื่อง
2. ธุรกิจเสริมความงาม รวมถึงธุรกิจที่เกี่ยวเนื่อง
3. ธุรกิจด้านพาณิชยกรรม การขายปลีก การขายส่งและธุรกิจ E-commerce รวมถึงธุรกิจที่เกี่ยวเนื่อง
4. ธุรกิจด้านอสังหาริมทรัพย์ บ้านจัดสรร คอนโด รับสร้างบ้าน รวมถึงธุรกิจที่เกี่ยวเนื่อง
5. ธุรกิจด้านการสื่อสาร โทรคมนาคม การติดต่อผ่านคอมพิวเตอร์ การติดต่อผ่านอุปกรณ์ดิจิทัล Social Media รวมถึงธุรกิจที่เกี่ยวข้อง
6. ธุรกิจด้านความปลอดภัย รวมถึงธุรกิจที่เกี่ยวเนื่อง
7. ธุรกิจด้านการคมนาคม ขนส่ง และการเก็บสินค้า รวมถึงธุรกิจที่เกี่ยวเนื่อง
8. ธุรกิจด้านการท่องเที่ยวและการพักผ่อน รวมถึงธุรกิจที่เกี่ยวเนื่อง
9. ธุรกิจด้านความบันเทิง นันทนาการ (คอนเสิร์ต แข่งขันกีฬา) ธุรกิจข้อมูลข่าวสาร สื่อมวลชน สื่อบันเทิงดิจิทัล รวมถึงธุรกิจที่เกี่ยวเนื่อง
10. ธุรกิจด้านการแพทย์ สาธารณสุข รวมถึงธุรกิจที่เกี่ยวเนื่อง (โรงพยาบาลและคลินิกต่างๆ)
11. ธุรกิจด้านการศึกษา (โรงเรียน มหาวิทยาลัย โรงเรียนกวดวิชา ฝึกอบรม สัมมนา) รวมถึงธุรกิจที่เกี่ยวเนื่อง
12. หน่วยงานของรัฐ
13. มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร

คุ้มครองในกิจกรรมตลอดวงจรชีวิตของข้อมูล

1 สร้างข้อมูล (Create)

- สัมภาษณ์
- กรอกแบบฟอร์ม
- บันทึกค่า
  - Sensor
  - ระบบ
- ซื้อข้อมูล
- Collect จากแหล่งข้อมูลอื่น

2 จัดเก็บข้อมูล (Store)

- แฟ้มข้อมูล
- เก็บในไฟล์ข้อมูล
- ฐานข้อมูล
- ระบบ
- Cloud Storage

3 ใช้ข้อมูล (Use)

- ประมวลผลข้อมูล
- รายงาน
- ทำกราฟ - แผนภาพ
- สถิติ
- Data Analytics
- Data Science
- AI

4 เปิดเผยข้อมูล (Publish)

- ประชาสัมพันธ์
- แชร์ในแพลตฟอร์ม
- ส่งให้ผู้มีส่วนเกี่ยวข้อง
- เผยแพร่แก่ประชาชน
- ส่งให้บุคคลที่สามผ่านระบบ

5 จัดเก็บข้อมูลถาวร (Achieve)

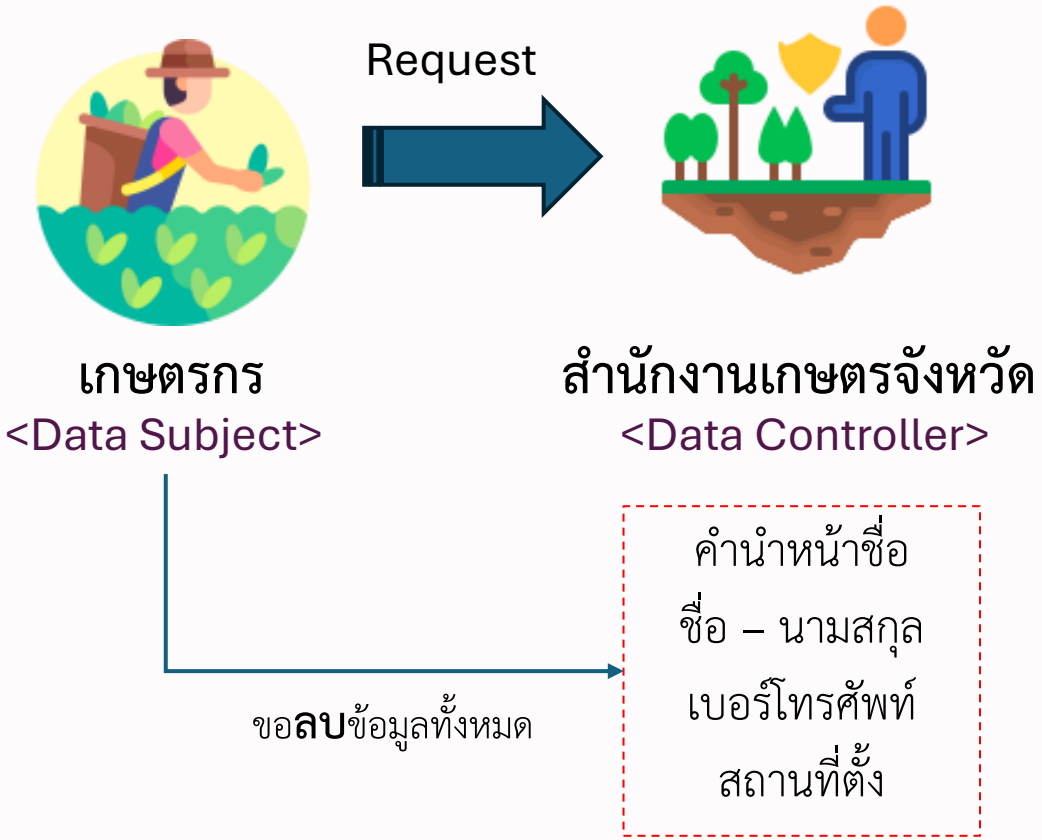
- ฐานข้อมูล
- แฟ้มข้อมูล
- ไฟล์ข้อมูล
- Cloud Storage

6 ทำลายข้อมูล (Destroy)

- ทำลายเอกสาร
  - ย่อยเอกสาร
  - เผา
- ลบชุดข้อมูล
- Purge Data

PD Inventory

กรณีสมมติ – คำถาม (ต่อ)



Q. กรณีตัวสอบคำร้องขอและอนุมัติให้ ดำเนินการลบข้อมูลสำนักงานฯ ในฐานะผู้ควบคุมข้อมูลต้องดำเนินการอย่างไร

เกษตรกร
<Data Subject>

Request

สำนักงานเกษตรจังหวัด
<Data Controller>

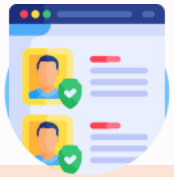
ค้นหา

ฝ่ายบริหารข้อมูล

ฝ่ายทะเบียนเกษตรกร

ฝ่ายสนับสนุนผ่านโทรศัพท์

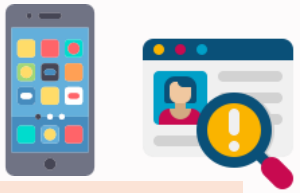
ไฟล์ข้อมูล



ฐานข้อมูล - ระบบ

เอกสาร

เจ้าหน้าที่ปฏิบัติงาน



Smart Phone

ขอ**ลบ**ข้อมูลทั้งหมด

คำนำหน้าชื่อ
ชื่อ – นามสกุล
เบอร์โทรศัพท์
สถานที่ตั้ง

Personal Data Inventory

Consent Management

<Data Subject>

<Request>

Consent

Privacy Notice

Consent

Privacy Notice

เอกสาร

Web Cookies Platform

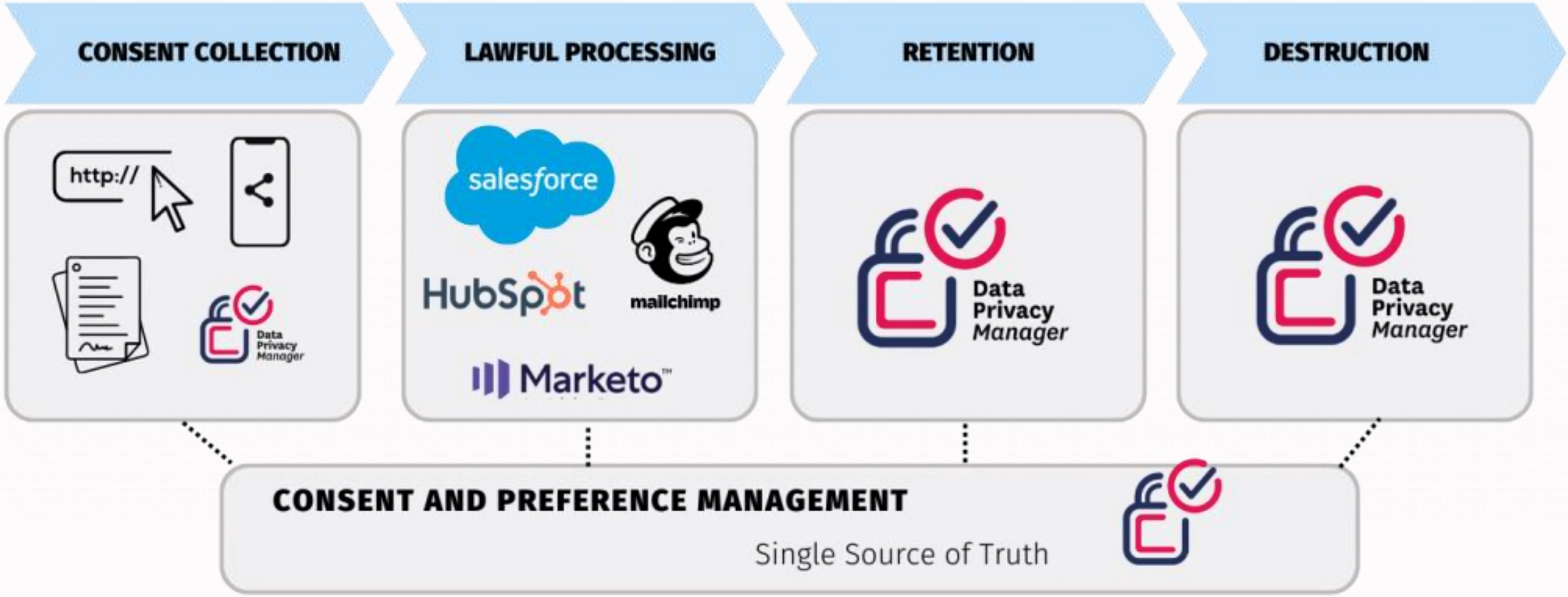
<Data Controller>

Consent management Procedure

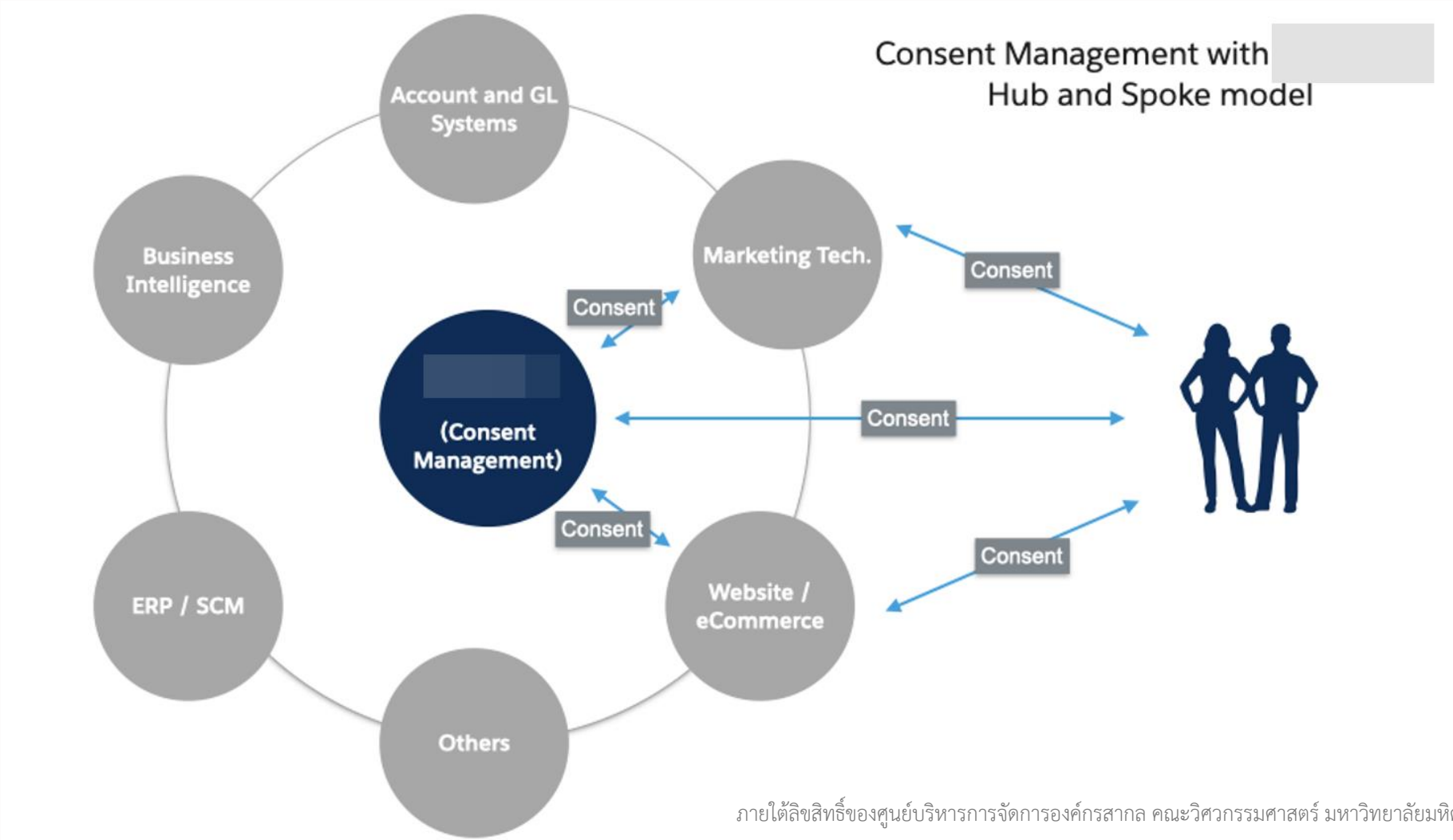
Consent management Platform

<Many Data Subject>

Example of Consent management platform



Example of Consent management platform



การใช้งานหรือเปิดเผยข้อมูลที่ต่างจากวัตถุประสงค์เดิม

การคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับอาชญากรรม

ข้อมูลประวัติอาชญากรรม หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับการสืบสวนสอบสวนการกระทำความผิดอาญา การดำเนินคดีอาญา หรือการรับโทษทางอาญาที่เป็นข้อมูลที่เป็นทางการหรือรับรองโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมายเกี่ยวกับการดำเนินการดังกล่าว ทั้งนี้ ไม่ว่าการดำเนินการนั้นจะถึงที่สุดแล้วหรือไม่ก็ตาม

การส่งหรือโอนข้อมูลส่วนบุคคล
ในเครือกิจการหรือเครือธุรกิจเดียวกันตามมาตรา 29 วรรคหนึ่ง

เครือกิจการหรือเครือธุรกิจเดียวกัน

หมายความว่า กิจการที่ผู้ประกอบกิจการมีอำนาจควบคุมหรือบริหารจัดการเหนือกิจการอื่น หรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือกิจการอื่นในรูปแบบบริษัทใหญ่ บริษัทย่อย หรือบริษัทร่วม รวมทั้งบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันทางกฎหมาย หรือเกี่ยวข้องกันเนื่องจากประกอบกิจการหรือธุรกิจร่วมกัน โดยใช้หลักเกณฑ์การพิจารณาตามกฎหมายที่เกี่ยวข้องและมาตรฐานทางบัญชีอันเป็นที่ยอมรับโดยทั่วไป

ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

ที่มีความสัมพันธ์ในลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกัน สามารถดำเนินการจัดให้มี...

นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules)

เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของกลุ่มองค์กรในเครือกิจการหรือเครือธุรกิจเหล่านั้นได้

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว **อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** ร่วมกันได้

โดยสถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้น ต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

(ข้อมูลเดือนมีนาคม 2567)

ที่มา : 1. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 29 และมาตรา 41 วรรคสอง
2. ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 ข้อ 3 และข้อ 5

NO. 76
Ver. 0.2

การเปิดเผยข้อมูลเท่าที่จำเป็น

การพรางหรือแทนข้อมูลส่วนบุคคลด้วยตัวอักษร X 5 ตัว เป็นอย่างน้อย เช่น

เบอร์โทรศัพท์

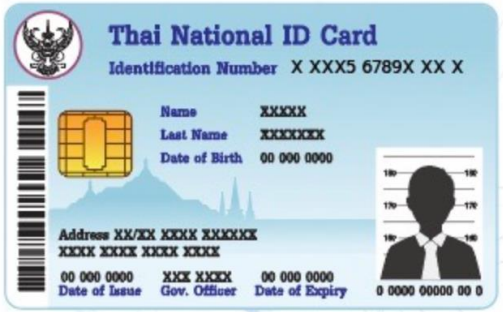
ควรแทนตัวเลขด้านหน้าหรือด้านหลังด้วย X5

ตัวอย่าง: XX XXXX 5678
08 123X XXXX

เลขบัตรประชาชน

ควรแทนด้วย X 4 ตัวด้านหน้าและหลัง

ตัวอย่าง: X XXX5 6789X XX X



การขอเข้าถึงข้อมูลจากหน่วยงานรัฐ

ข้อกำหนด: ต้องมีอำนาจตามกฎหมายเท่านั้น

พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ

☐ เจ้าหน้าที่และต้นสังกัด ☐ วันที่ได้รับคำร้อง ☐ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย

ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร

☐ เจ้าหน้าที่ไม่มีเอกสารมาแสดง ☐ เจ้าหน้าที่มีเอกสารมาแสดง เช่น หมายศาล/คำสั่งศาล

อื่น.....

พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)

☐ กรณีหมายศาล/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ ☐ กรณีเอกสารอื่น ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาสถานะของผู้ร้องขอ

☐ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร ให้ไม่ดำเนินการตามคำร้องขอ จนกว่าจะพิสูจน์สิทธิ์ได้

สรุปผล: ☐ ดำเนินการตามคำขอ ☐ ไม่ดำเนินการตามคำขอ ☐ บันทึกเกี่ยวกับกระบวนการร้องขอ ตั้งแต่ต้นจนจบ

แบบฟอร์มหลักฐาน กรณีเปิดเผยข้อมูล

ส่วนที่ ๑ ผู้ขอ

ชื่อ-สกุล ..... ตำแหน่ง ....

ต้นสังกัด ....

ที่อยู่/ข้อมูลติดต่อ..... .....

ส่วนที่ ๒ เจ้าของข้อมูล

ชื่อ-สกุล ....

ข้อมูลเบื้องต้น

ส่วนที่ ๓ ข้อมูลที่ขอเข้าถึง (โปรดระบุ)

....

....

เหตุผล/วัตถุประสงค์ที่จะนำเอาข้อมูลไปใช้

....

....

....

ระยะเวลาที่จะเก็บข้อมูลส่วนบุคคลไว้

....

....

แบบฟอร์มหลักฐาน กรณีเปิดเผยข้อมูล

ส่วนที่ ๔ ช่องทางในการจัดส่งข้อมูล

☐ ทางอิเล็กทรอนิกส์ผ่านทางอีเมลที่มีความมั่นคงปลอดภัย

☐ เข้ามารับด้วยตนเอง (ต้องมีการยืนยันตัวตนเมื่อเข้ามาติดต่อรับข้อมูลด้วย)

ส่วนที่ ๕ ฐานทางกฎหมายในการเปิดเผยข้อมูลและคำยืนยัน

ข้าพเจ้า (ผู้ขอ) ขอยืนยันว่าข้าพเจ้ามีอำนาจตามกฎหมายที่จะเข้าถึงข้อมูลส่วนบุคคลตามกฎหมายโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตาม.....(ระบุชื่อกฎหมายและมาตราที่เกี่ยวข้องหรือคำสั่งหรือหมายศาลที่ให้อำนาจ) และ.....(ผู้ได้รับคำร้องขอ) มีหน้าที่ตามกฎหมายที่จะสามารถเปิดเผยข้อมูลดังกล่าวได้เพราะมีหน้าที่ตามกฎหมายมาตรา ๒๗ ประกอบมาตรา ๒๔ (๖) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

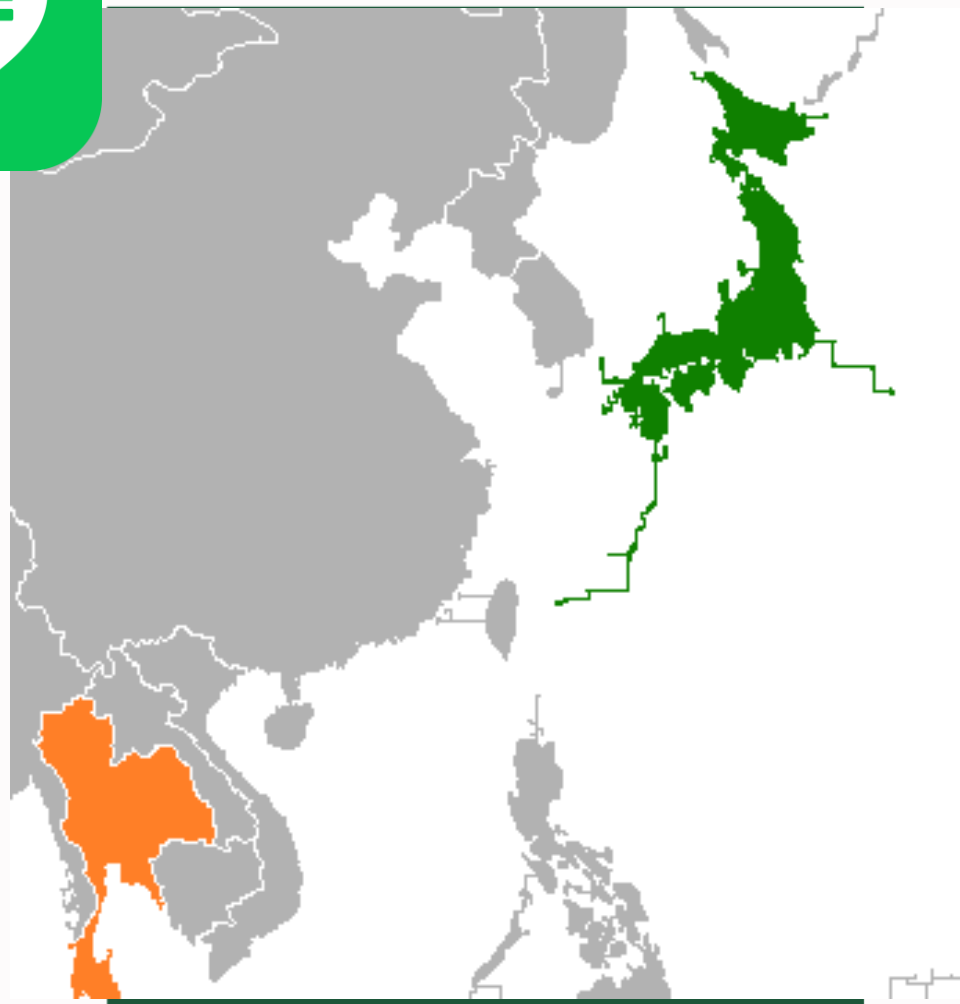
ข้าพเจ้า (ผู้ขอ) ยืนยันว่าข้อมูลที่ได้รับจะนำเอาไปใช้เพื่อวัตถุประสงค์อันได้ระบุไว้ข้างต้นเท่านั้น โดยไม่นำไปใช้เพื่อโยชน์ใด รวมถึงขอยืนยันว่าข้อมูลที่ได้กรอกลงในแบบฟอร์มนี้เป็นความจริงทุกประการ และข้าพเจ้าเข้าใจดีว่าการกรอกข้ออมูลที่ไม่ถูกต้องลงในแบบฟอร์มนี้อาจเป็นการกระทำฝ่าฝืน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

ลงชื่อ .....(ผู้ร้องขอ) วันที่ .....

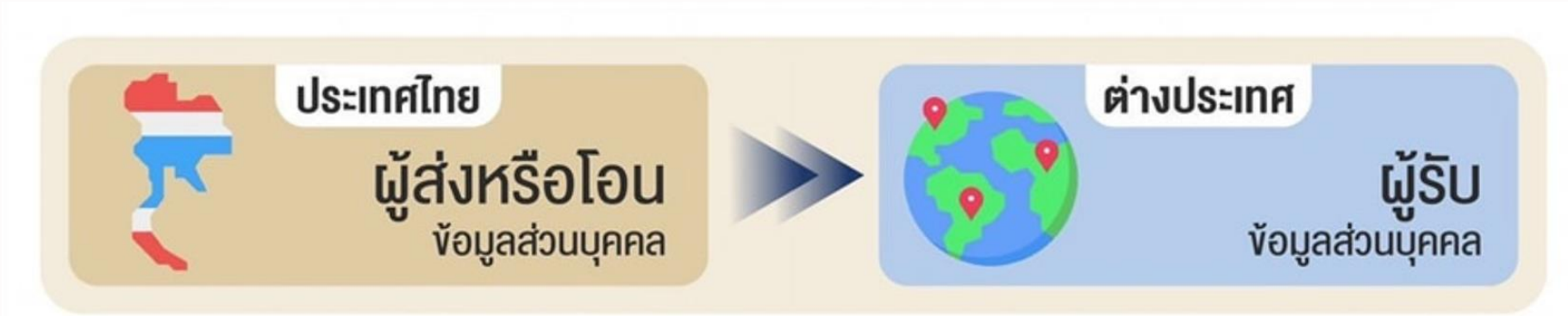
ผู้มอบอำนาจ (ในกรณีผู้ร้องขอเป็นผู้อยู่ใต้บังคับบัญชาที่อาจไม่มีอำนาจในการลงนามหรือใช้อำนาจตามกฎหมาย)
ชื่อ-สกุล ..... ตำแหน่ง .....
ลงชื่อ ..... วันที่ .....

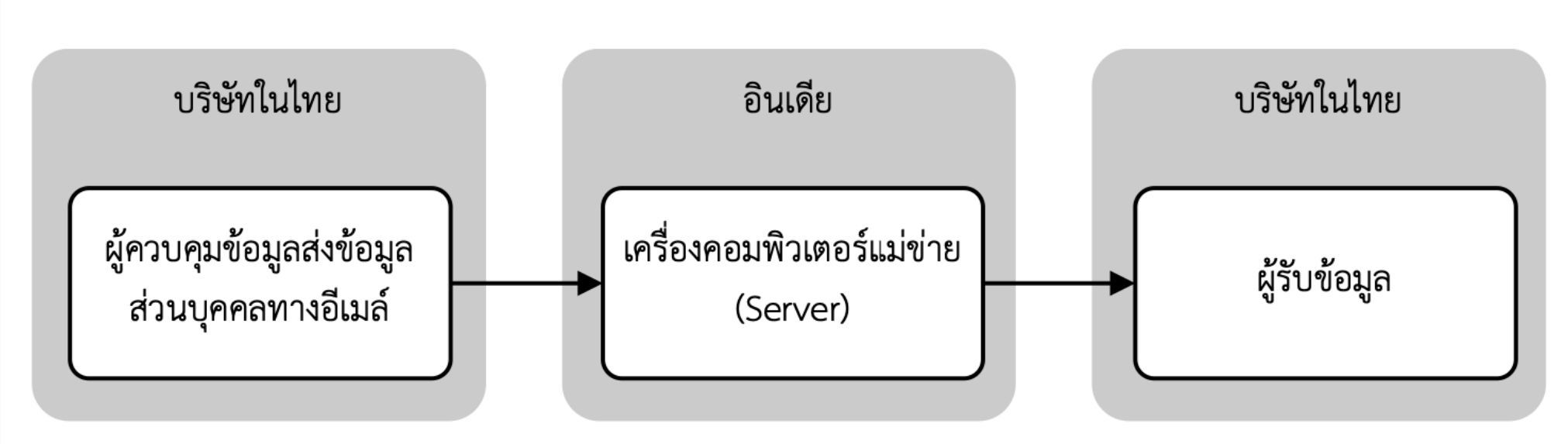
Quiz Session

การส่งไฟล์เอกสารใบรายชื่อพร้อมที่อยู่ให้กับเพื่อนร่วมงาน ในแผนกเดียวกันผ่านแอปพลิเคชัน Lineที่ Server อยู่ในประเทศญี่ปุ่น จัดเป็น การส่งข้อมูลหรือโอนข้อมูล (Data Transfer) ไปต่างประเทศหรือไม่ ?



Transfer and Transit





หลักเกณฑ์สำหรับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอในการส่งหรือโอนไปยังต่างประเทศ

กระดาษ Reuse

จากกรณีที่มีข่าวพบเอกสารของหน่วยงาน (ผู้ควบคุมข้อมูลส่วนบุคคล) มีข้อมูลส่วนบุคคลไม่ใช้แล้ว ถูกนำไปใช้เป็นถุงขนมต่าง ๆ นั้น

"การกระทำดังกล่าวอาจเป็นการละเมิดข้อมูลส่วนบุคคล เนื่องจากไม่ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามระดับความเสี่ยง"

เพื่อป้องกันไม่ให้เกิดเหตุการณ์ดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคล ควรมีมาตรการดังนี้...

1. ตรวจสอบเอกสารก่อนการนำไปใช้ซ้ำ
2. มีกระบวนการและระเบียบขั้นตอนในการทำลายเอกสารอย่างเหมาะสม
3. ในกรณีที่ใช้ผู้รับจ้าง ต้องจัดให้มีมาตรการควบคุมและกำกับ

ผู้ควบคุมข้อมูลส่วนบุคคล

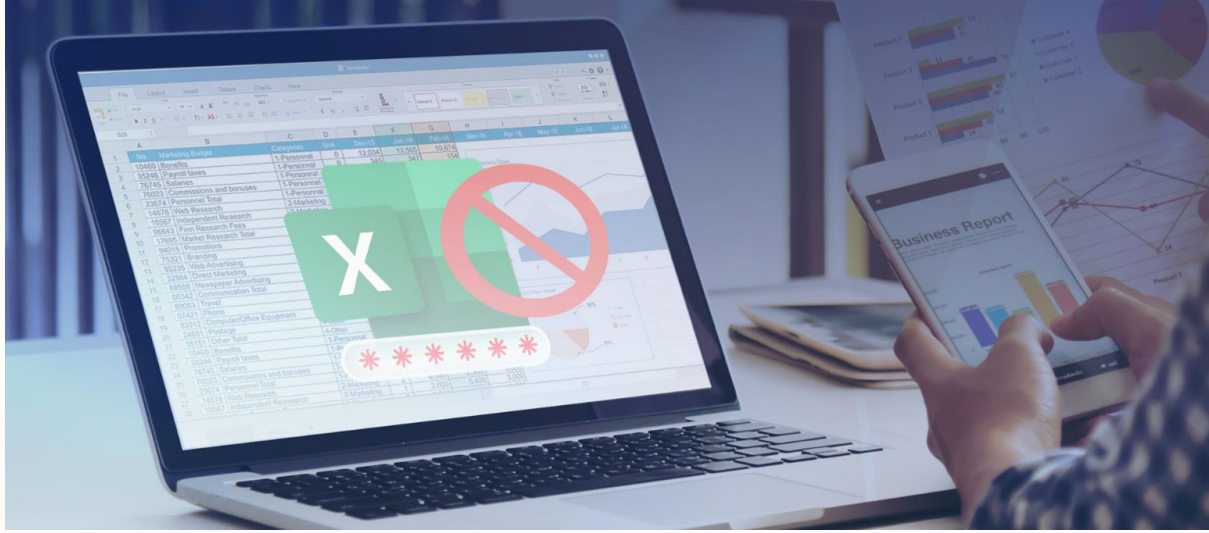
(ข้อมูลเดือนมิถุนายน 2567)

ที่มา :
1. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (4)
2. ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
3. ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
www.pdpc.or.th | PDPC Thailand

Excel ที่มีข้อมูลส่วนบุคคล ควรทำเป็น PDF และให้มีการเข้ารหัสทุกครั้ง

อีกหนึ่งวิธี "ป้องกัน" การละเมิดข้อมูลส่วนบุคคล



ฐานทางกฎหมาย

ฐานทางกฎหมายจะบัญญัติไว้ในมาตรา 24 และ มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การพิจารณาฐานทางกฎหมายจะต้องพิจารณาตามประเภทของข้อมูลส่วนบุคคลและวัตถุประสงค์ที่ใช้ในการเก็บรวบรวมข้อมูลส่วนบุคคล

ขอขอบคุณแหล่งที่มา : PDPC Thailand

แนวปฏิบัติเมื่อเกิดการละเมิดความเป็นส่วนบุคคล (Data Breach)

การละเมิดข้อมูลส่วนบุคคล

"**การละเมิดข้อมูลส่วนบุคคล**" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจ หรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่นใด

ช่องทาง:

- หน่วยงานตรวจพบเหตุการณ์ละเมิด
- ได้รับแจ้งจากหน่วยงานรัฐ – DP
- ได้รับการร้องเรียนจาก Data Subject

Cr. StationX

ตัวอย่างการละเมิดข้อมูลส่วนบุคคล

เหตุการณ์ (Incident)	การละเมิด (Breach)		
	C ความลับ (Confidentiality)	I ความถูกต้องครบถ้วน (Integrity)	A ความพร้อมใช้งาน (Availability)
1 เอกสารสูญหาย/ถูกขโมย	○		○
2 เอกสารถูกทิ้งไว้ในสถานที่ที่ไม่ปลอดภัย	○	○	○
3 ข้อมูลส่วนบุคคลถูกลบ/ทำลาย โดยไม่มีการสำรองข้อมูลไว้			○
4 จดหมาย/อีเมลที่มีข้อมูลส่วนบุคคลถูกส่งผิดไปยังบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล	○		
5 พนักงานเข้าถึงและเปลี่ยนแปลงหรือลบข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต	○	○	○

ทั้งนี้ ลักษณะของเหตุการละเมิดขึ้นอยู่กับข้อเท็จจริงของเหตุการณ์ในแต่ละกรณี และเป็นหนึ่งในปัจจัยของการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากพบว่ามีความเสี่ยงหรือมีความเสี่ยงสูงให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมายัง สคส. หรือแจ้งแก่เจ้าของข้อมูลส่วนบุคคลด้วยแล้วแต่กรณีตามที่กฎหมายกำหนด

ตัวอย่างการละเมิดข้อมูลส่วนบุคคล

เหตุการณ์ (Incident)	การละเมิด (Breach)		
	C ความลับ (Confidentiality)	I ความถูกต้องครบถ้วน (Integrity)	A ความพร้อมใช้งาน (Availability)
1 ข้อมูลส่วนบุคคลในระบบคอมพิวเตอร์ ไม่ว่าจะเป็นระบบภายในของบริษัทหรือระบบที่ใช้ผ่านอินเทอร์เน็ตถูก Malware เข้าถึง	O	O	O
2 อุปกรณ์ที่มีข้อมูลส่วนบุคคลสูญหาย/ถูกขโมย	O		O
3 อุปกรณ์หรือระบบคอมพิวเตอร์ถูกเข้ารหัส/ถูกเรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware) โดยแฮกเกอร์	O		O
4 บัญชีของผู้ใช้งานหรือผู้ดูแลระบบถูกนำไปใช้โดยไม่ได้รับอนุญาต	O	O	O
5 ข้อมูลส่วนบุคคลถูกแก้ไขโดยไม่ได้รับอนุญาต		O	

ทั้งนี้ ลักษณะของเหตุการละเมิดขึ้นอยู่กับข้อเท็จจริงของเหตุการณ์ในแต่ละกรณี และเป็นหนึ่งในปัจจัยของการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากพบว่ามีความเสี่ยงหรือมีความเสี่ยงสูงให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมายัง สคส. หรือแจ้งแก่เจ้าของข้อมูลส่วนบุคคลด้วยแล้วแต่กรณีตามที่กฎหมายกำหนด

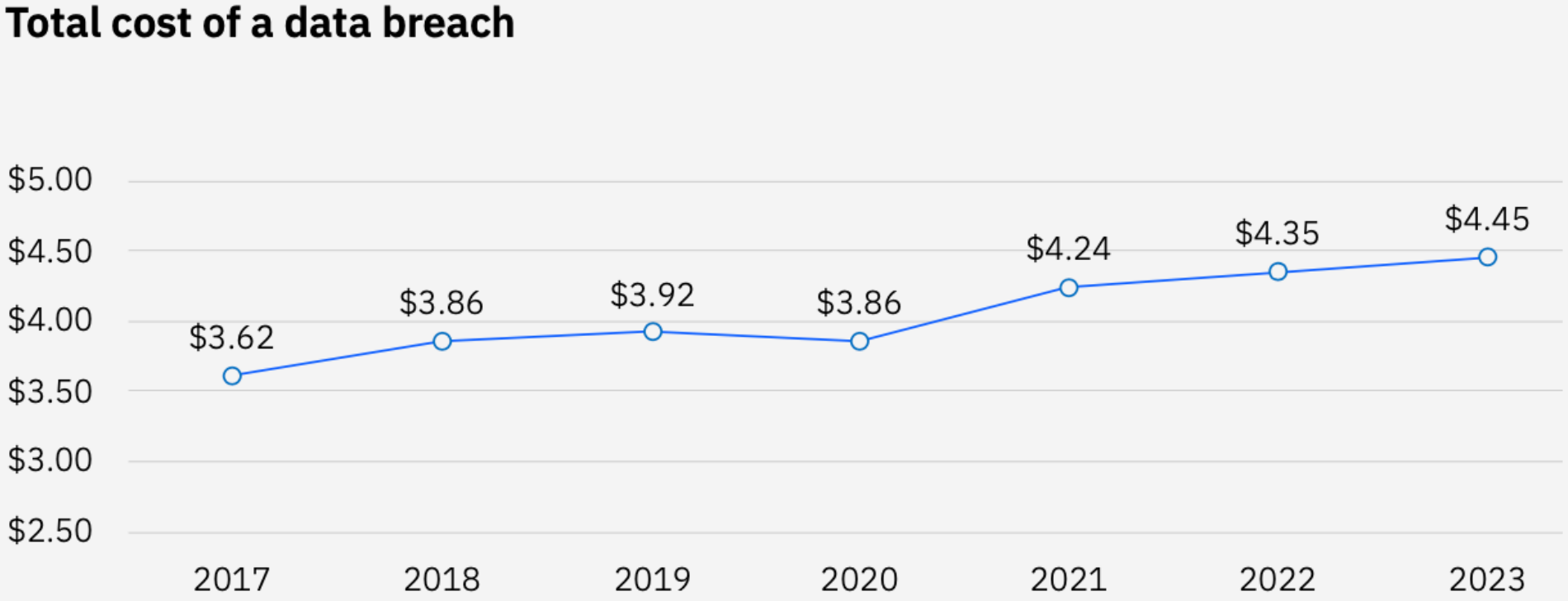


Figure 1. Measured in USD millions

สถิติความเสียหายจากการละเมิดความเป็นส่วนบุคคล

IBM Security, “Cost of a Data Breach Report 2023”

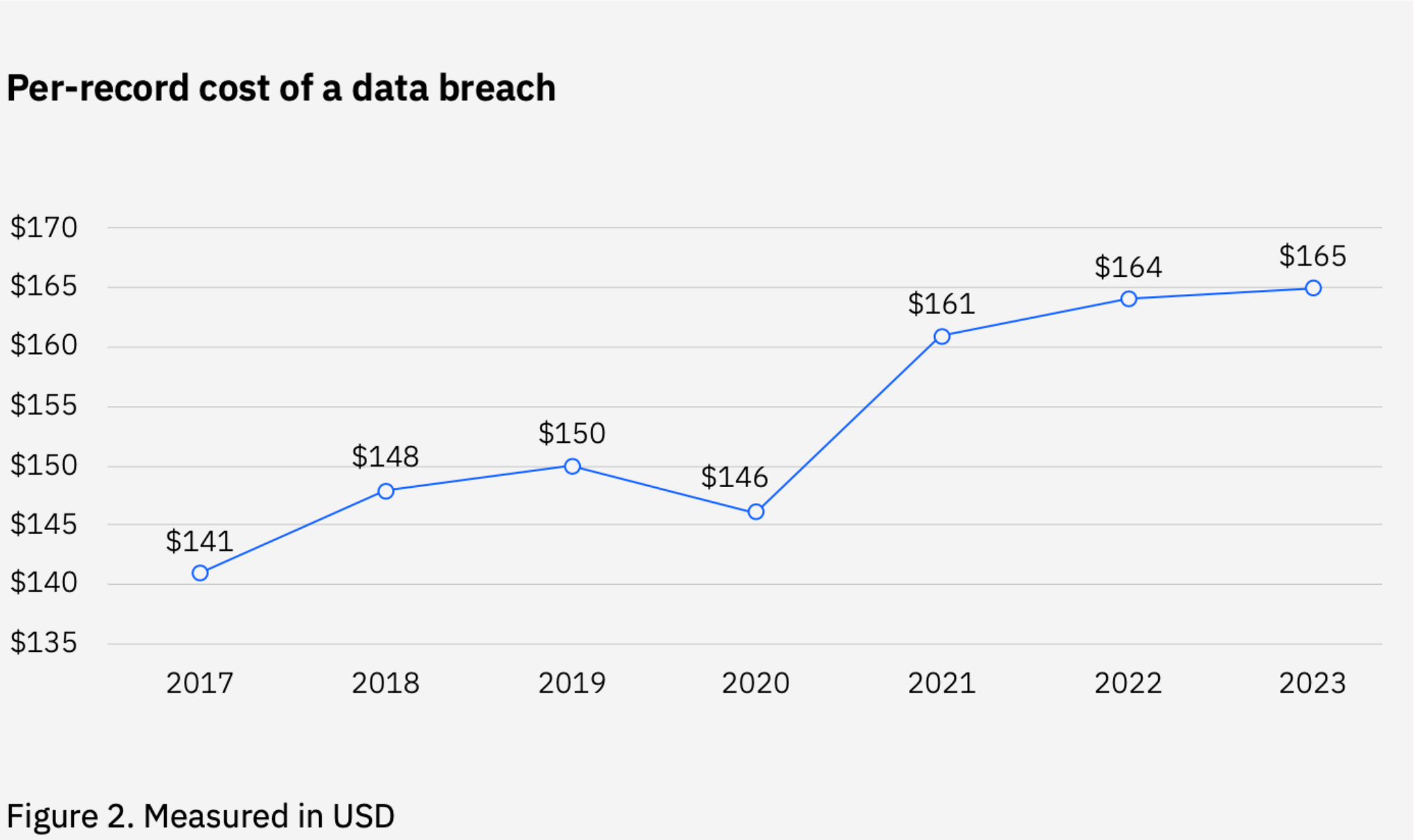
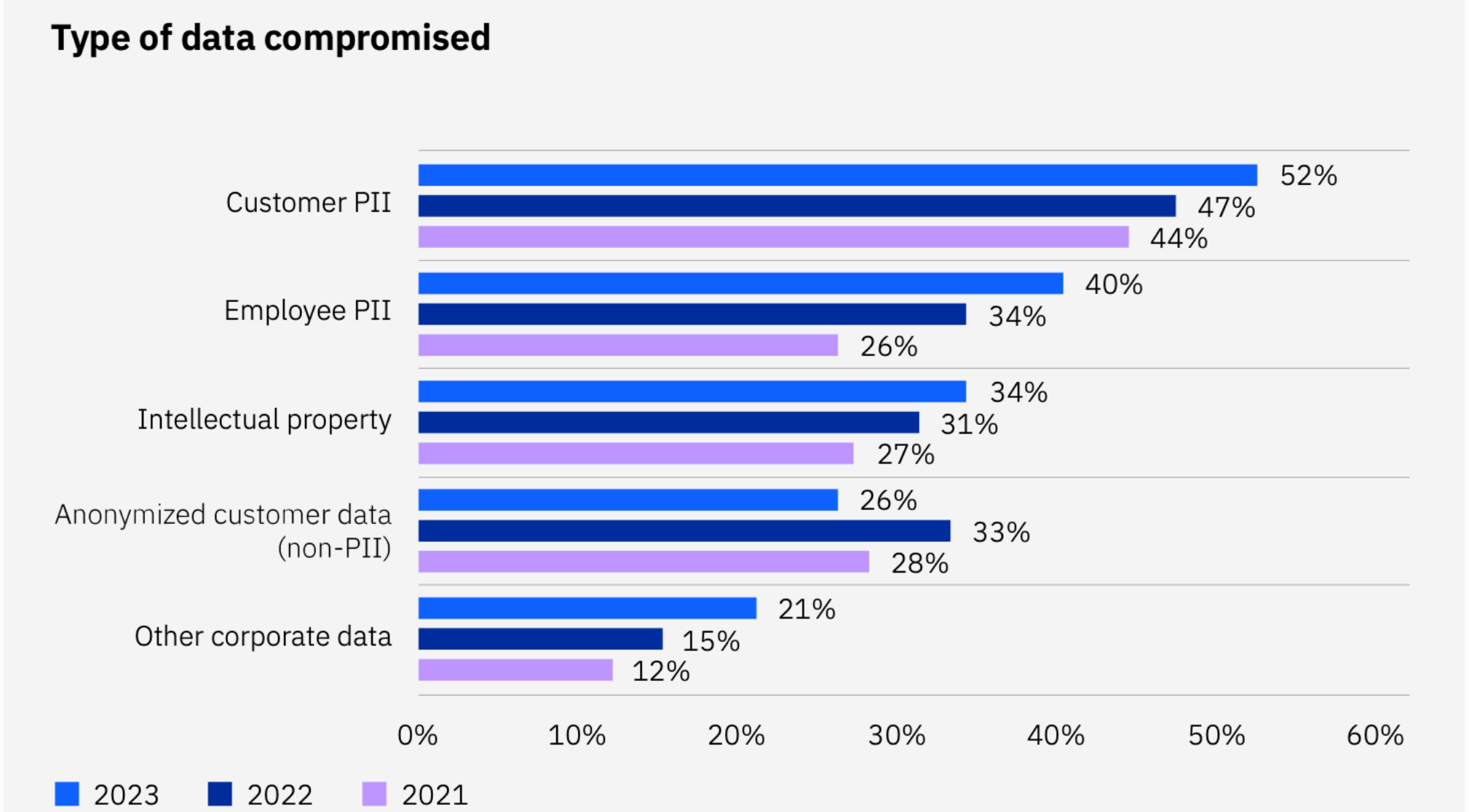


Figure 2. Measured in USD

มูลค่าความเสียหายจากการละเมิดความเป็นส่วนบุคคลต่อรายการ

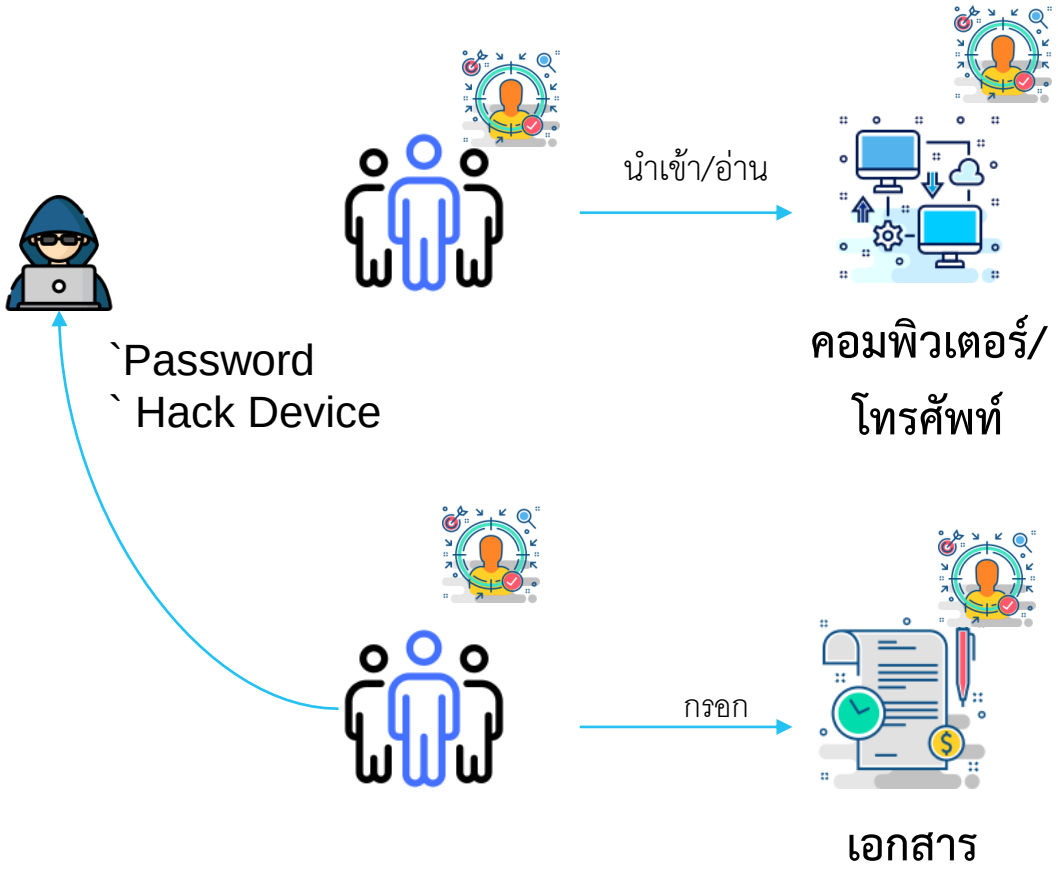
IBM Security, “Cost of a Data Breach Report 2023”

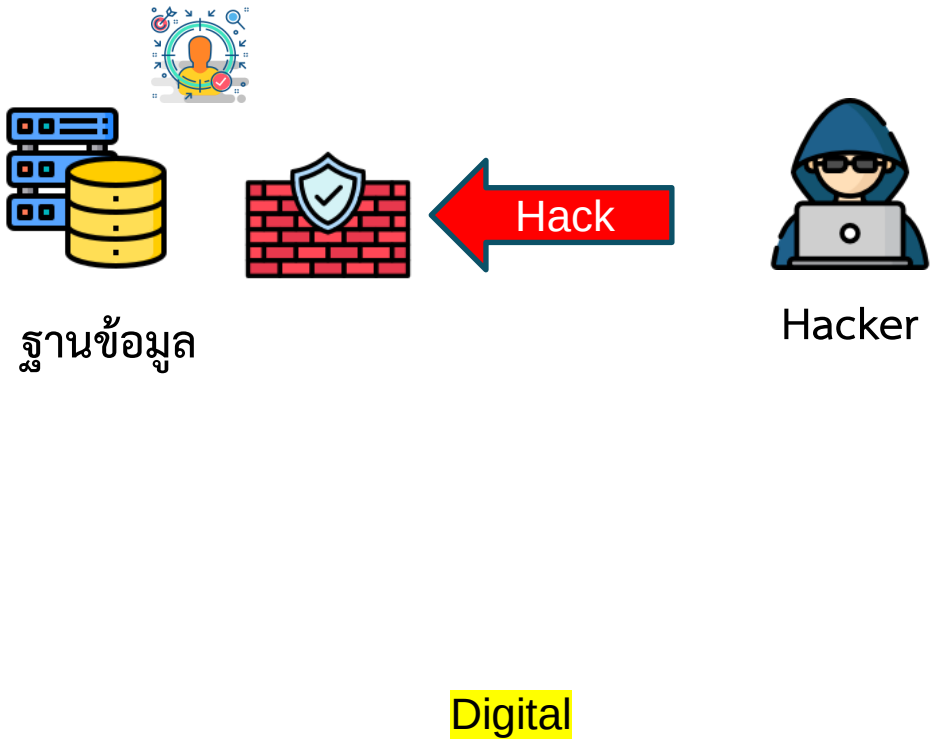


ประเภทข้อมูลที่ถูกละเมิดความเป็นส่วนบุคคล

IBM Security, “Cost of a Data Breach Report 2023”

การรั่วไหล หรือ ละเมิดความเป็นส่วนบุคคล เกิดจากที่ไหนได้บ้าง





Cost and frequency of a data breach by initial attack vector

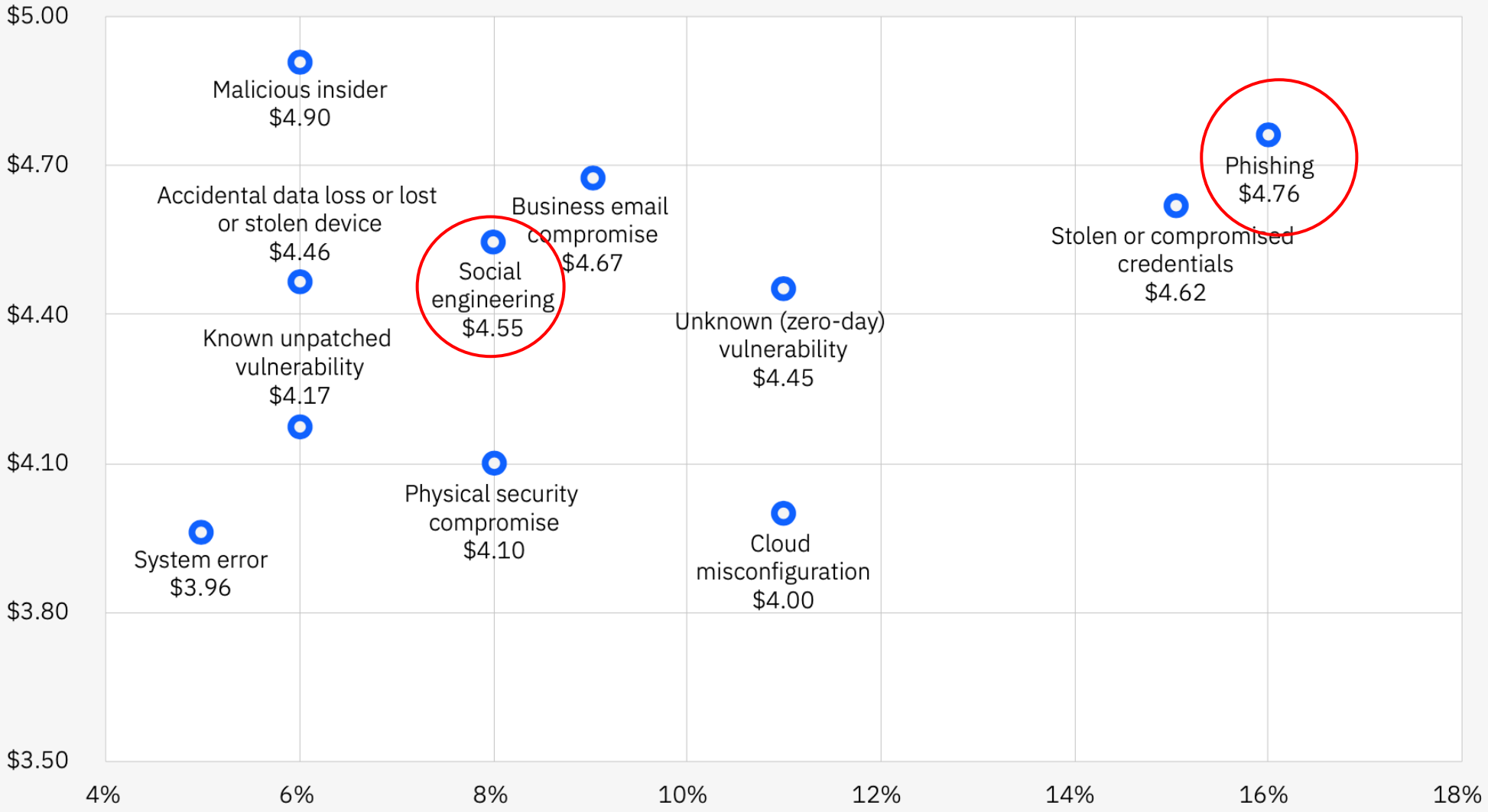
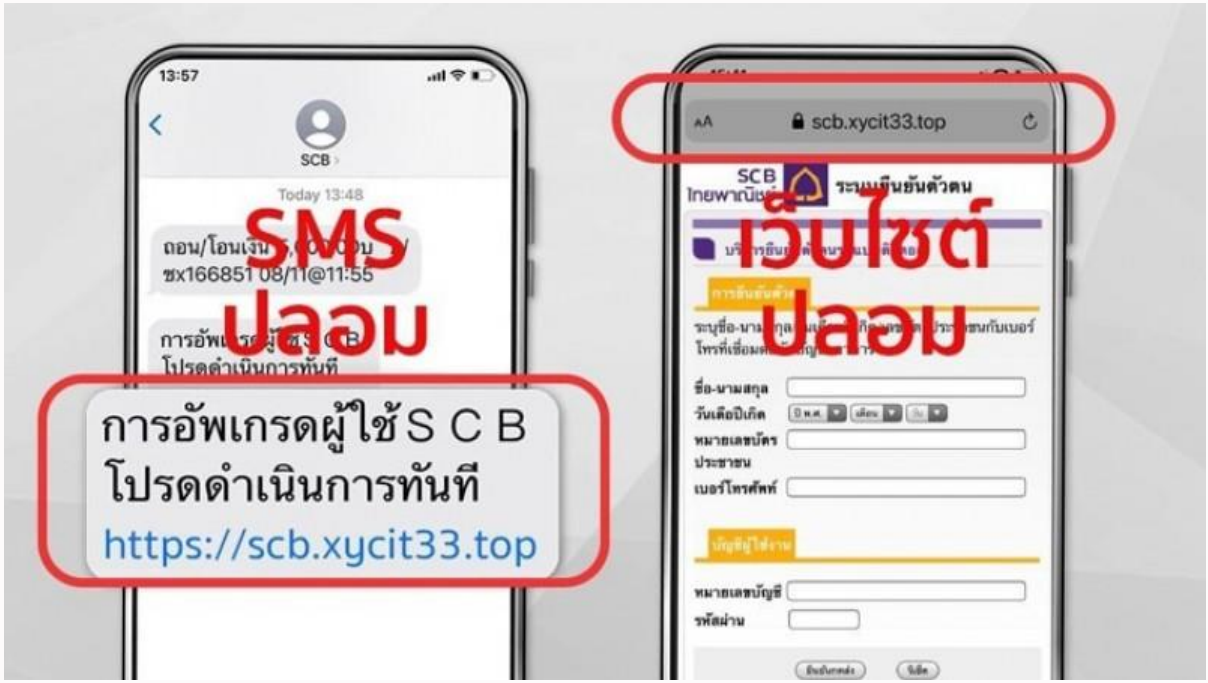


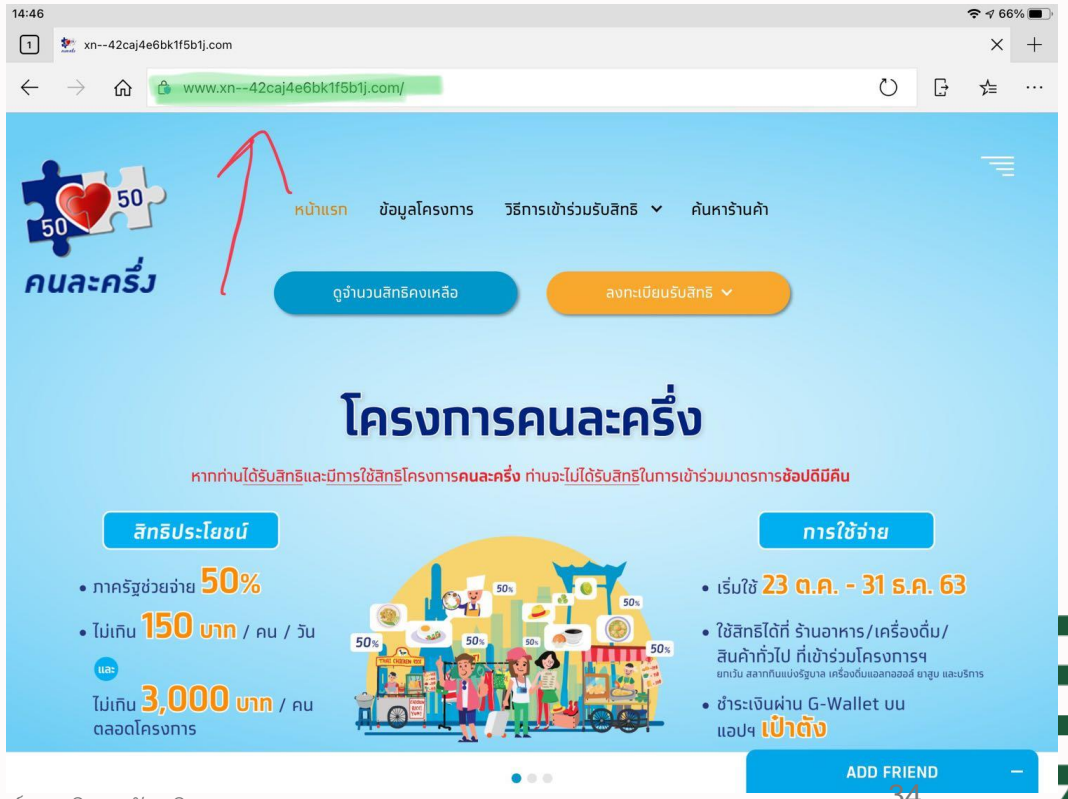
Figure 10. Measured in USD millions

แอปดูดเงิน: แอปปลอม

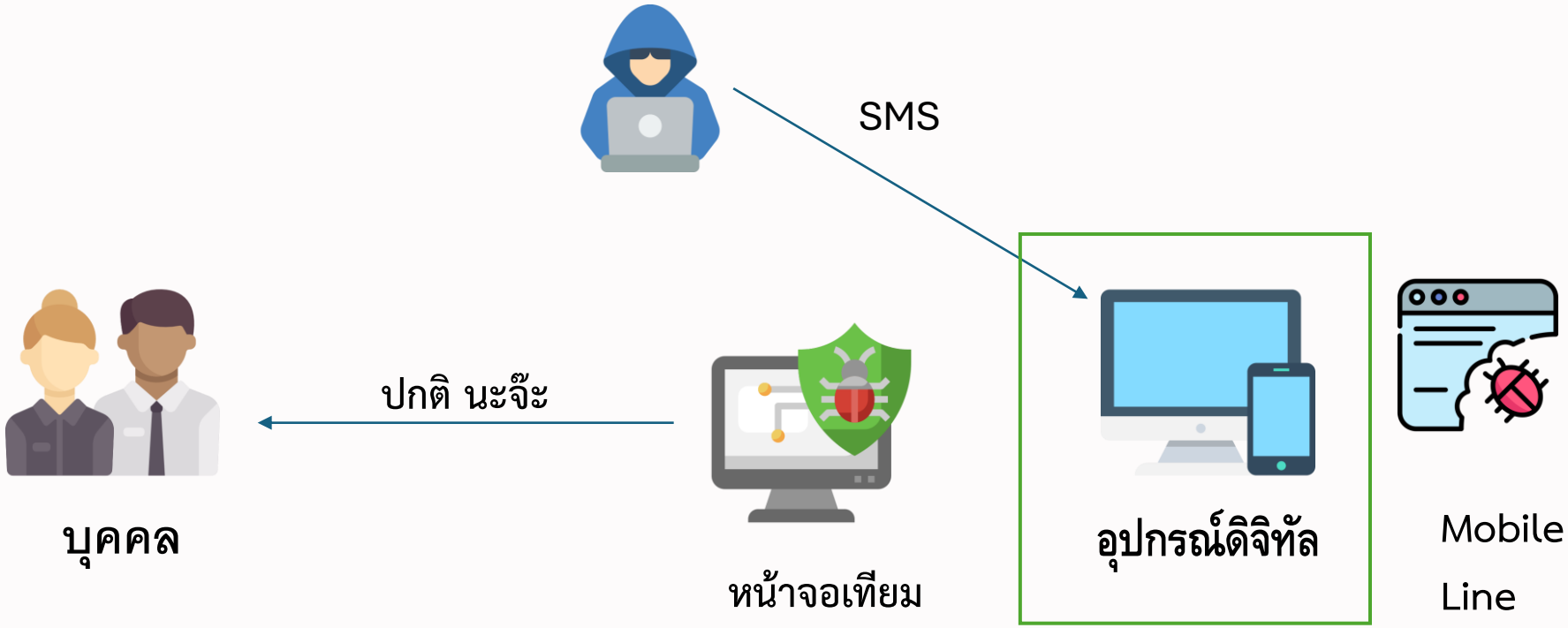
บุคคล

- แอปพลิเคชัน เถื่อนนอก Play store ,App store
- แอปจาก SMS , Email ต้องสงสัย





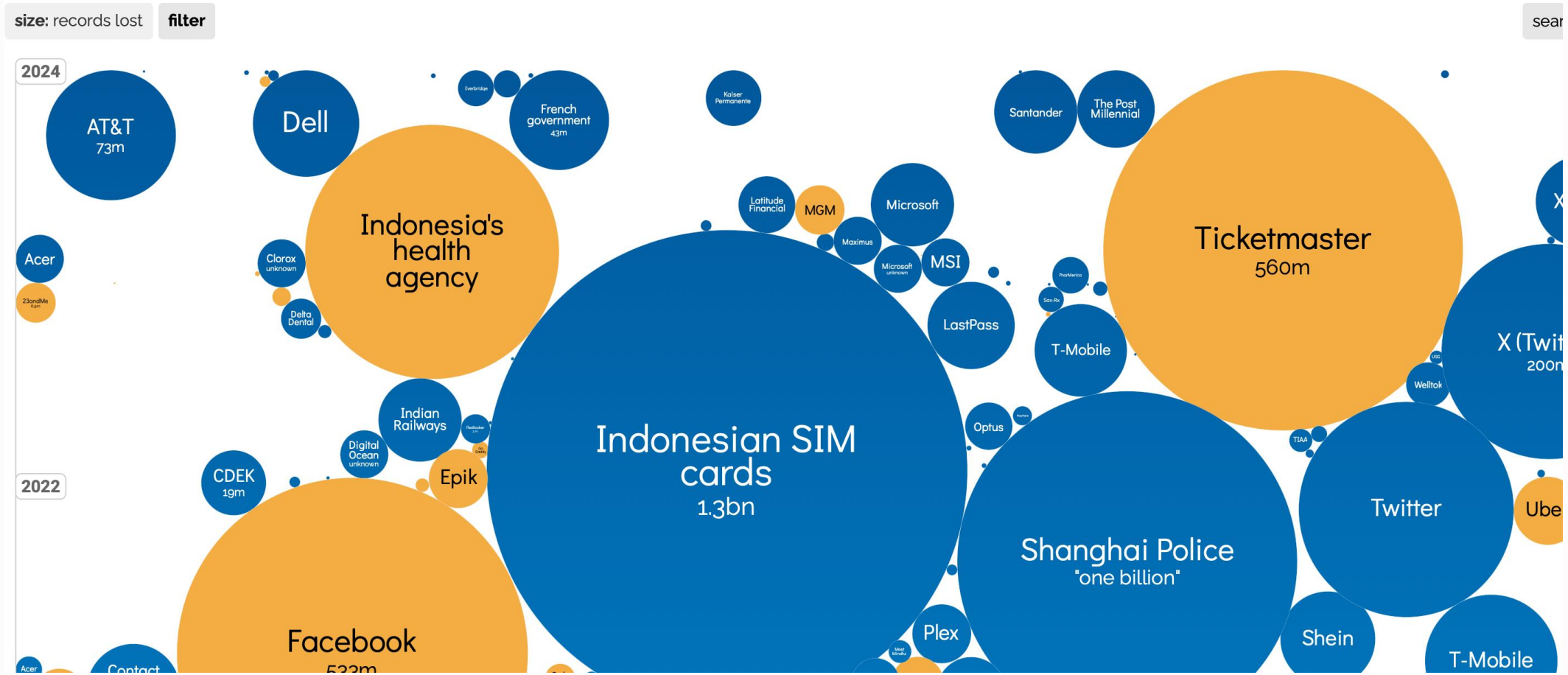
แอปดูดเงิน: แอปปลอม



กรณีตัวอย่าง เคสความเสียหายเมื่อเกิดการละเมิดความเป็นส่วนบุคคล

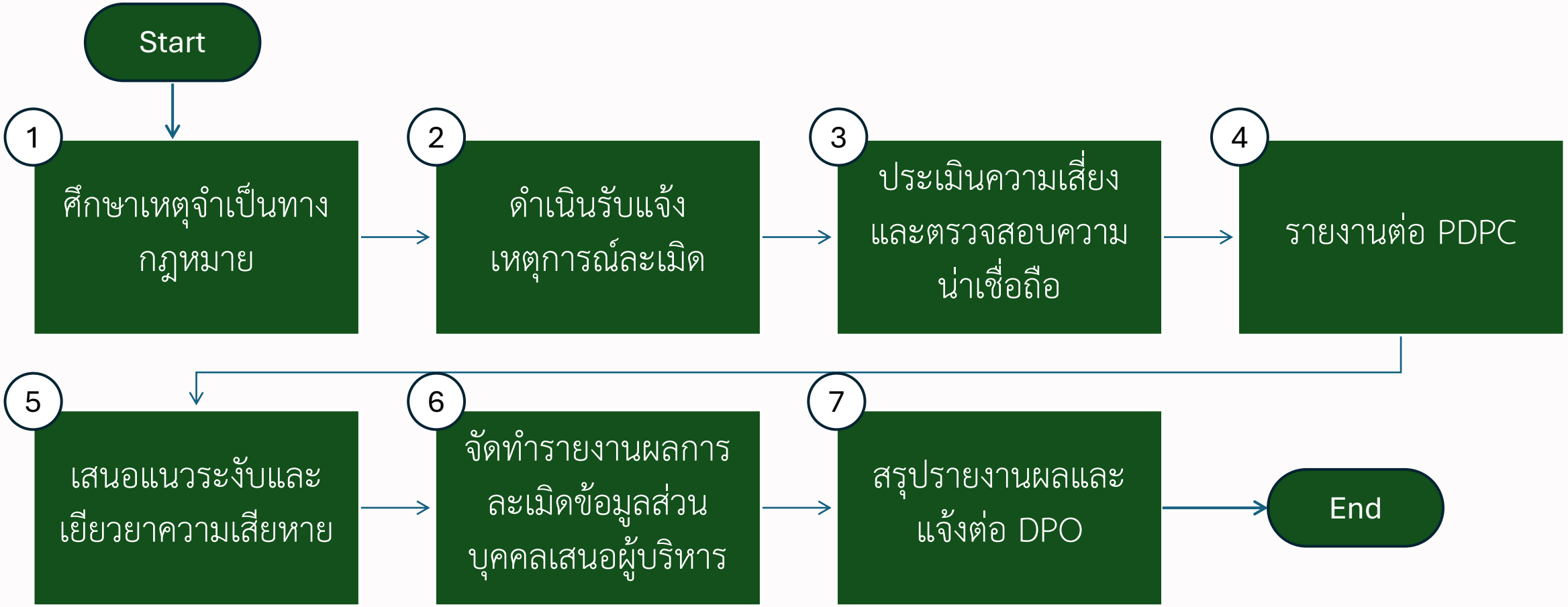
ป้องกันไว้ดีกว่าแก้ไข
เมื่อเกิดเหตุแล้ว หลายเหตุการณ์ยากที่จะแก้ไขให้กลับมาเป็นเหมือนเดิม

World's Biggest Data Breaches & Hacks



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/?fbclid=IwZXh0bgNhZW0CMTAAAR0rrtCRExROABFVz_Mzhocksf0GtuVt2YIr6ELi2GXMB4TnnV-SSyYDHeU_aem_cxyEb1EJlok0-5jG5bpueQ

ขั้นตอนปฏิบัติเมื่อเกิดการรั่วไหล/ละเมิดข้อมูลส่วนบุคคล



Cr: แนวทางปฏิบัติตาม PDPA สป.ก.เกษตรและสหกรณ์

ข้อควรปฏิบัติเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล

- **แจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง แก่สำนักงาน ฯ และแจ้งเจ้าของข้อมูลกรณีความเสี่ยงสูง (มาตรา 37)(4)**
- การรายงาน และรายงานต่อ PDPC
  - ข้อมูลเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล
  - ชื่อสถานที่ติดต่อ DC
  - ผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล
  - แนวทางเยียวยาความเสียหาย
- **บทลงโทษ หากฝ่าฝืน: ปรับสูงสุด 3 ล้านบาท**

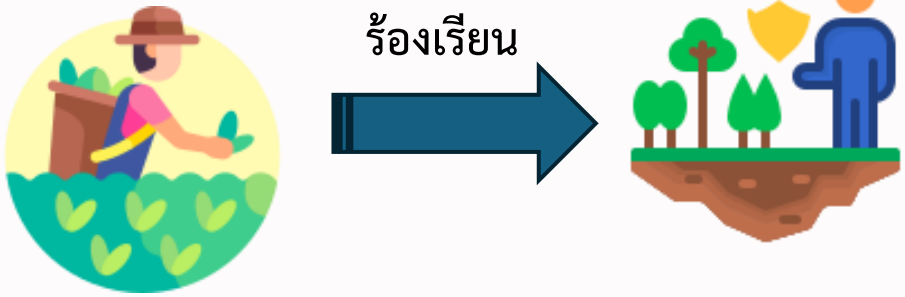
กรณีการละเมิดมีความเสี่ยงกระทบต่อสิทธิและเสรีภาพของบุคคล

- ต้องรีบระงับเหตุทันทีและยับยั้งความเสียหายที่เกิดขึ้น (Incident Respond)
- กรณีที่ต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคล (Data Subject) หากไม่สามารถแจ้งเป็นรายบุคคลได้ ให้แจ้งเป็นกลุ่มโดยไม่ให้ส่งผลต่อเจ้าของข้อมูลส่วนบุคคล
- กรณีความเสี่ยงสูงต้องจัดทำรายงานแก่ DPO ให้ไปรายงานต่อ สดช.

ถุงกล้วยแขก Reuse กับ PDPA

ขอขอบคุณแหล่งที่มา : PDPC Thailand

Discussion: กรณีศึกษา



เกษตรกร
<Data Subject>

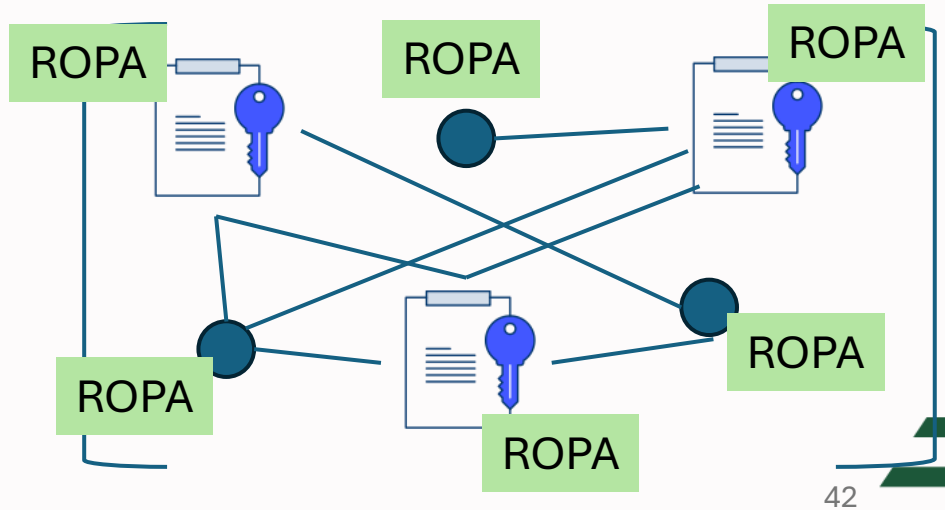
สำนักงานเกษตรจังหวัด
<Data Controller>

Q1> ถ้ามีคำร้องเรียนจากเกษตรกรในลักษณะนี้ จะต้องดำเนินการอย่างไร

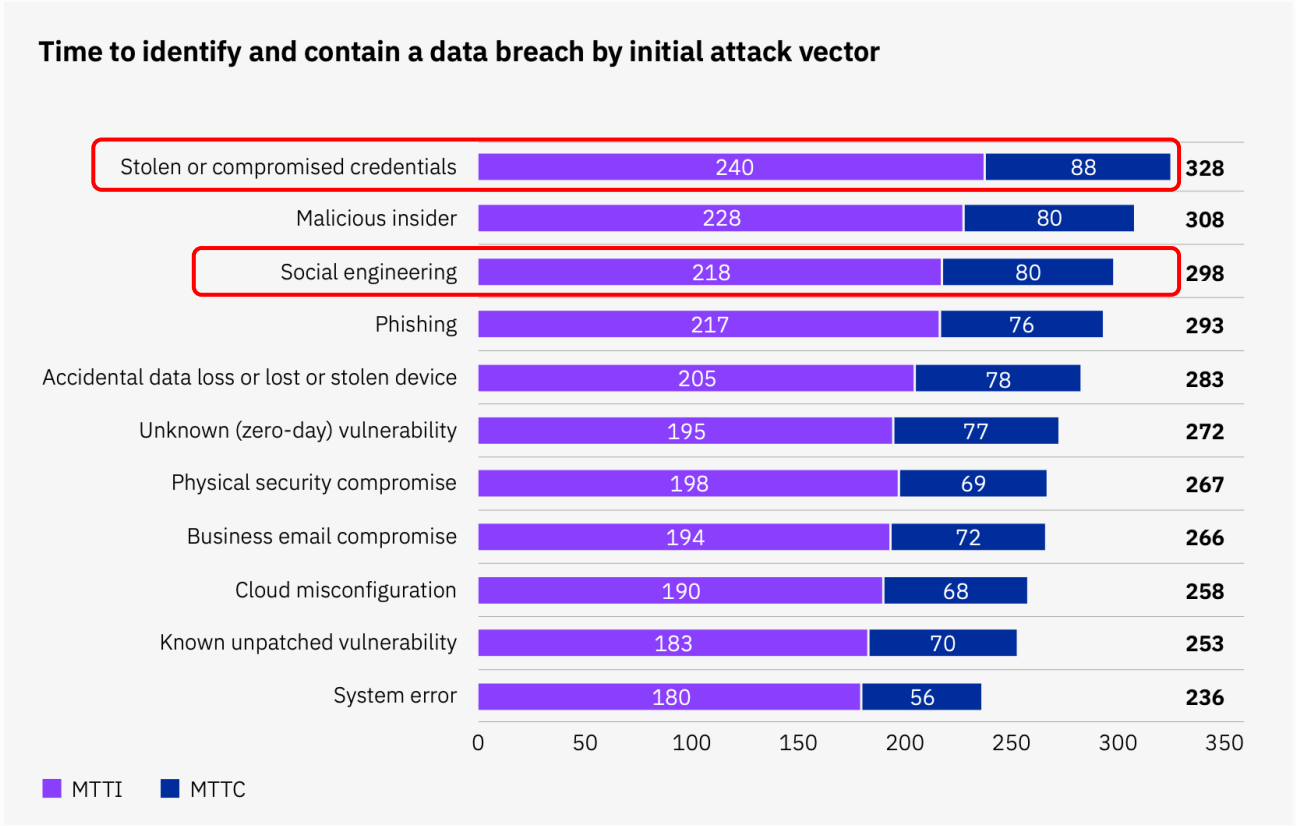
Q2> เราจะทราบได้อย่างไรว่าเกิดการรั่วไหลที่ไหนที่เรา?

คำนำหน้าชื่อ, ชื่อ – นามสกุล,เบอร์โทรศัพท์,หมายเลขบัตรประชาชน, หมายเลขบัญชีธนาคาร, Prompt pay

ข้อมูลส่วนบุคคล **รั่วไหล – หลุด**ใน Dark web และมีมิจฉาชีพ โทรมารบกวน



กรณีตัวอย่าง



IBM Security, “Cost of a Data Breach Report 2023”

https://www.pptvhd36.com/news/สังคม/217179

บันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล [Record of Data Processing Activity: ROPA]

การบันทึกรายการประมวลผลข้อมูลของ DC และตัวแทน (มาตรา 39)

- ประเภทข้อมูลส่วนบุคคลที่เก็บรวบรวมและประเภทของเจ้าของข้อมูล
- วัตถุประสงค์ในการเก็บรวบรวมแยกตามประเภทข้อมูลส่วนบุคคล
- ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล, DPO
- ระยะเวลาการเก็บรักษาและการลบข้อมูล
- สิทธิของบุคคล เงื่อนไขการกำหนดสิทธิ์ วิธีการเข้าถึง และเงื่อนไขการเข้าถึง
- การใช้หรือเปิดเผยข้อมูลที่ไม่ต้องขอ Consent (มาตรา 27 วรรค 3)
- บันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูล (มาตรา 30 วรรค 3 , 31 วรรค 3 ,32 วรรค 3 และ 36 วรรค 1)
- มาตรการรักษาความมั่นคงปลอดภัย (มาตรา 37 (1))

ความสำคัญของ [ROPA]

1. การปฏิบัติตามกฎหมาย:
การทำ ROPA เป็นข้อกำหนดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งทำให้องค์กรสามารถแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดทางกฎหมายได้

2. ความโปร่งใส
ROPA ช่วยให้องค์กรมีข้อมูลที่โปร่งใสเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ทำให้สามารถให้ข้อมูลแก่เจ้าของข้อมูลหรือหน่วยงานกำกับดูแลได้เมื่อถูกขอ

3. การบริหารความเสี่ยง
การทำ ROPA ช่วยให้องค์กรสามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล และนำมาตรการที่เหมาะสมมาปรับใช้เพื่อควบคุมความเสี่ยงเหล่านั้น

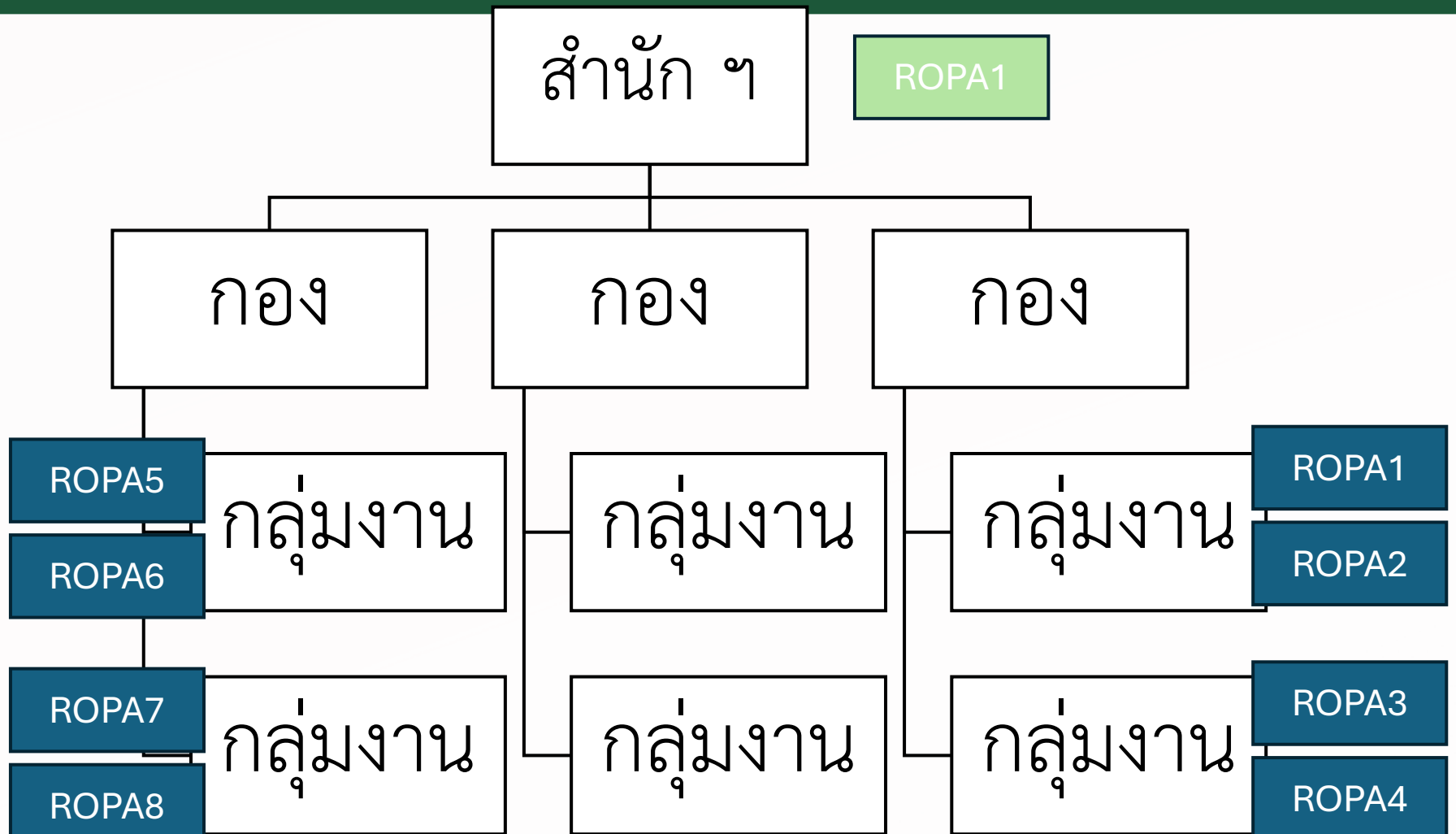
4. การจัดการข้อมูลที่มีประสิทธิภาพ
ROPA ทำให้องค์กรมีข้อมูลที่ชัดเจนเกี่ยวกับแหล่งที่มาของข้อมูลส่วนบุคคล การประมวลผลข้อมูล และการเก็บรักษาข้อมูล ซึ่งช่วยให้การจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ

5. การตรวจสอบและบังคับใช้
ROPA ช่วยให้องค์กรสามารถตรวจสอบและบังคับใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลได้ง่ายขึ้น โดยสามารถตรวจสอบและทบทวนกระบวนการประมวลผลข้อมูลได้อย่างสม่ำเสมอ

6. การเตรียมพร้อมต่อเหตุการณ์ข้อมูลรั่วไหล
เมื่อเกิดเหตุการณ์ข้อมูลรั่วไหล การมี ROPA ช่วยให้องค์กรสามารถระบุและประเมินผลกระทบได้รวดเร็วขึ้น รวมถึงสามารถเตรียมแผนรับมือและรายงานต่อหน่วยงานกำกับดูแลได้ทันที

7. การสร้างความเชื่อมั่นให้กับลูกค้าและคู่ค้า
การทำ ROPA ทำให้องค์กรสามารถแสดงให้ลูกค้าและคู่ค้าเห็นถึงความตั้งใจและความมุ่งมั่นในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะสร้างความเชื่อมั่นและความไว้วางใจในองค์กร

ความสำคัญของ ROPA กับขีดความสามารถการคุ้มครองข้อมูลส่วนบุคคลระดับองค์กร



ความสำคัญของ ROPA กับขีดความสามารถการคุ้มครองข้อมูลส่วนบุคคลระดับประเทศ

สำนักคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC)

GPPC Government Platform for PDPA Compliance

National ROPA

การรักษาความเป็นส่วนบุคคลระดับประเทศ

- สำนัก
  - ROPA1
  - ROPA N
- กรม
  - ROPA1
  - ROPA N
- กระทรวง
  - ROPA1
  - ROPA N
- อื่น ๆ
  - ROPA1
  - ROPA N

PDPC

- ประสานงาน ช่วยเหลือเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ฝึกอบรม สนับสนุนขีดความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคล

ประกาศความเป็นส่วนตัวของผู้ใช้งานระบบ GPCC

ฉบับย่อ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ต่อไปนี้จะเรียกว่า "**สคส.**") เคารพในสิทธิความเป็นส่วนตัวของท่าน ในฐานะผู้รับบริการหรือเจ้าของข้อมูลส่วนบุคคล ที่สำนักงานเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับแพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Government Platform for PDPA Compliance : GPPC) และเพื่อให้เกิดความมั่นใจว่าเจ้าของข้อมูลส่วนบุคคลได้รับการคุ้มครองข้อมูลส่วนบุคคล จึงได้จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) ฉบับนี้ขึ้น เพื่อแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์และรายละเอียดที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ดังนี้

กิจกรรมและวัตถุประสงค์	กลุ่มข้อมูลส่วนบุคคล	ฐานการประมวลผล
· เพื่อพิจารณาคุณสมบัติ · เพื่อการติดต่อประสานงานหน่วยงานผู้ขอรับการสนับสนุนฯ	· ข้อมูลอัตลักษณ์ (ชื่อ-นามสกุล, ลายมือชื่อ) · ข้อมูลที่อยู่และที่ติดต่อ (เบอร์โทรศัพท์, อีเมล) · ข้อมูลเกี่ยวกับการทำงาน (ตำแหน่ง, ชื่อหน่วยงาน, ประเภทหน่วยงาน, อีเมลของหน่วยงาน)	· เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา มาตรา 24 (3) · เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย มาตรา 24 (5)

สคส. จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน ภายในระยะเวลาที่จำเป็นในการดำเนินการตามวัตถุประสงค์ เป็นระยะเวลา 2 ปี นับแต่วันที่ท่านลงทะเบียนขอสนับสนุนแพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Government Platform for PDPA Compliance : GPPC) และเมื่อหมดความจำเป็นที่จะต้องเก็บข้อมูลตามระยะเวลาดังกล่าว สคส. จะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลนั้นอย่างถาวรหรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้

ทั้งนี้ สคส. มีมาตรการรักษาความมั่นคงปลอดภัย ตาม (37) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ท่านสามารถใช้สิทธิของเจ้าของข้อมูลท่านตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ที่ dpo@pdpc.or.th

หน่วยงาน/ส่วนงาน ผู้ติดต่อ (Required)

การดำเนินการที่ประสงค์เข้าร่วม (โปรดระบุในส่วนที่ประสงค์รับการสนับสนุน โดยสามารถเลือกอย่างใดอย่างหนึ่ง หรือทั้งสามส่วน) (Required)

ขั้นตอน การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงาน ระดับ กอง/ศูนย์/สำนัก/สถาบัน ในสังกัด สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

1. ทบทวน

- หน่วยงาน ทบทวน กิจกรรม ที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคล พร้อมกำหนดผู้รับผิดชอบ

2. แบบฟอร์ม

- เมื่อได้กิจกรรมที่เกี่ยวข้องกับให้หน่วยงานบันทึกกิจกรรมดังกล่าวตามแบบฟอร์ม template_RoPA และ template_Privacy Notice

สามารถดาวน์โหลดแบบฟอร์มได้ที่เว็บไซต์การคุ้มครองข้อมูลส่วนบุคคล สป.กษ. (https://www.opsmoac.go.th/pdpa-home)

3. พิจารณา

- เมื่อจัดทำข้อมูลเรียบร้อยแล้วให้หน่วยงานเสนอหัวหน้าส่วนพิจารณากิจกรรมการประมวลผลข้อมูลส่วนบุคคลและประกาศความเป็นส่วนตัว(Privacy Notice)ที่ดำเนินการในข้อ 2 พร้อมจัดส่งข้อมูลในรูปแบบไฟล์อิเล็กทรอนิกส์และเอกสารให้ ศทส.

4. ตรวจสอบ

- เมื่อศทส.ได้รับข้อมูล RoPA และ Privacy Notice จะดำเนินการตรวจสอบความถูกต้องและให้ข้อแนะนำ ในกรณีที่ต้องปรับแก้ไข พร้อมส่งให้หน่วยงานเจ้าของเรื่องปรับปรุงให้ถูกต้อง

5. กฎหมาย

- เมื่อหน่วยงานปรับปรุงเสร็จแล้ว ศทส.จะเสนอให้สำนักกฎหมาย พิจารณาให้ความเห็นก่อนเผยแพร่ Privacy Notice บนเว็บไซต์ ส่วนข้อมูล RoPA จะจัดเก็บลงแหล่งข้อมูลกลาง (Next Cloud) ของสป.กษ.

6. GPPC

- ศทส.จะนำข้อมูล RoPA ที่ผ่านการพิจารณาแล้วบันทึกเข้าสู่ระบบ GPPC

7. เข้าระบบ

- เจ้าหน้าที่ ศทส. ประสานแจ้งกลับไปที่หน่วยงานเจ้าของ RoPA ให้บันทึกข้อมูล RoPA ในระบบ GPPC

8. สิ้นสุด

สิ้นสุดการดำเนินงาน

GPPC
Government Platform for PDPA Compliance
(https://gppc-app.onde.go.th)

จัดทำโดย กลุ่มบริหารข้อมูลการเกษตร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร E-mail : ict_aim@opsmoac.go.th Tel : 02-281-5955 ต่อ 363

#Workshop

การบันทึกรายการประมวลผลข้อมูลข้อมูลส่วนบุคคล

(Record of Data Processing Activity: ROPA)

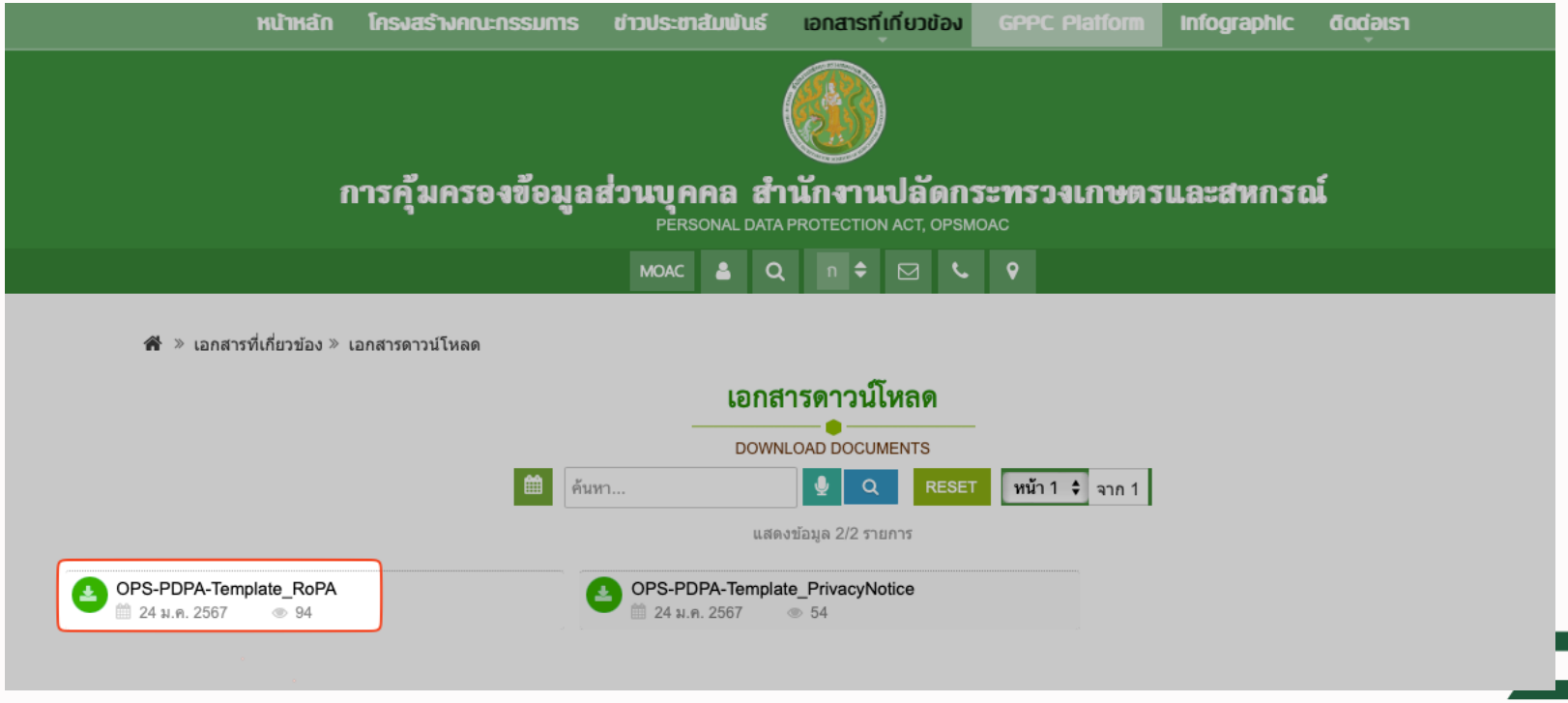
วันที่ 12 กรกฎาคม พ.ศ. 2567

https://docs.google.com/spreadsheets/d/18cEHkoKJrlY1-VSmtl_UTpP9gVVK2xqACk3wUQujUyQ/edit?usp=sharing

#Workshop (Assignment)

ขั้นตอนที่ 1 : ให้ผู้เข้าร่วมอบรม กลับไปสำรวจ การเก็บ-ใช้งานข้อมูลส่วนบุคคลในองค์กร

ขั้นตอนที่ 2 : จัดทำ ROPA ส่งให้กับ ศูนย์เทคโนโลยีสารสนเทศ



https://www.opsmoac.go.th/pdpa-doc-download

QA