POWERED BY
SECURITY PiTCH
Touchable Security

ความเข้าใจ “PDPA” เบื้องต้น

ประเด็น

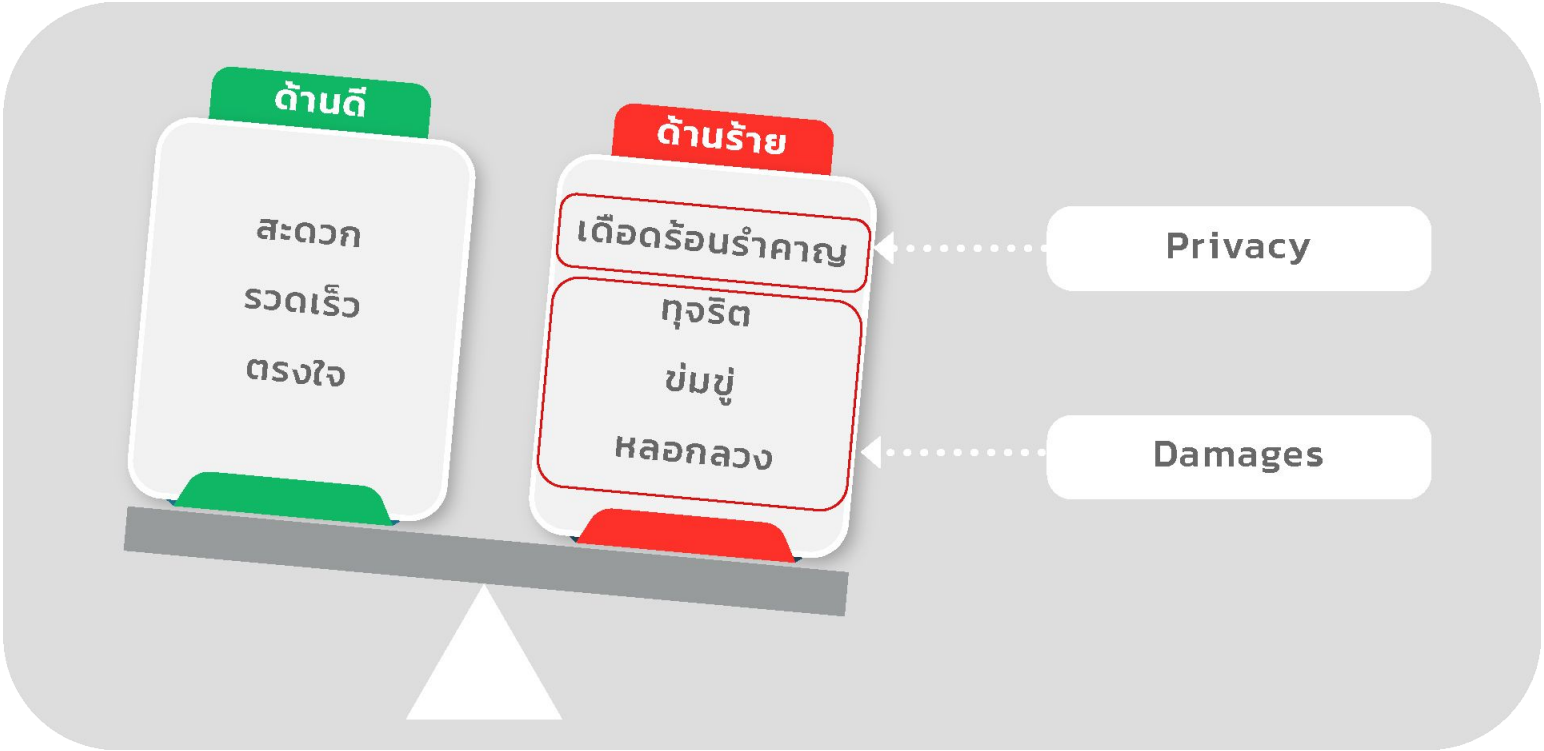
- ความเป็นมาของกฎหมาย PDPA
- ข้อมูลส่วนบุคคล และบุคคลที่เกี่ยวข้องใน PDPA
- หลักการประมวลผลข้อมูลส่วนบุคคล
- การดำเนินการที่กำหนดไว้ใน PDPA
- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ความเสี่ยงและความรับผิดในกฎหมาย PDPA

ความเป็นมา
ของกฎหมาย PDPA

การประกอบธุรกิจ อดีต & ปัจจุบัน

Know Your Customer's (DATA)

การประกอบธุรกิจ & ข้อมูลส่วนบุคคล



ความจำเป็นของการมีกฎหมาย PDPA

POWERED BY SECURITY PiTCH Touchable Security

ก่อนมี PDPA

- กฎหมายไทยมุ่งคุ้มครองกรรมสิทธิ์ (Ownership) มากกว่า สิทธิความเป็นส่วนตัว (Privacy Rights)
- การฟ้องคดีมีโอกาสชนะยากและได้ค่าเสียหายน้อย (ภาระการพิสูจน์อยู่ที่เจ้าของข้อมูล)

ความจำเป็นของการมีกฎหมาย PDPA

POWERED BY SECURITY PiTCH Touchable Security

หลังมี PDPA

- ให้ความคุ้มครองกรรมสิทธิ์ (Ownership) เท่ากับ สิทธิความเป็นส่วนตัว (Privacy Rights)
- การฟ้องคดี เจ้าของข้อมูลมีโอกาสชนะง่าย (ผลักภาระการพิสูจน์ ให้ผู้ประกอบการ : Data Controller) และได้ค่าเสียหายมาก (ศาลให้ค่าเสียหายเชิงลงโทษเพิ่มได้)

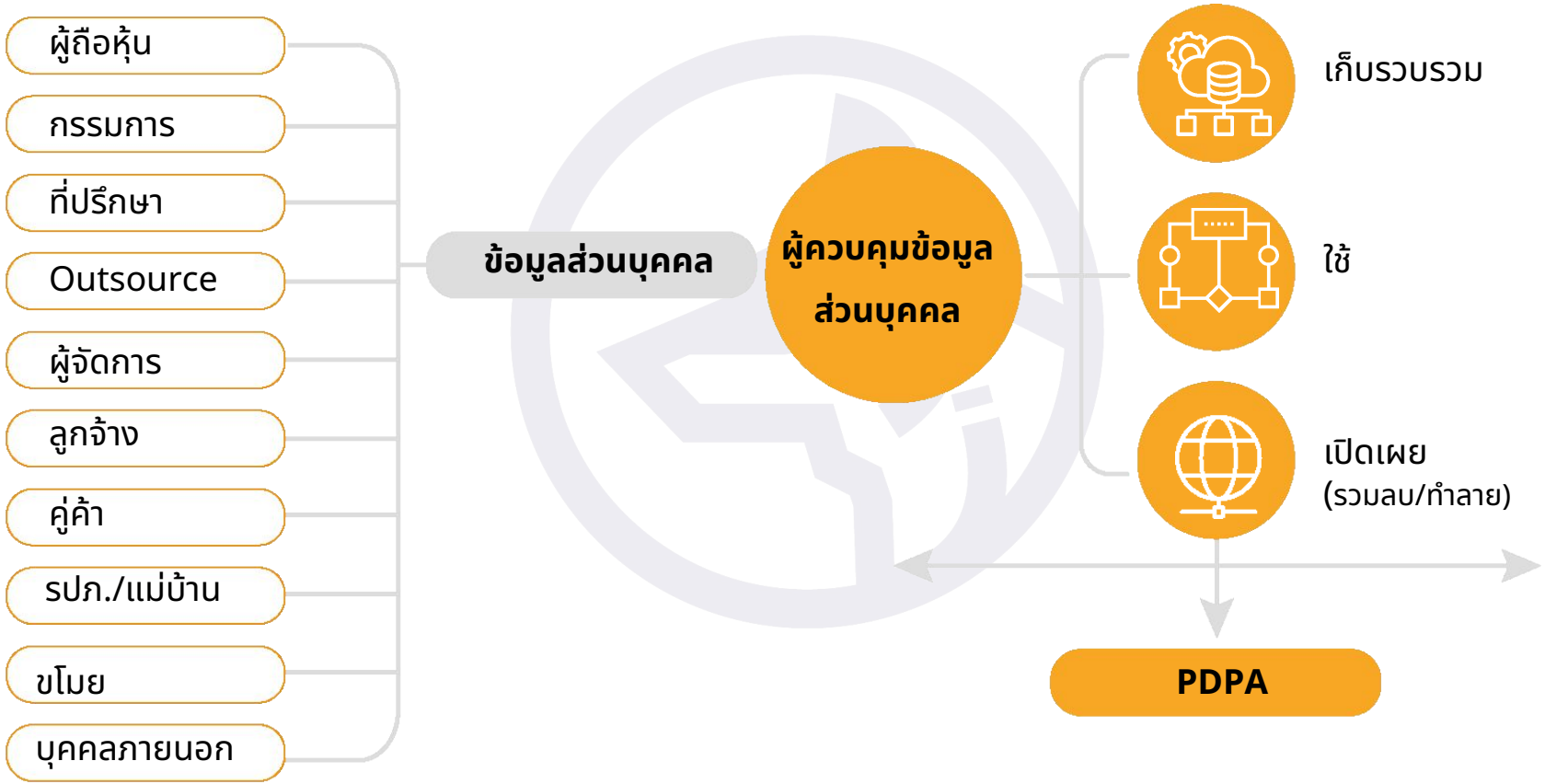
หลักการสำคัญของกฎหมาย PDPA

POWERED BY SECURITY PiTCH Touchable Security

1. PDPA ไม่ใช่ระบบขออนุญาต (Not any Licenses under PDPA)
2. PDPA กำหนดเพียงหลักการ แต่ไม่ได้กำหนดรูปแบบมาตรฐานในการปฏิบัติตามกฎหมาย (Processing Data by Design)
3. ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้ประมวลผลข้อมูลส่วนบุคคล) มีหน้าที่ ต้องพิสูจน์ตนเอง ว่าได้ปฏิบัติตามที่ PDPA กำหนดไว้ครบถ้วนแล้ว

Know Your DATA

หลักการสำคัญของกฎหมาย PDPA



หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

DS

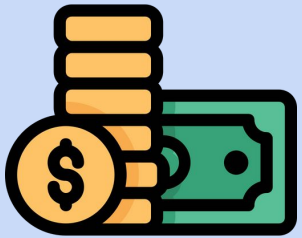
DC

จำเป็น / อธิบายได้
(มีฐาน)

โปร่งใส
(Privacy Policy / Consent etc.)

มีความปลอดภัย
(ประกาศ ส.ค.ส.)

ความรับผิดของผู้ประกอบการ



ทางแพ่ง

Data Subject
เป็นผู้ฟ้องร้อง

ทางอาญา

Data Subject
เป็นผู้ฟ้องร้อง

ทางปกครอง

ส.ค.ส.
เป็นผู้มีอำนาจบังคับใช้

PDPA

ข้อมูลส่วนบุคคล
และบุคคลที่เกี่ยวข้องใน PDPA

ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคล

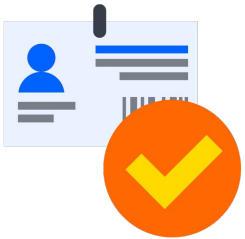
หมายความว่า ข้อมูลเกี่ยวกับบุคคล(ธรรมดา) ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม

แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

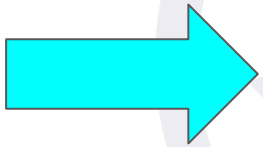
** ทั้งข้อมูลในรูปแบบเอกสาร และอิเล็กทรอนิกส์ **

ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูล
ข้อมูลเดี่ยว / ชุดข้อมูล



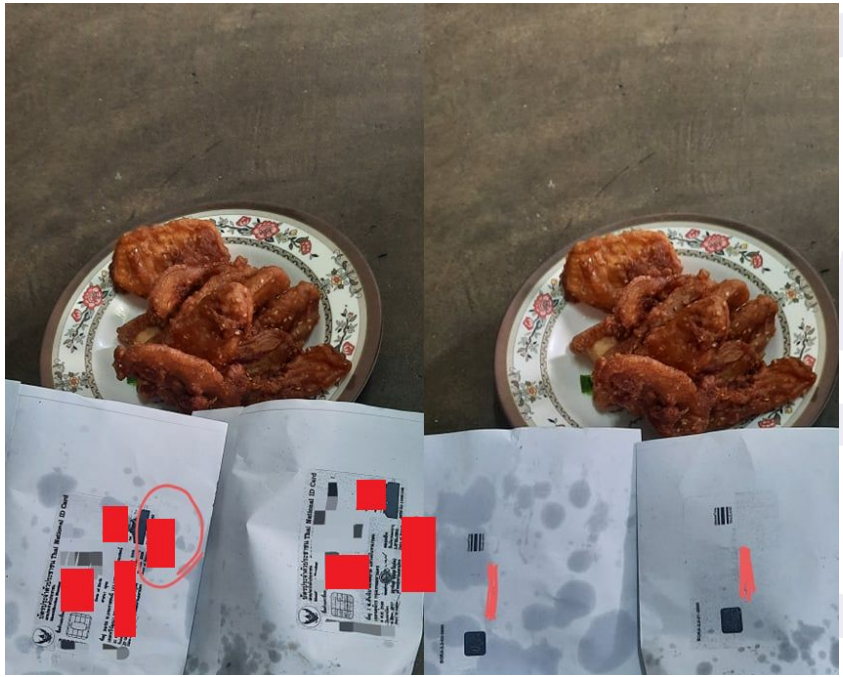
ระบุตัวบุคคลได้



ข้อมูลส่วนบุคคล

ไม่คำนึงว่า **“ข้อมูลส่วนบุคคล”** นั้น จะมีคุณค่าหรือมูลค่าในทางเศรษฐกิจหรือไม่ และข้อมูลนั้นจะเป็นจริงหรือเท็จ

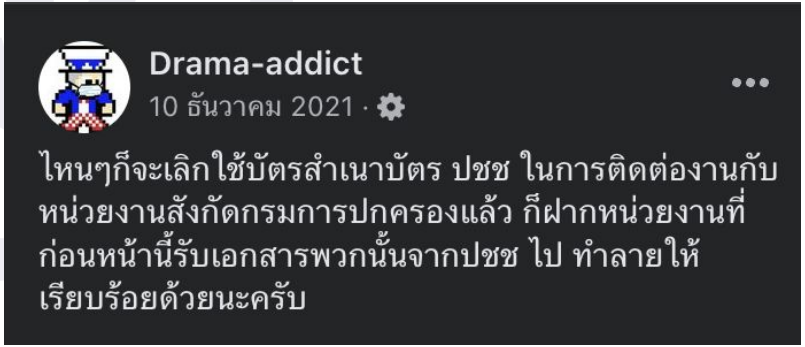
กรณีศึกษา (ประเทศไทย)



การถมสีในข้อมูลบางส่วนแล้วทำให้ ข้อมูลส่วนที่เหลือ

ระบุตัวตนไม่ได้จะ ช่วยให้เอกสารชุดนั้น ไม่เป็นข้อมูลส่วน

บุคคลอีกต่อไป



ประเภทของข้อมูลส่วนบุคคล

<u>แบ่งเป็น 2 ประเภท</u>

- ข้อมูลส่วนบุคคลทั่วไป (Personal Data)
- ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ได้แก่ เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ หรืออื่น ๆ ตามที่คณะกรรมการประกาศกำหนด

บุคคลที่เกี่ยวข้องใน PDPA

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลธรรมดาที่ข้อมูลส่วนบุคคลสามารถเชื่อมโยงไปถึง

หรือสามารถระบุตัวตนได้ ไม่ว่าทางตรงหรือทางอ้อม

บุคคลที่เกี่ยวข้องใน PDPA

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ

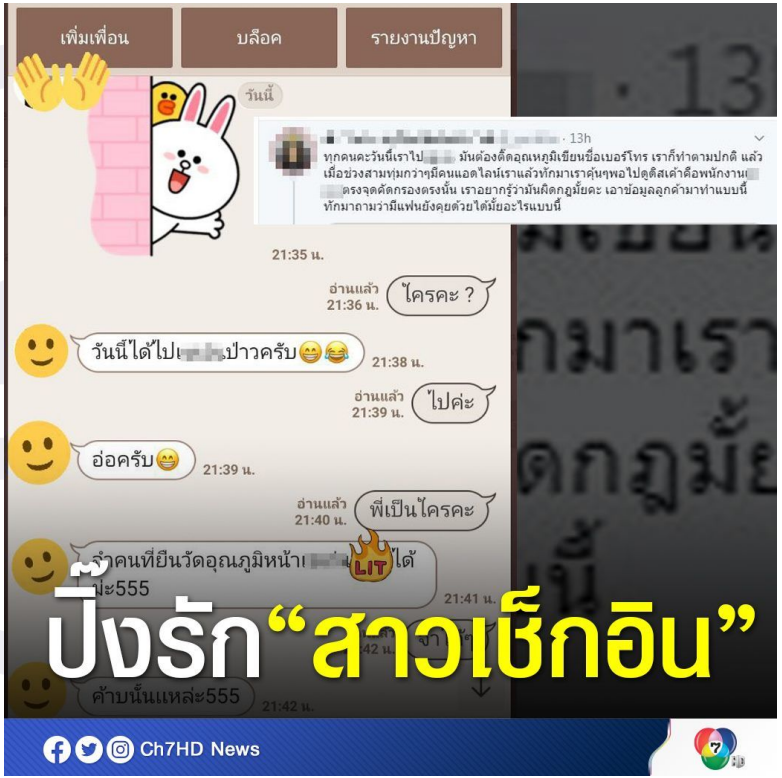
เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน

บุคคล

ลูกจ้าง ไม่ใช่ ผู้ควบคุมข้อมูลส่วนบุคคล

กรณีศึกษา (ประเทศไทย)

https://hilight.kapook.com/view/194855



https://www.ch7.com/sports/415190

- การที่**พนักงาน**ทำนอกหน้าที่ หรือคำสั่ง ในกิจกรรมใดกิจกรรมหนึ่ง อาจทำให้พนักงานท่านนั้นกลายเป็น**ผู้ควบคุมข้อมูลส่วนบุคคล** ในกิจกรรมนั้น
- แต่**บริษัท**ก็ยังมีความรับผิดอยู่ หากการกระทำของพนักงานนั้นเกิดจากการที่บริษัทมี**มาตรการรักษาความมั่นคงปลอดภัย** ที่ไม่เหมาะสมเพียงพอ

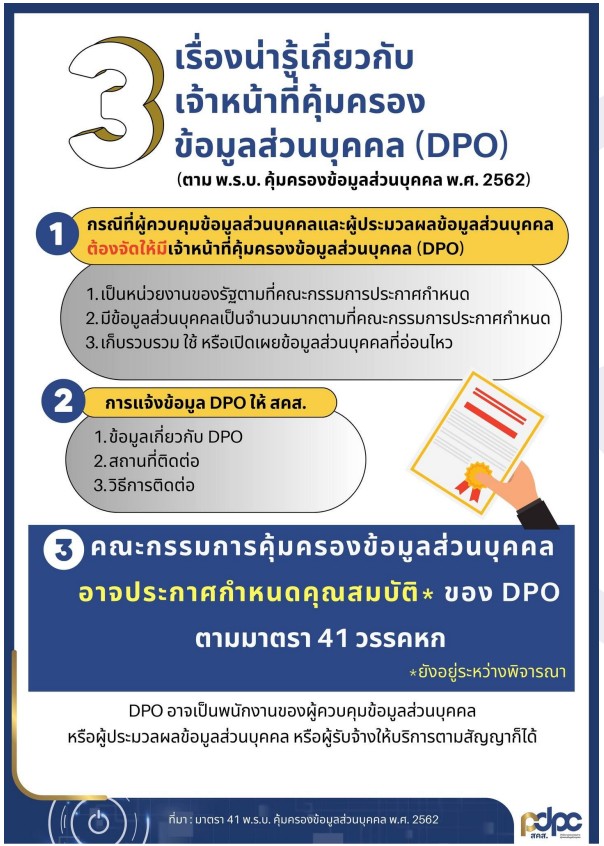
บุคคลที่เกี่ยวข้องใน PDPA

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการ**เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคล ซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

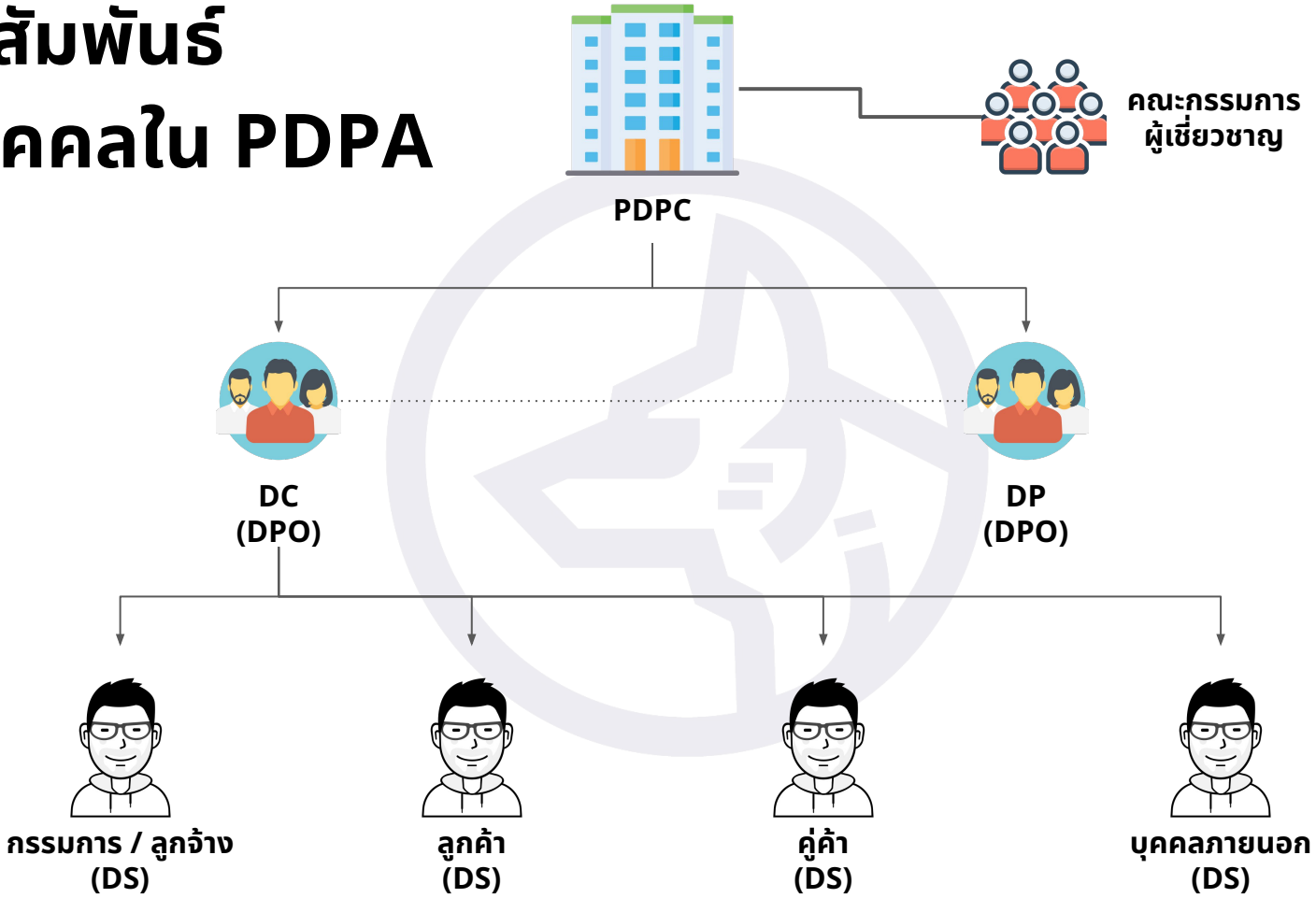
ลูกจ้าง ไม่ใช่ ผู้ประมวลผลข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)



ม. 41

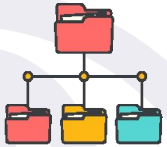
ความสัมพันธ์ของบุคคลใน PDPA



หลักการประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล

การประมวลผล
ข้อมูลส่วนบุคคล



เก็บ รวบรวม

ใช้

เปิดเผย รวมถึง /ทำลาย

การเก็บรวบรวม

กฎหมายระบุว่า

เก็บได้เท่าที่จำเป็น และ ห้าม เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

กรณีเก็บจากแหล่งอื่น

1. แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วัน และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. เป็นการเก็บ รวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

หลักการเก็บเท่าที่จำเป็น

POWERED BY SECURITY PiTCH Touchable Security

การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น (Data Minimization)

- วัตถุประสงค์ (PurposeLimitation)
- ฐานทางกฎหมาย (Lawful Basis)
- ระยะเวลาในการจัดเก็บ (Time Limit)
- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

“จำเป็น” รวมถึง เก็บ “ถูกเวลา” ด้วย

ฐานในการประมวลผล (ข้อมูลส่วนบุคคลทั่วไป)

หลัก : ความยินยอม

ข้อยกเว้น (ไม่ต้องขอความยินยอม)

1. เพื่อปฏิบัติตามสัญญา (เอกชน)
2. เพื่อปฏิบัติตามภารกิจของรัฐ (หน่วยงานของรัฐ)
3. ปฏิบัติตามกฎหมาย
4. เพื่อประโยชน์อันชอบธรรม
5. ป้องกันหรือระงับอันตรายต่อชีวิตและสุขภาพ
6. จัดทำเอกสารประวัติศาสตร์ การศึกษา วิจัย

ม. 24

ภาพจาก Facebook

ฐานสัญญา (Contract)

ฐานนี้ควรเป็นฐานที่นำมาปรับใช้มากที่สุด

1. เป็นกรณีที่ข้อมูลส่วนบุคคลนั้นมีความจำเป็นต่อการปฏิบัติตามสัญญา หรือการให้บริการระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วน บุคคล เช่น สัญญากู้ยืม สัญญาซื้อขาย หรือสัญญาจ้างแรงงาน เป็นต้น ซึ่งหากไม่มีข้อมูลดังกล่าวจะไม่สามารถปฏิบัติตามสัญญาระหว่างกันได้ (ทั้งนี้น่าจะรวมถึงขั้นตอนก่อนเข้าทำสัญญาด้วย เช่น การขอสินเชื่อ หรือ การรับสมัครงาน หรือการขอสมัครสมาชิก เป็นต้น)
2. ฐานสัญญานี้ใช้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น **ไม่นำมาใช้**กับข้อมูลส่วน บุคคลอ่อนไหวด้วย

ฐานเพื่อประโยชน์อันชอบธรรม (Legitimate Interest)

มาตรา 24 (5)

เป็นการจำเป็นเพื่อประโยชน์โดย ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วน บุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่า สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ฐานเพื่อประโยชน์อันชอบธรรม (Legitimate Interest)

ข้อสังเกต

1. ฐานนี้เป็นฐานที่มีความยืดหยุ่นมากที่สุดเพื่อช่วยให้การประมวลผลข้อมูลส่วนบุคคลของผู้ประกอบการดำเนินการต่อไปได้ตาม วัตถุประสงค์ของกิจการ
2. แต่เป็นฐานที่มีความเสี่ยงจากการตีความมากที่สุดว่าจะเป็น ประโยชน์อันชอบธรรมของผู้ประกอบกิจการที่ DS พึงคาดหมายได้ หรือ กระทบต่อความเป็นส่วนตัวของ DS เล็กน้อยจริงหรือไม่

ฐานในการประมวลผล (ข้อมูลส่วนบุคคลอ่อนไหว)

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ม.26

(๕) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ม.26

ข้อมูลที่เก็บก่อนกฎหมายใช้บังคับ

POWERED BY SECURITY PiTCH Touchable Security

1. ผู้ควบคุมข้อมูลส่วนบุคคล**เก็บรวบรวมและใช้** (ไม่รวมเปิดเผย) ข้อมูลส่วนบุคคลนั้นต่อไป **ได้ตามวัตถุประสงค์เดิม**
2. ต้อง**กำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์**ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูล ส่วนบุคคลเก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถ**แจ้งยกเลิก ความยินยอมได้โดยง่าย**
3. **การเปิดเผย**และการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการ ใช้ข้อมูลส่วนบุคคลให้ดำเนินการให้**เป็นไปตามที่กฎหมายกำหนด**

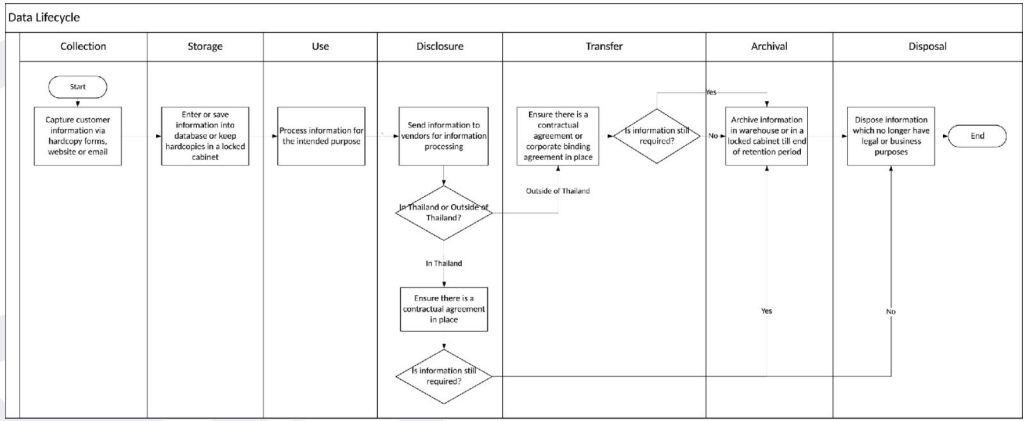
การดำเนินการ
ที่กำหนดไว้ใน PDPA

การดำเนินการที่สำคัญใน PDPA

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

วงจรชีวิตของข้อมูลส่วนบุคคล (Data Life Cycle)

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



ภาพตัวอย่างการเขียน Data Flow ของ PDPC

แบบบันทึกรายการ
ตามกฎหมาย PDPA

การบันทึกรายการตามกฎหมาย PDPA

1. การบันทึกรายการข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 39 **[RoPA]** (เพื่อให้ DS หรือ สคส. ตรวจสอบได้)
2. การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล ตามมาตรา 40 (3) ประกอบ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูล ส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 (เพื่อให้ DC หรือ สคส. ตรวจสอบได้)

จัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้

ข้อยกเว้น ไม่ต้องทำ ROPA

มาตรา 39 วรรคท้าย

ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้ บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตาม หลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำ ROPA เสมอ

พักเบรก
10 นาที

ประกาศ
/ นโยบายคุ้มครองข้อมูลส่วนบุคคล

ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 23

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือ ในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่ เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการน าข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึงรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อ านาจ ในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความ จ าเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลา ในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลา ดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐาน ของการเก็บรวบรวม

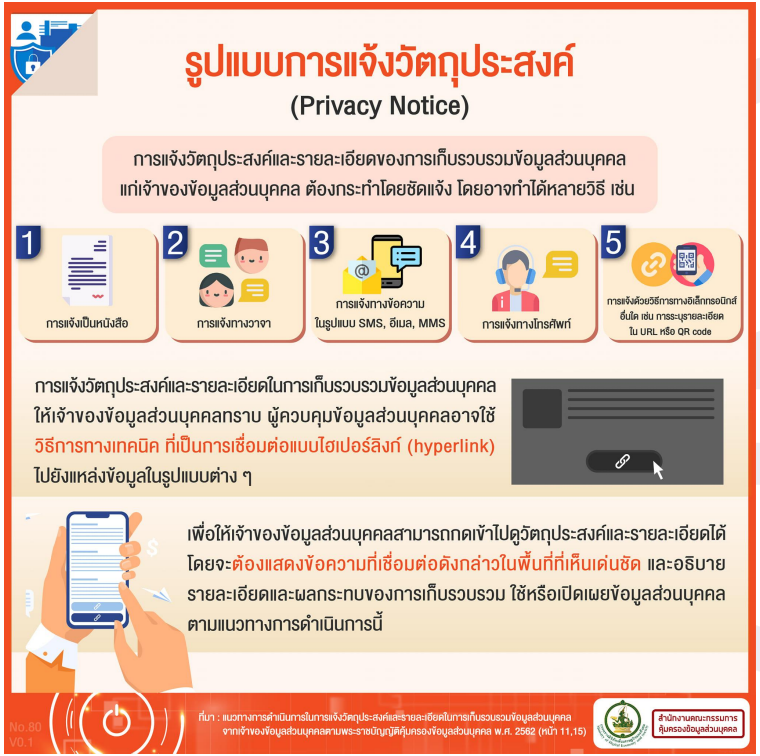
(4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บ รวบรวมอาจจะถูกเปิดเผย

ประกาศ / นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และ วิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 73 วรรคหนึ่ง

แนวทางการแจ้ง Privacy Notice

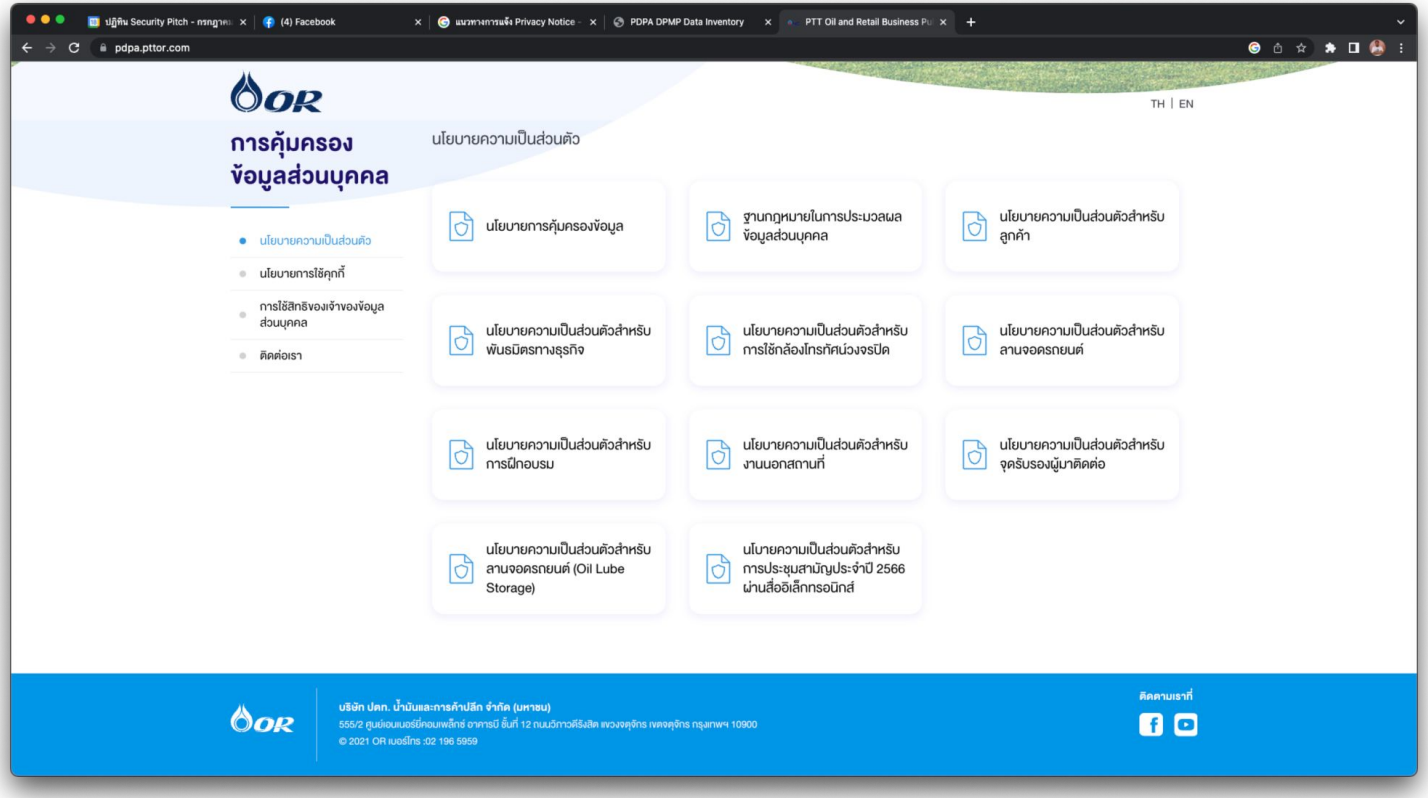


ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

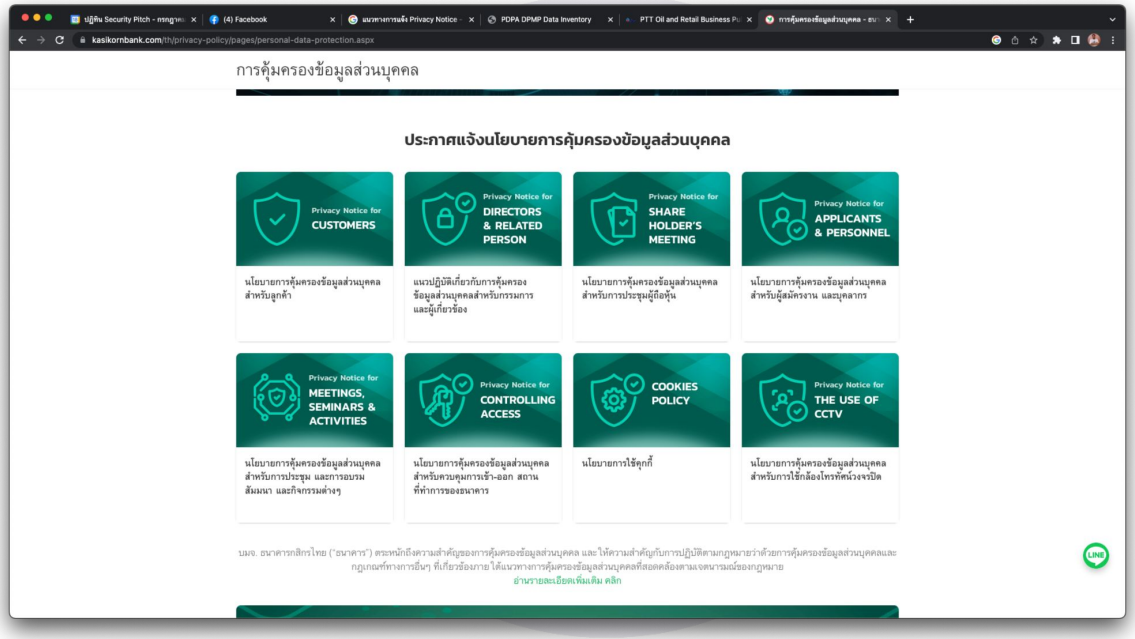
ตัวอย่างการแจ้ง Privacy Notice

ภาพจาก Facebook

ตัวอย่าง Privacy Notice (แบบแยก)



ตัวอย่าง Privacy Notice (แบบแยก)



ภาพจาก https://www.kasikornbank.com/th/personal

การใช้สิทธิ
ของเจ้าของข้อมูลส่วนบุคคล

การขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิการได้รับการแจ้งให้ทราบ (มาตรา 23)
- สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล (มาตรา 33)
- สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (มาตรา 30)
- สิทธิในการเพิกถอนความยินยอม (มาตรา 19)
- สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล (มาตรา 28,31)
- สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล (มาตรา 34)
- สิทธิในการคัดค้านการประมวลผล (มาตรา 32)
- สิทธิในการแก้ไขข้อมูลส่วนบุคคล (มาตรา 35)

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การปฏิเสธการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐ หรือหน้าที่ตามกฎหมาย	ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล [162]	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓

ภาพจาก Thailand Guideline Personal Data Protection (TGPD) 2.0, 2563

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

การขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา 40 วรรคสาม

การ

ดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลที่ไ
ด้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่
ง **ผู้ควบคุมข้อมูล ส่วนบุคคลต้องจัดให้มีข้อตกลง
ระหว่างกัน** เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้
ประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามพระราชบัญญัติ
นี้

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

นโยบายการลบ / ทำลายข้อมูลส่วนบุคคล

การเปิดเผย (การลบ / ทำลาย)

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

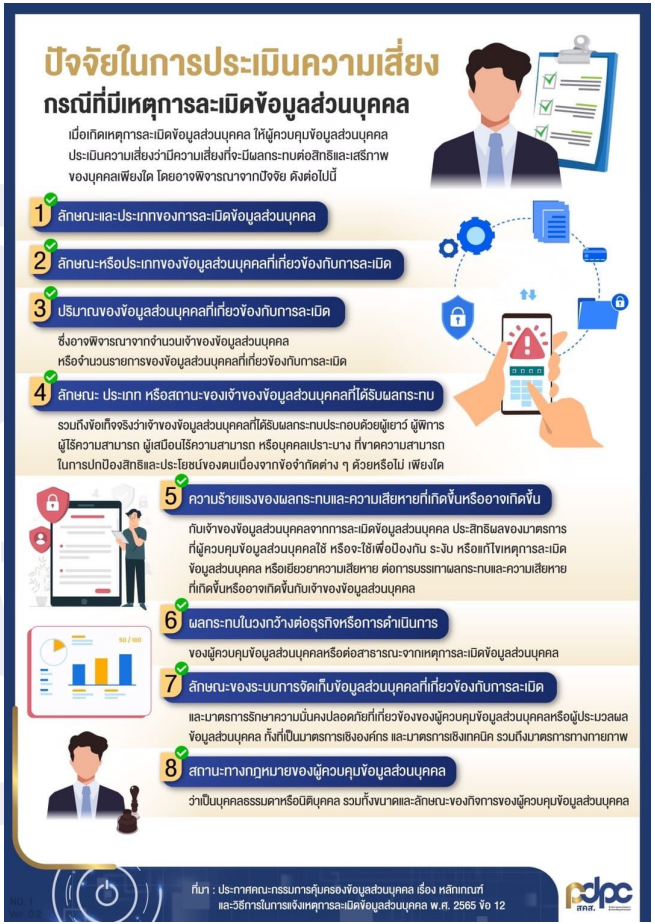
การเปิดเผย (การลบ / ทำลาย)

ม.37 (4)

การดำเนินการของ DC

1. DC ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อ สคส. โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ที่ทราบเหตุเท่าที่สามารถทำได้ เว้นแต่ การละเมิดนั้นไม่มีความเสี่ยงที่จะกระทบสิทธิและเสรีภาพของ DS
2. กรณีการละเมิดมีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของ DS ให้แจ้งการละเมิดข้อมูลส่วนบุคคลนั้นให้ DS ทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาพจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การรักษา
ความมั่นคงปลอดภัย

การรั่วไหลของข้อมูลส่วนบุคคล

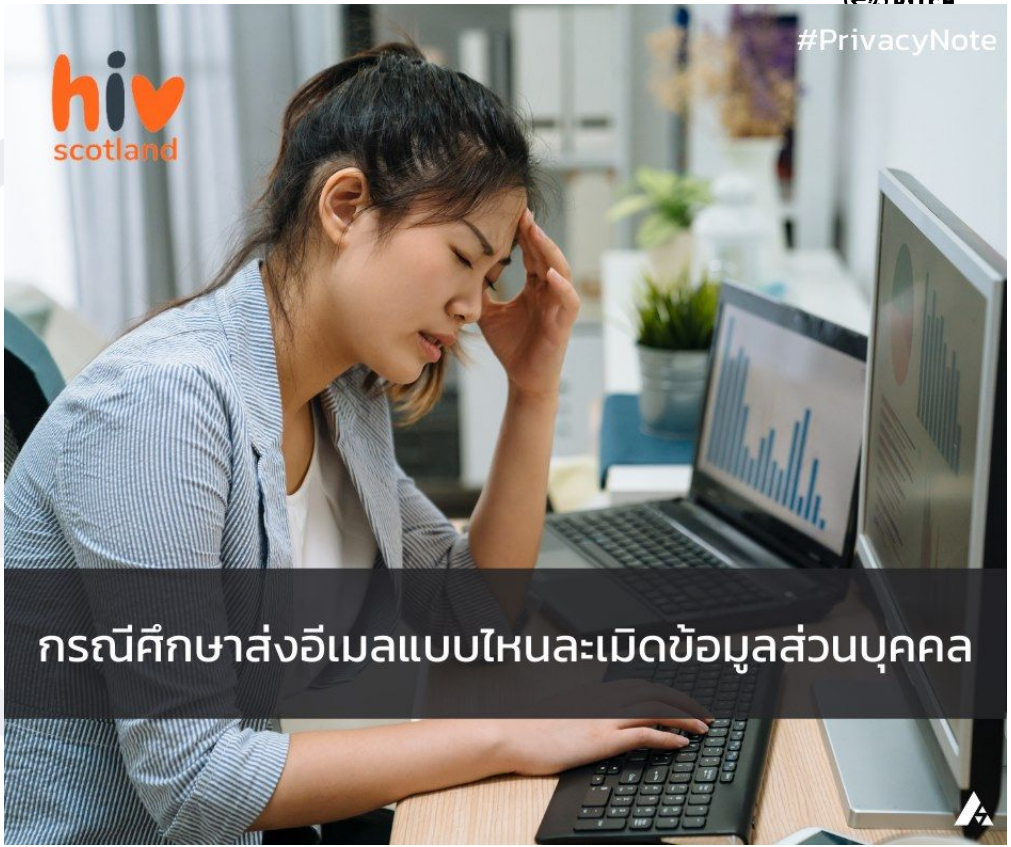
การรั่วไหลของข้อมูลส่วนบุคคลอาจเกิดขึ้น ทั้งทางด้านกายภาพและทางด้านเทคนิค โดยสามารถเกิดขึ้นได้ใน 2 ช่องทาง

1. **จากบุคคลภายนอก** เช่น ขโมย หรือ แฮ็กเกอร์ (Hacker) เป็นต้น
2. **จากบุคลกรภายใน**
   - 2.1. บุคลากรภายในนำข้อมูลส่วนบุคคลไปใช้โดยไม่มีอำนาจ หรือ ไม่ชอบด้วยกฎหมาย **(คนทำผิด)**
   - 2.2. บุคลากรภายในสามารถเข้าถึง หรือ ได้รับข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น **(อยู่ผิดที่ / ผิดคน)**

กรณีศึกษา (ต่างประเทศ)

พนักงานของสถาบันโรคภูมิคุ้มกันบกพร่องสกอตแลนด์ที่ได้ส่งอีเมล์ไปยังผู้ป่วย 150 คน ซึ่งอีเมล์ของทุกคนจะปรากฏอยู่ในรายการของผู้รับของทั้งหมด โดยผู้รับ 65 ใน 150 คน มีอีเมล์บ่งบอกถึงชื่อและสามารถระบุตัวตน ได้ จึงเป็นการเปิดเผยข้อมูลส่วนบุคคลโดย ทางอ้อมว่าบุคคล 65 คนนั้น ติดเชื้อ HIV

สำนักงานคุ้มครองข้อมูลส่วนบุคคลพิจารณา แล้วเห็นว่าสถาบันฯ บกพร่องที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่ดี โดยไม่มีการสร้างความตระหนักด้านความมั่นคงปลอดภัยให้กับพนักงานในการส่ง อีเมล์ให้คนจำนวนมาก จึงมีคำสั่งปรับสถาบันฯ เป็นเงินประมาณ 450,000 บาท



ภาพจาก Facebook Privacynote

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

(2) ป้องกันมิให้ผู้อื่นใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ

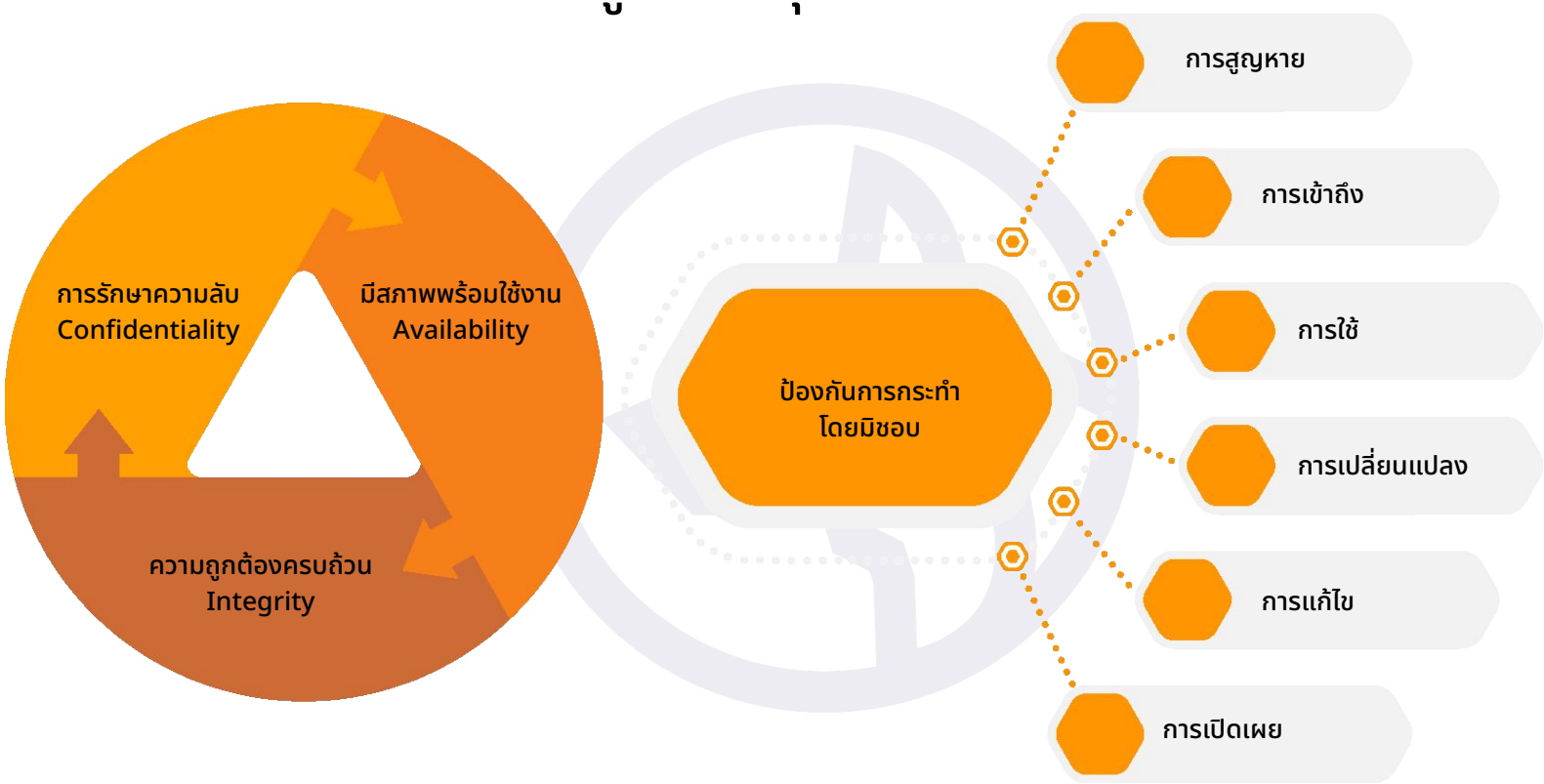
(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือ ทำลายข้อมูล

(4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ

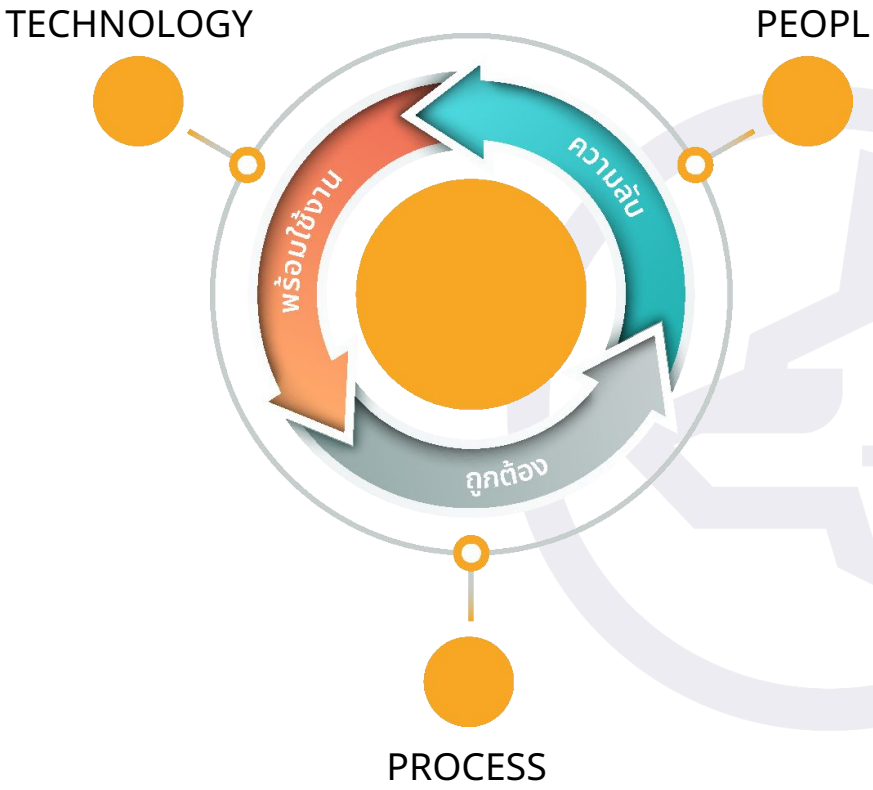
(5) แต่งตั้งตัวแทนในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ

(6) จัดทำบันทึกรายการ ตามมาตรา 39 (ROPA)

ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล



อ้างอิงจากหลักสูตร Workshop : PDPA - RoPA การจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล



PEOPLE = คนต้องมีความรู้

PROCESS = ต้องกำหนดขั้นตอน

TECHNOLOGY = หาอุปกรณ์มาสนับสนุน

อ้างอิงจากหลักสูตร Workshop : PDPA - RoPA การจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล

ความเสี่ยง
และความรับผิดใน PDPA

ความเสี่ยงและความรับผิดใน PDPA

DS เป็นผู้บังคับใช้

DS เป็นผู้บังคับใช้

สคส. เป็นผู้บังคับใช้

ความรับผิดตาม PDPA (ทางแพ่ง)

มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการ**ฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล** ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล **ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม** เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

1. ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้น การกระทำของเจ้าของข้อมูลนั้นเอง
2. เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ความรับผิดตาม PDPA (ทางแพ่ง)

มาตรา 78

ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล**จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้น จากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร** แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น

ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือ การที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

ตัวอย่างการคำนวนค่าสินไหมทดแทน ตามความรับผิดตาม PDPA (ทางแพ่ง)

ความรับผิดตาม PDPA (ทางอาญา)

มาตรา 79

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือ ได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุก ไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

ความรับผิดตาม PDPA (ทางอาญา)

POWERED BY SECURITY PiTCH Touchable Security

มาตรา 81

ในกรณีที่**ผู้กระทำ**ความผิดตามพระราชบัญญัตินี้เป็น**นิติบุคคล** ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของ **กรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น** หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการ หรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด **ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย**

ความรับผิดตาม PDPA (ทางอาญา)

มาตรา 80

ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น **ต้องระวาง โทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ**

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศ หรือ ต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

ความรับผิดตาม PDPA (ทางปกครอง)

ปรับ ไม่เกิน 1,000,000 ถึง 5,000,000 บาท

(เช่น การไม่จัดให้มีมาตรการรักษาความปลอดภัย การไม่แจ้งกรณี มีเหตุละเมิดข้อมูลส่วนบุคคล หรือการไม่ให้สำเนาข้อมูลส่วนบุคคล เป็นต้น)

เป็นความผิดแม้ไม่มีผู้เสียหาย/ความเสียหาย

กรณีศึกษา (ต่างประเทศ)

ภาพจาก
https://appsecco.com/blog/the-big-uber-hack-what-can-we-learn-from-the-incident

แฮกเกอร์เจาะเข้าระบบของแอปพลิเคชันบริการ “เรียกรถ” Uber ในปี 2016 และได้ข้อมูลของลูกค้าและคนขับรถ กว่า 57 ล้านรายไป อูเบอร์พยายามแก้ไขความผิดพลาดด้วยการจ่ายเงิน ให้กับแฮกเกอร์เป็นเงินกว่า **3,142 ล้านบาท** แลกกับการลบข้อมูล แต่ หน่วยงานกำกับดูแลข้อมูลของอเมริกาก็คงยังไม่ปลื้ม รัฐบาลกลาง สหรัฐฯ รวมตัวกับรัฐต่าง ๆ ส่งเรื่องขึ้น ศาล และสั่งฟ้องอูเบอร์เป็นเงินกว่า **4,638 ล้านบาท**

กรณีศึกษา (ต่างประเทศ)

ภาพจาก https://thenextweb.com/news/british-airways-website-hacked

สายการบิน British Airways ถูกหน่วยงานกำกับดูแลด้านข้อมูลของสหราชอาณาจักร (ICO) สั่งปรับเป็น เงินสูงถึง **7,218 ล้านบาท** โดย ICO ระบุว่าทางสายการบินมี “การจัดการ ด้านความมั่นคงปลอดภัยของข้อมูลที่หละหลวม” ซึ่งส่งผลให้ข้อมูลส่วน บุคคลของลูกค้ากว่า 5 แสนรายเสี่ยง ต่อการถูกละเมิดโดยแฮกเกอร์

ความรับผิดของลูกจ้าง

- โดยหลักการปฏิบัติหน้าที่ของลูกจ้างไม่ทำให้ลูกจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย PDPA ***แต่หากลูกจ้างทำเกินหรือนอกเหนือหน้าที่อาจทำให้ลูกจ้างกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลและมีความรับผิดตามกฎหมาย PDPA ได้***
- กรณีการปฏิบัติหน้าที่ของลูกจ้างทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเกิด ความรับผิดตามกฎหมาย PDPA ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการต่อลูกจ้าง ได้ดังต่อไปนี้
    - ดำเนินการทางวินัย : ลงโทษ หรือ เลิกจ้าง
    - ฟ้องร้องทางแพ่งเพื่อให้ลูกจ้างชดใช้ค่าเสียหายฐานผิด สัญญาจ้าง หรือกระทำละเมิด

Q & A
Thank You