ธนาคารแห่งประเทศไทย
BANK OF THAILAND

“PDPA Workshop
หลังบังคับใช้...อะไรที่ต้องยกระดับ”

วันศุกร์ที่ 9 ธันวาคม 2565 เวลา 09.00-12.30 น.

ณ อาคารอเนกประสงค์ ธนาคารแห่งประเทศไทย สำนักงานภาคเหนือ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

กำหนดการ

08:30-09:00 น. **ลงทะเบียน (พร้อมรับอาหารว่าง)**

09:00-09:10 น. **กล่าวเปิดงาน**

โดย คุณพรวิภา ตั้งเจริญมั่นคง ผอส. สำนักงานภาคเหนือ ธปท.

09:10-09:30 น. **ทำไมต้องเข้าใจ PDPA**

โดย คุณบุษกร ธีระปัญญาชัย ผอส. ฝ่ายนโยบายระบบการชำระเงิน ธปท.

09:30-10:00 น. **ไขข้อสงสัย...ยกระดับความเข้าใจ PDPA (ช่วง 1)**

- PDPA Recap โดย ทีมงานธนาคารแห่งประเทศไทย

10:00-12:30 น. **ไขข้อสงสัย...ยกระดับความเข้าใจ PDPA (ช่วง 2)**

- Workshop ความเข้าใจของผู้ปฏิบัติงาน (กิจกรรมกลุ่ม)
- ปัญหา อุปสรรคที่พบ และการแก้ไขหลัง PDPA บังคับใช้

โดย ทีมงานธนาคารแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

PDPA workshop

หลังบังคับใช้...อะไรที่ต้องยกระดับ

คุณพรวิภา ตั้งเจริญมั่นคง

ผู้อำนวยการอาวุโส สำนักงานภาคเหนือ ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ทำไมต้องเข้าใจ PDPA

PDPA workshop

หลังบังคับใช้...อะไรที่ต้องยกระดับ

คุณบุษกร ธีระปัญญาชัย

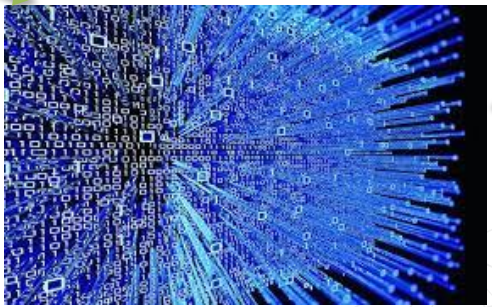
ผู้อำนวยการอาวุโส ฝ่ายนโยบายระบบการชำระเงิน ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

โลกดิจิทัล ....โลกของข้อมูล

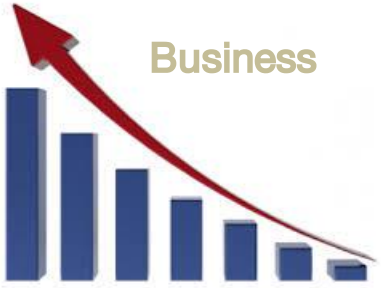
Internet & Technology

Data Flow



Data Usage

Business



ธนาคารแห่งประเทศไทย

ปรับ Mindset : ทำไมต้องมี PDPA

PDPA

- ให้ความสำคัญกับเจ้าของข้อมูล ให้สิทธิ ดูแล และ เยียวยา
- ให้มีการจัดการข้อมูลอย่างเป็นระบบ
- ป้องกันผู้ไม่ประสงค์ดี มาละเมิดเอาข้อมูลส่วนตัว ไปใช้ในทางที่ไม่ดี
- มีหน้าที่ความรับผิดชอบชัดเจน
- เป็นเรื่องของทุกคนในองค์กร ไม่ใช่ IT

ปี 2018 Facebook ส่งข้อมูลส่วนบุคคลของ User มากกว่า 50 ล้านคนให้บริษัท Cambridge Analytica ซึ่งเป็นบริษัทวิเคราะห์ความคิดเห็น ของประชาชนด้านการเมือง โดยที่ไม่ได้ขอความยินยอมจาก User

ผลตัดสิน ปี ค.ศ. 2019 ประเทศต่างๆ

- Federal Trade Commission ปรับ $5,000 ล้าน

- องค์กรคุ้มครองข้อมูลส่วนบุคคลของอิตาลีปรับ € 1 ล้าน

- องค์กรคุ้มครองข้อมูลส่วนบุคคลของอังกฤษปรับ Facebook £ 500,000

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ใครได้ประโยชน์จาก PDPA

ประชาชน

- ได้รับความคุ้มครองข้อมูลส่วนบุคคล
- สามารถร้องเรียนและได้รับการเยียวยาเมื่อถูกละเมิด

หน่วยงานรัฐ และเอกชน

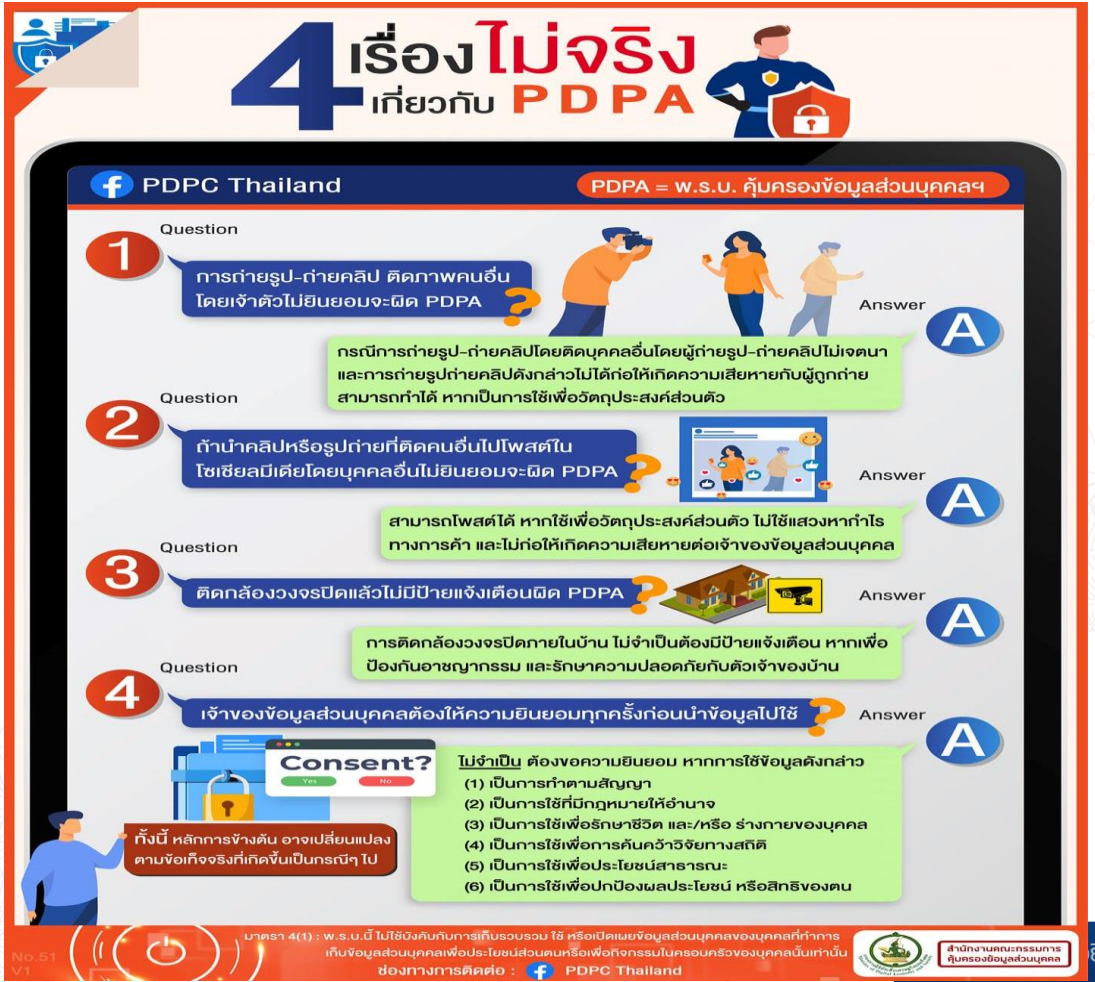
- มีมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล
- ส่งเสริมการดำเนินการและทำธุรกิจเกี่ยวกับข้อมูล
- สะดวกและลดค่าใช้จ่ายในการทำธุรกิจระหว่างประเทศ

ประเทศ

- ได้รับการยอมรับในระดับสากล
- มีกลไกและมาตรการในการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลจาก: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เรื่องไม่จริง!! เกี่ยวกับ PDPA



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ไขข้อสงสัย...ยกระดับความเข้าใจ PDPA

PDPA workshop

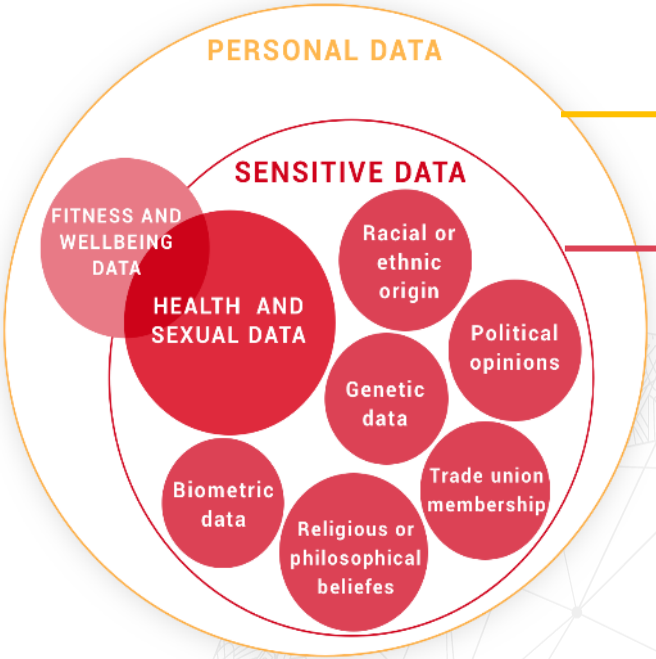
หลังบังคับใช้...อะไรที่ต้องยกระดับ

คุณวริศรา มั่นสกุล

รองผู้อำนวยการ ฝ่ายนโยบายระบบการชำระเงิน ธนาคารแห่งประเทศไทย

นิยาม “ข้อมูลส่วนบุคคล”

บุคคล = บุคคลธรรมดา



ข้อมูลส่วนบุคคล (Personal data)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลอ่อนไหว (Sensitive Personal Data)

ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

1 **Data Subject**

ให้ความยินยอม

2 **Data Controller**
Bank/ Non-bank

ทำข้อตกลงร่วมกัน

3 **Data Processor**
Bank/ Non-bank/ 3rd party

วัตถุประสงค์

ได้รับความคุ้มครองตามกฎหมาย สามารถตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลได้

มีกลไกการดูแลความมั่นคงปลอดภัยที่เหมาะสม ป้องกันการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผิดวัตถุประสงค์

มีมาตรฐานสำหรับการใช้อำนาจกฎหมายและเกณฑ์สำหรับภาคปฏิบัติ

Data Subject

เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคล

Data Controller
Bank/Non-bank

ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อาจเป็นเจ้าของธุรกิจหรือผู้ให้บริการ

Data Processor
Bank/ Non-bank/ 3rd party

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

Regulator

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีหน้าที่กำหนดมาตรการและออกแนวปฏิบัติ รวมทั้งวินิจฉัยข้อโต้แย้ง

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ข้อมูลส่วนบุคคลก่อน พ.ร.บ. มีผลบังคับใช้

ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้**เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ** ให้ผู้ควบคุมข้อมูลส่วนบุคคล**สามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม**

ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนด
วิธีการยกเลิกความยินยอม

เผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้
ผู้ควบคุมข้อมูลส่วนบุคคล เก็บรวบรวม และใช้ข้อมูลส่วนบุคคลดังกล่าว
สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอม (Consent) จากเจ้าของข้อมูลส่วนบุคคล

ยกเว้น

1. เพื่อการปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา (Contract)
2. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal Obligation)
3. เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)
4. เพื่อการปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public Task)
5. เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัย ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด (Research)
6. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal data) ต้องได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent) จากเจ้าของข้อมูลส่วนบุคคล

ยกเว้น

1. **เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)**
2. **การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน (Social Protection and Non-profit)**
3. **เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (Manifestly Made Public)**
4. **เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้อง หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย (Legal Claims)**
5. **เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ**
   - เวชศาสตร์ป้องกันหรืออาชีวศาสตร์
   - ประโยชน์สาธารณะด้านการสาธารณสุข
   - การคุ้มครองแรงงาน การประกันสังคม
   - การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ
   - ประโยชน์สาธารณะที่สำคัญ

การขอความยินยอม (Consent)

- **เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมไว้ก่อนหรือในขณะ**ที่เก็บรวบรวมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดผ่าน Privacy Notice
- **ต้องทำโดยชัดแจ้ง** เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์
- **แยกส่วนออกจากข้อความอื่น**อย่างชัดเจน **ข้อความเข้าใจง่าย ไม่หลอกลวง**ให้เข้าใจผิดในวัตถุประสงค์
- **คำนึงถึงความเป็นอิสระ**ของเจ้าของข้อมูล **ไม่มีเงื่อนไข**การให้ความยินยอมที่ไม่จำเป็นหรือเกี่ยวข้องกับการทำสัญญา
- เจ้าของข้อมูลส่วนบุคคล**ถอนความยินยอมได้โดยง่าย**

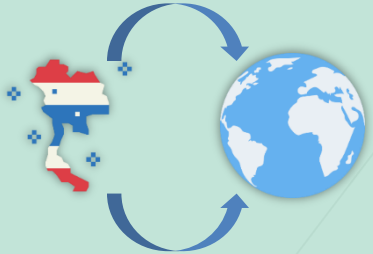
ประกาศความเป็นส่วนตัว (Privacy Notice)

รายละเอียดในการประมวลผลข้อมูลส่วนบุคคลที่ต้องแจ้งไว้ใน Privacy Notice

1. วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย
2. ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา
3. ข้อมูลส่วนบุคคลที่จะเก็บรวบรวม และระยะเวลาในการเก็บ
4. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลอาจถูกเปิดเผย
5. รายละเอียดการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล และ DPO
6. สิทธิของเจ้าของข้อมูลส่วนบุคคล

การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลเพียงพอ (Adequacy Decision)



คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะพิจารณาว่าประเทศปลายทางมีความคุ้มครองที่เพียงพอ

เข้าข้อยกเว้นตามกฎหมาย (Derogations for specific situations)

- ปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยแจ้งให้ทราบถึงมาตรฐานการคุ้มครองที่ไม่เพียงพอของประเทศปลายทาง
- การจำเป็นเพื่อปฏิบัติตามสัญญา (ก่อนเข้าทำสัญญานั้น)
- กระทำตามสัญญาระหว่างผู้ควบคุมข้อมูล เพื่อประโยชน์ของเจ้าของข้อมูล
- ป้องกัน/ระงับอันตรายต่อชีวิต
- ภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Binding Corporate Rules : BCRs)

เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน

ทั้งนี้ ต้องให้สำนักงานฯ (สคส.) ตรวจสอบและรับรอง

สิทธิของเจ้าของข้อมูลส่วนบุคคล

 สิทธิขอถอนความยินยอม (Right to withdraw consent)	 สิทธิขอเข้าถึง/ขอรับสำเนา/ ขอให้เปิดเผยถึงการได้มา (Right of access)	 สิทธิขอรับ ส่งหรือโอน ข้อมูลส่วนบุคคล (Right to data portability)	 สิทธิขอคัดค้านการประมวลผล (Right to restriction)
 สิทธิขอลบหรือทำลาย (Right to be forgotten)	 สิทธิขอให้ระงับการใช้ข้อมูล (Right to object)	 สิทธิขอให้ข้อมูล ส่วนบุคคลนั้นถูกต้อง (Right to rectification)	 สิทธิร้องเรียนต่อ คณะกรรมการผู้เชี่ยวชาญ (Right to complain)

การขอใช้สิทธิ (Data subject requests)

หน้าที่ดำเนินการตามคำร้อง ขอใช้สิทธิ ของเจ้าของข้อมูลส่วนบุคคล

1 ระยะเวลาดำเนินการ

กรณีคำร้องขอเข้าถึงและขอรับสำเนา ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ*

2 การให้เหตุผลในการปฏิเสธ

สิทธิแต่ละประเภทมีเงื่อนไขและองค์ประกอบของการใช้สิทธิที่แตกต่างกัน เช่น สิทธิในการขอรับสำเนา อาจปฏิเสธคำขอได้ในกรณีเป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล หรือการเข้าถึงหรือขอรับสำเนานั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น* เป็นต้น

3 กระบวนการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ควรกำหนดเป็นนโยบายโดยระบุขั้นตอนการดำเนินงานสำหรับจัดการและตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กรอบที่กฎหมายกำหนด ให้ชัดเจน

* ที่มา : มาตรา 30 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

6 ขั้นตอน พร้อมรับ DSRs

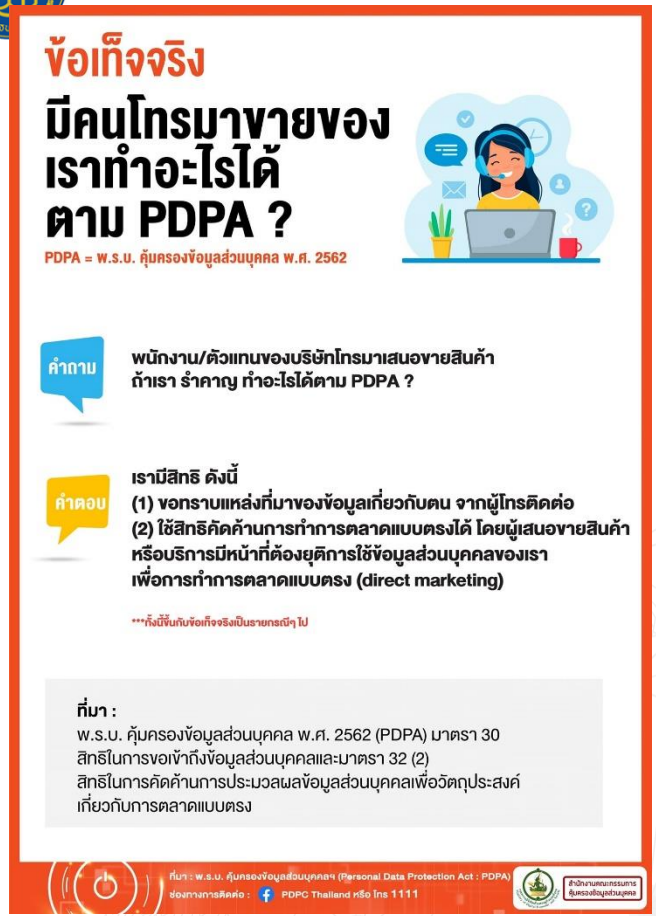
DSRs (Data Subject Requests)

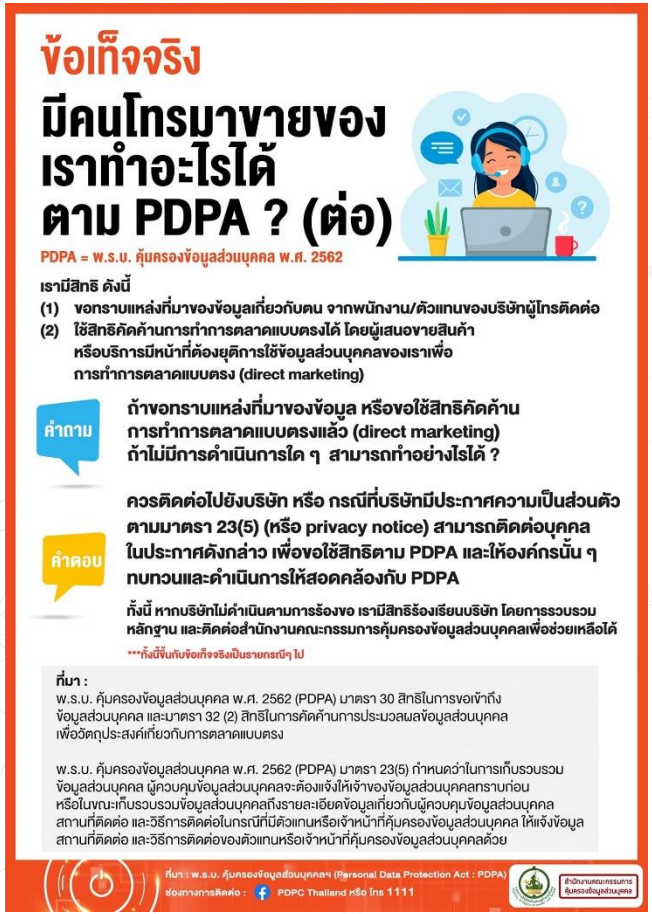
หมายเหตุ : กระบวนการนี้เป็นเพียงข้อแนะนำเท่านั้น องค์กรสามารถออกแบบกระบวนการเป็นอย่างอื่นให้สอดคล้องกับกฎหมายได้
: ปัจจุบันกรณีคำร้องขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลตามมาตรา 30 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลจาก: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

การขอใช้สิทธิ (Data subject requests)





ข้อมูลจาก: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

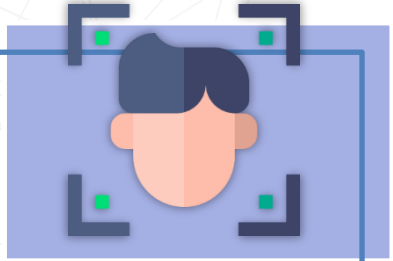
มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรการรักษามั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรการป้องกันด้านบริหารจัดการ

มาตรการป้องกันด้านเทคนิค



มาตรการป้องกันด้านกายภาพ

Identify

Detect

Protect

Response

Recovery

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"ความมั่นคงปลอดภัย" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

ธนาคารแห่งประเทศไทย

18 พฤศจิกายน 2562

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง

ที่ ฝนส.(01)ว. 125 /2562 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ธนาคารแห่งประเทศไทยขอนำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน ลงวันที่ 1 ตุลาคม 2562 ซึ่งได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 136 ตอนพิเศษ 280 ง ลงวันที่ 14 พฤศจิกายน 2562 แล้ว และมีผลบังคับใช้ตั้งแต่วันที่ 15 พฤศจิกายน 2562 เป็นต้นไป

สาระสำคัญของประกาศฉบับนี้ คือ สถาบันการเงินสามารถพิจารณาการนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีด้วยตนเอง เพื่อรองรับรูปแบบทางธุรกิจและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว โดย

1. ธนาคารพาณิชย์ที่มีนัยต่อความเสี่ยงเชิงระบบในประเทศ (Domestic Systemically Important Banks: D-SIBs) และสถาบันการเงินที่มีความเสี่ยงตั้งต้นทางไซเบอร์ (cyber inherent risk) ในระดับสูง ต้องมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
และหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงิน

แนวทางดำเนินการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

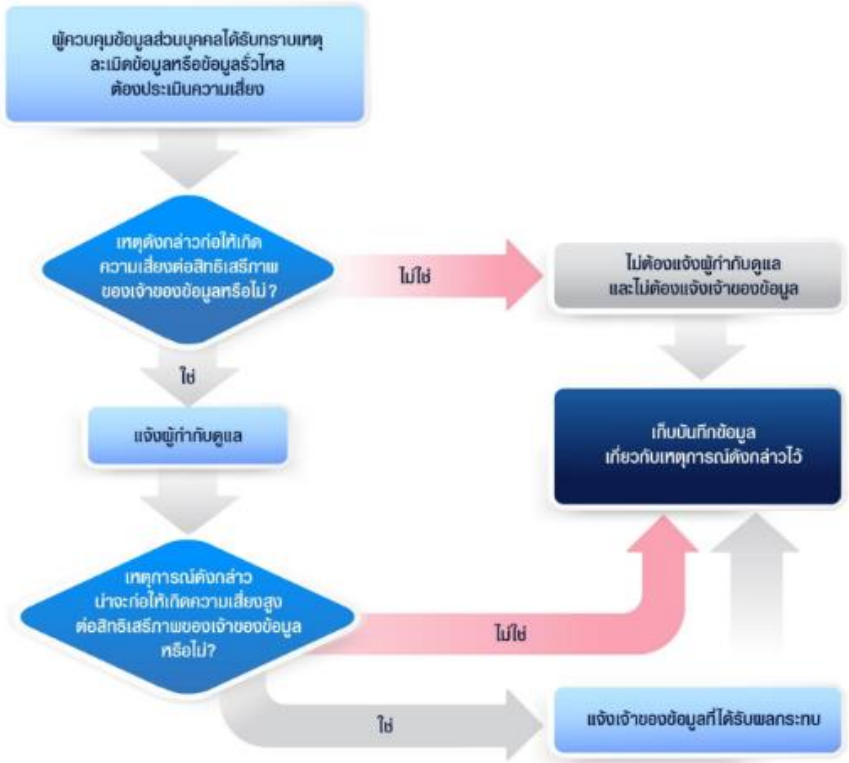
ต้องทำอย่างไร เมื่อมีการ ละเมิดข้อมูลส่วนบุคคล?

การแจ้ง \ ความเสี่ยง	ไม่มีความเสี่ยงฯ	มีความเสี่ยงฯ	มีความเสี่ยงสูงฯ
ไม่ต้องแจ้ง	✓	✗	✗
เจ้าของข้อมูลส่วนบุคคล	✗	✗	✓
สคส.	✗	✓	✓

- ความเสี่ยง : ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานฯ โดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เท่าที่จะสามารถกระทำได้
- แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ที่มา : มาตรา 37 (4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

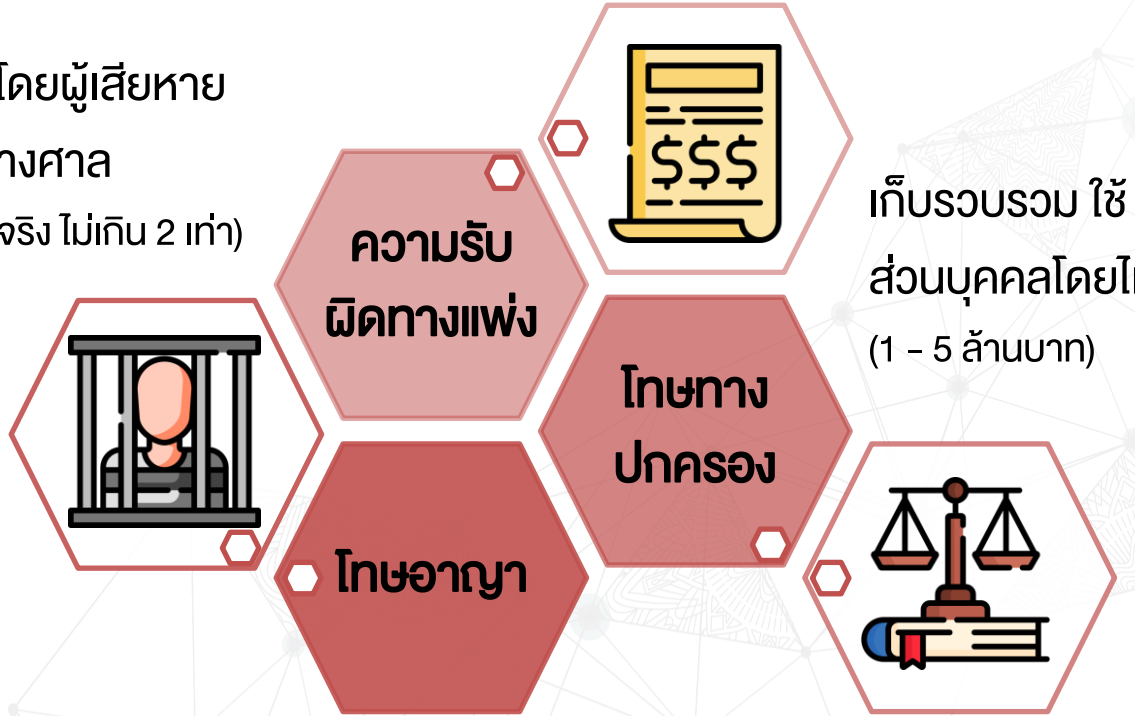
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



ข้อมูลจาก: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาฯ

ภาพรวมบทลงโทษ PDPA

เมื่อมีการเรียกร้องโดยผู้เสียหาย
ผ่านกระบวนการทางศาล
(ค่าสินไหมทดแทนตามจริง ไม่เกิน 2 เท่า)



เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
ส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
(1 – 5 ล้านบาท)

ทำให้เกิดการเสียชื่อเสียง ได้รับความอับอาย หรือลงโทษนิติบุคคล
(ผู้มีอำนาจ) ในการสั่งการหรือละเว้นสั่งการ
(โทษจำคุก 6 เดือน – 1 ปี หรือปรับ 5 แสน – 1 ล้านบาท หรือทั้งจำทั้งปรับ)

ความพร้อมด้านการกำกับดูแล: ความร่วมมือระหว่างหน่วยงานกำกับดูแลภาคการเงิน และ สคส.

วัตถุประสงค์:

เพื่อเป็นกรอบความร่วมมือระหว่างหน่วยงานกำกับดูแลในการกำกับดูแลการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล การแลกเปลี่ยนข้อมูล เพื่อประโยชน์ในการกำกับดูแล ตลอดจนร่วมกันสนับสนุนการสร้างความรู้และการพัฒนาบุคลากร

MOU's Key Deliverables

1. กำหนดขอบเขตและบทบาทหน้าที่ระหว่างกันให้ชัดเจน
2. ดูแลนโยบาย หลักเกณฑ์ และแนวทางกำกับดูแลให้สอดคล้อง
3. แลกเปลี่ยนข้อมูลที่เป็นประโยชน์ต่อการกำกับดูแล
4. สร้างความรู้และพัฒนาบุคลากรด้าน PDPA

ความพร้อมด้านการกำกับดูแล: การจัดการอบรมและแนวปฏิบัติของภาคการเงิน

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การดำเนินการเกี่ยวกับ PDPA ของสมาคมธนาคารไทย

PDPA workshop

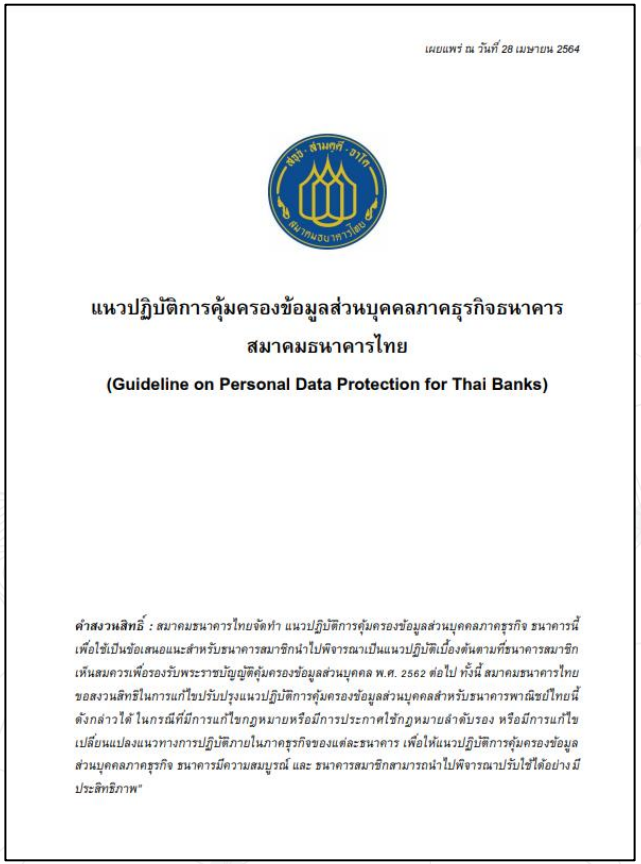
หลังบังคับใช้...อะไรที่ต้องยกระดับ

คุณรณน แก้วสุทธิ

ผู้ช่วยเลขาธิการ สมาคมธนาคารไทย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ความพร้อมด้านการกำกับดูแล: แนวปฏิบัติ PDPA ของภาคการเงิน



เผยแพร่ ณ วันที่ 28 เมษายน 2564

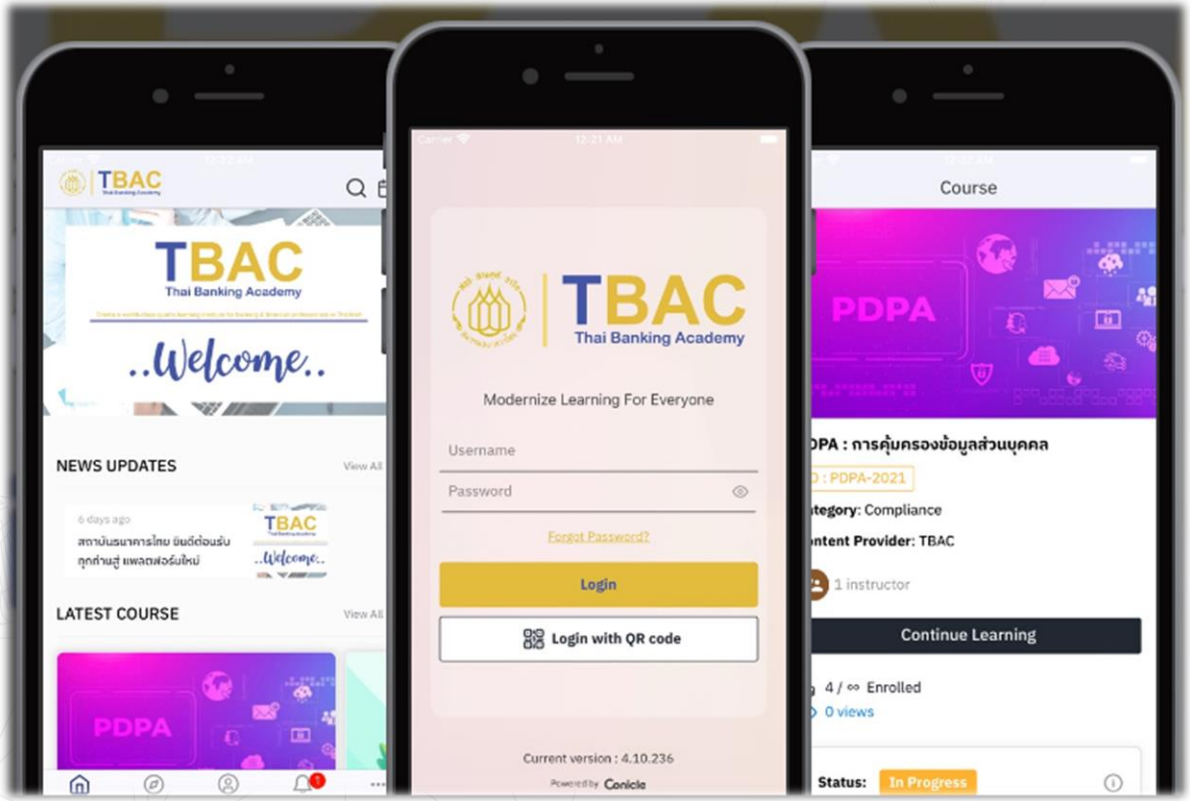
แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร
สมาคมธนาคารไทย
(Guideline on Personal Data Protection for Thai Banks)

คำสงวนสิทธิ์ : สมาคมธนาคารไทยจัดทำ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจ ธนาคารนี้ เพื่อใช้เป็นข้อเสนอแนะสำหรับธนาคารสมาชิกนำไปพิจารณาเป็นแนวปฏิบัติเบื้องต้นตามที่ธนาคารสมาชิกเห็นสมควรเพื่อรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไป ทั้งนี้ สมาคมธนาคารไทยขอสงวนสิทธิในการแก้ไขปรับปรุงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับธนาคารพาณิชย์ไทยนี้ดังกล่าวได้ ในกรณีที่มีการแก้ไขกฎหมายหรือมีการประกาศใช้กฎหมายลำดับรอง หรือมีการแก้ไขเปลี่ยนแปลงแนวทางการปฏิบัติภายในภาคธุรกิจของแต่ละธนาคาร เพื่อให้แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจ ธนาคารมีความสมบูรณ์ และ ธนาคารสมาชิกสามารถนำไปพิจารณาปรับใช้ได้อย่างมีประสิทธิภาพ"

TBAC

PDPA COURSE

PERSONAL DATA PROTECTION ACT



โครงสร้างหลักสูตร

EPISODE

1. บทนำ: การคุ้มครองข้อมูลส่วนบุคคล
2. ภาพรวมของ PDPA
3. ขอความยินยอมอย่างไรให้ถูกต้อง?
4. เหตุผลกรณีไม่ต้องขอความยินยอม
5. หลักการ และแนวปฏิบัติการประมวลผลข้อมูลส่วนบุคคล
6. การบริหารความเสี่ยง ‘ข้อมูลส่วนบุคคล’
7. บทลงโทษ และข้อปฏิบัติสำคัญเพื่อลดความเสี่ยง

การคุ้มครองสิทธิของเจ้าของข้อมูล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

WORKSHOP ความเข้าใจของผู้ปฏิบัติงาน

(กิจกรรมกลุ่ม)

PDPA workshop

หลังบังคับใช้...อะไรที่ต้องยกระดับ

คุณวีรชัย ชื่นชมพูนุท

ผู้ช่วยกรรมการผู้จัดการใหญ่

ธนาคารยูโอบี จำกัด (มหาชน)

คุณชนิดา พันธุ์เถกิงอมร

ผู้อำนวยการอาวุโส Data Protection Officer Office

ธนาคารยูโอบี จำกัด (มหาชน)

คุณอรชุมา ประชาศรัยสรเดช

ผู้ช่วยผู้อำนวยการ

ฝ่ายนโยบายระบบการชำระเงิน ธปท.

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

QR : Download กรณีศึกษาเกี่ยวกับ PDPA

Workshop : กรณีศึกษาเกี่ยวกับ PDPA

ลักษณะกิจกรรม

- ผู้เข้าอบรมแบ่งกลุ่ม**ประมาณ 10 คน** แต่ละกลุ่มวิเคราะห์กรณีศึกษาที่ต่างกัน **ใช้เวลา 20 นาที**
- **กรณีศึกษามีทั้งหมด 5 เรื่อง** ซึ่งเป็นสถานการณ์จำลองเพื่อวิเคราะห์ประเด็นที่ไม่เหมาะสม หรือไม่สอดคล้องตามหลักการ PDPA **แต่ละเรื่องมี 5 ประเด็นที่ต้องพิจารณา**
- ขอผู้แทนกลุ่มที่ได้กรณีศึกษาเดียวกัน นำเสนอความเห็นประเด็นที่ไม่สอดคล้องตาม PDPA
- สรุปและอธิบายการวิเคราะห์กรณีศึกษาโดยทีมงาน ธปท. และ TBA

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

1 กรณีศึกษาเกี่ยวกับ Privacy notice และ Consent form

1. privacy notice มีการแจ้งรายละเอียดการเก็บรวบรวม ใช้และเปิดเผยข้อมูลตามที่กฎหมายกำหนดครบถ้วนหรือไม่

2. การขอความยินยอมและการให้ถอนความยินยอมเป็นไปตามเงื่อนไขของกฎหมายหรือไม่

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

2 กรณีศึกษาเกี่ยวกับ การดำเนินการรองรับเหตุละเมิด

1. องค์กรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามข้อกำหนดของกฎหมายแล้วหรือไม่

2. องค์กรมีลักษณะเข้าข่ายที่จะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือไม่

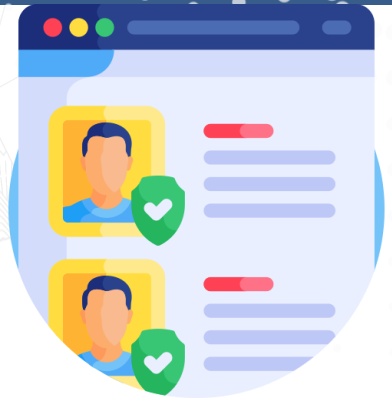
3. องค์กรจัดเตรียมกระบวนการจัดการเหตุละเมิดอย่างเหมาะสมแล้วหรือไม่

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

3 กรณีศึกษาเกี่ยวกับ การขอใช้สิทธิของเจ้าของข้อมูล

1. การดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดของกฎหมายหรือไม่

2. องค์กรมีการจัดเตรียมกระบวนการภายในเพื่อรองรับเมื่อเจ้าของข้อมูลมาขอใช้สิทธิตามกฎหมายหรือไม่



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 กรณีศึกษาเกี่ยวกับ การประมวลผลข้อมูลส่วนบุคคล

1. การปฏิบัติตามหลักเกณฑ์การจ้างผู้ประมวลผลข้อมูลส่วนบุคคล และหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายในกรณีศึกษานี้เหมาะสมหรือไม่

2. เมื่อลูกค้าถอนความยินยอมทางการตลาดแล้ว ธนาคารสามารถดำเนินการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นได้อีกหรือไม่

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5

กรณีศึกษาเกี่ยวกับ
การจัดการข้อมูลก่อน PDPA บังคับใช้ และมาตรการรักษาความปลอดภัยของข้อมูล

1. การประมวลผลข้อมูลส่วนบุคคลมีอยู่ก่อน PDPA บังคับใช้ตามกรณีศึกษานี้เหมาะสมหรือไม่

2. การแจ้งรายละเอียดให้เจ้าของข้อมูลทราบจะต้องทำเมื่อใด

3. การรักษาความปลอดภัยของข้อมูลตามกรณีศึกษานี้เหมาะสมหรือไม่ มีจุดใดบ้างที่ถือเป็นการละเมิดมาตรการรักษาความปลอดภัย

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

สรุปและอธิบายการวิเคราะห์กรณีศึกษา

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

1 กรณีศึกษาเกี่ยวกับ Privacy notice และ Consent form

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

1 กรณีศึกษาเกี่ยวกับ privacy notice และ consent form

privacy notice มีการแจ้งรายละเอียดการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลตามที่กฎหมายกำหนดครบถ้วนหรือไม่

2 หัวข้อนี้ไม่ได้ระบุในกรณีศึกษา

หัวข้อที่อยู่ใน privacy notice ของธนาคาร ABC

1. ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่ธนาคารจะเก็บรวบรวม ใช้ และเปิดเผย
2. วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล (ระบุวัตถุประสงค์ที่นำข้อมูลไปใช้ในรายละเอียด)
3. การเก็บรักษาข้อมูลส่วนบุคคลของท่าน และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล
4. การส่งข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศ
5. ระบบเว็บไซต์ที่ธนาคารใช้ในการเก็บรวบรวมข้อมูล
6. สิทธิของเจ้าของข้อมูลส่วนบุคคล
7. การเปลี่ยนแปลงหนังสือแจ้งการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้

การขอความยินยอม เป็นไปตาม PDPA หรือไม่ ?

หนังสือให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)

ธนาคาร ABC จำกัด (มหาชน) (“ธนาคาร”) มีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาท่านไปสู่ความปลอดภัยทางการเงินและยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด ธนาคารจึงได้จัดทำหนังสือขออนุญาตจากท่านในการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของท่าน ที่ท่านได้ให้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น เพื่อเก็บรวบรวมข้อมูลของคุณ ใช้ และเปิดเผยข้อมูลของคุณให้แก่ บริษัทในเครือธนาคาร ABC เพื่อการวิเคราะห์ การส่งเสริมการขาย หรือการประชาสัมพันธ์ผลิตภัณฑ์และบริการ รวมถึงสิทธิพิเศษที่เป็นประโยชน์ เพื่อเก็บรวบรวมข้อมูลชีวภาพของคุณ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ เพื่อการระบุและพิสูจน์ตัวตนทางอิเล็กทรอนิกส์ จากการสมัครหรือใช้ผลิตภัณฑ์หรือบริการของธนาคาร ABC เพื่อเก็บรวบรวม ใช้ และ/หรือ เปิดเผยข้อมูลของคุณเกี่ยวกับศาสนา ซึ่งปรากฏอยู่ในสำเนาหรือรูปถ่ายของบัตรประชาชนในขั้นตอนกระบวนการแสดง ระบุ ยืนยันและพิสูจน์ตัวตนต่อ ธนาคาร ABC เพื่อเปิดเผย ส่งหรือโอนข้อมูลของคุณไปยังต่างประเทศ รวมถึงเพื่อ เปิดเผยข้อมูลของคุณ เพื่อประโยชน์ในการทำวิจัยหรือการจัดทำข้อมูลสถิติ และเพื่อการดำเนินการอื่น ๆ

ท่านสามารถดูรายละเอียดเพิ่มเติมที่เผยแพร่ภายใต้ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) บนเว็บไซต์ของธนาคาร www.ABCbank.com ธนาคารจะทำการเก็บข้อมูล ส่วนบุคคลและการให้ความยินยอมของลูกค้าไว้ตามนโยบายของธนาคาร หากท่านประสงค์จะเพิกถอนความยินยอมนี้หรือทำการยื่นข้อร้องเรียนใดๆที่เกี่ยวกับการละเมิดสิทธิของท่าน สามารถดำเนินการผ่านทาง ABC Contact Center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของธนาคาร นอกจากนี้ท่านยังสามารถรายงานหรือยื่นข้อเรื่องร้องเรียนใดๆที่เกี่ยวข้องกับการละเมิดสิทธิของท่าน ได้ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ DPO@abcbank.com

วันที่.....**2 ธันวาคม 2565**.....
ชื่อ-นามสกุล..... **น.ส. สาม** .....
.....12345678xxxxx.....หนังสือเดินทางเลขที่ (กรณีคนต่างด้าว).....
☐ ยินยอม ☑ ไม่ยินยอม
ลงชื่อ ..... **น.ส. สาม** ..... เจ้าของข้อมูลส่วนบุคคล
(.....**น.ส. สาม**.....)

ไม่แยกวัตถุประสงค์ให้ชัดแจ้ง และขอความยินยอมแต่ละข้อแยกกันอย่างชัดเจน

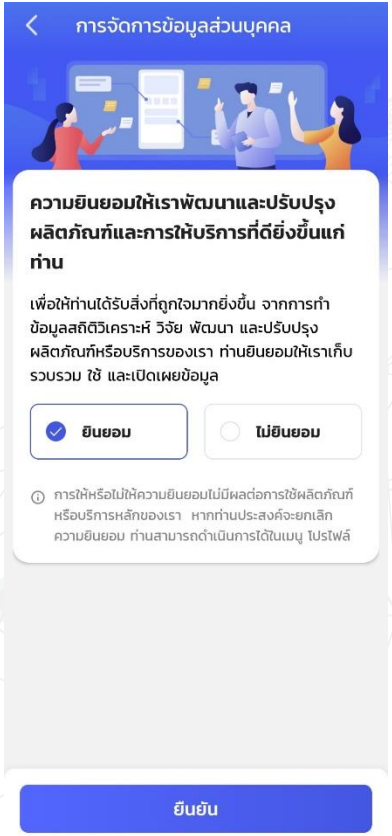
การขอความยินยอมเพื่อส่งข้อมูลไปยังต่างประเทศ ธนาคารจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางที่รับข้อมูลส่วนบุคคลด้วย

น.ส.สามเลือกว่าไม่ยินยอมให้ข้อมูลกับบริษัทในเครือธนาคาร ABC เพื่อเสนอขายผลิตภัณฑ์และบริการอื่น ดังนั้นธนาคารไม่ควรใช้ข้อมูลเพื่อเสนอขายผลิตภัณฑ์หรือบริการอีก

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ตัวอย่างการขอความยินยอม (Consent)



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การแจ้งวัตถุประสงค์และรายละเอียด

ในการเก็บรวบรวมข้อมูลส่วนบุคคล (Privacy notice) กรณีเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคล**โดยตรง**

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ**ก่อน**หรือ**ในขณะ**เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

1. วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย และ**ฐานทางกฎหมาย**ที่ทำให้สามารถเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลได้

2. แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคล**ต้องให้ข้อมูลส่วนบุคคล**เพื่อ**ปฏิบัติตามกฎหมาย** หรือ **สัญญา** หรือ มีความจำเป็นต้องให้ข้อมูลส่วนบุคคล**เพื่อเข้าทำสัญญา** รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

3. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

4. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนด**ระยะเวลาที่อาจคาดหมายได้**ตามมาตรฐานของการเก็บรวบรวม

5. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

6. ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล

7. ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)

8. ข้อมูล ชื่อ และรายละเอียด รวมถึงสถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)

9. รายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

10. สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

รายการข้างต้นเป็นแนวทางการดำเนินการเพื่อประโยชน์ในการปรับใช้และปฏิบัติให้ถูกต้องสอดคล้องตามมาตรา 23 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ที่มา : แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.70
V0.3

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

2 กรณีศึกษาเกี่ยวกับ
การดำเนินการรองรับเหตุละเมิด

2 กรณีศึกษาเกี่ยวกับ **การดำเนินการรองรับเหตุละเมิด**

นายหนึ่งเป็นลูกค้าประจำที่ชอบซื้อของผ่าน e-Commerce application ของบริษัท 123 ช้อปปิ้ง จำกัด ซึ่งเป็นบริษัทที่ได้รับความนิยมเป็นอันดับ 1 ในประเทศ มีลูกค้ากว่า 1 ล้านราย เหตุเพราะ application ของบริษัทใช้งานง่าย สามารถบันทึกข้อมูลบัตรเครดิตหรือบัญชีธนาคารไว้บน application ได้ ไม่ต้องกรอกข้อมูลซ้ำทุกครั้งที่ซื้อสินค้า วันที่ 15 พฤศจิกายน 2565 พนักงานของบริษัท 123 ช้อปปิ้งพบธุรกรรมซื้อสินค้าผ่าน application ที่ค่อนข้างผิดปกติ มียอดชำระเงินของลูกค้าหลายรายรวมถึงนายหนึ่ง ที่ถูกตัดเงินจากบัตรเครดิตที่ผูกไว้เป็นมูลค่าเท่ากันหลายครั้งในเวลาไล่เลี่ยกัน จึง cap screen ข้อมูลส่วนบุคคลของลูกค้ารวมถึงธุรกรรมชำระเงินที่ผิดปกติส่งใน LINE กลุ่มให้เพื่อนพนักงานที่อยู่แผนก IT ช่วยตรวจสอบให้ รวมถึงแจ้งไปยัง CEO ของบริษัทเพื่อรับทราบเหตุการณ์ดังกล่าว เนื่องจากบริษัทยังไม่มีการแต่งตั้ง DPO ซึ่ง CEO ได้สั่งการให้ฝ่าย IT หาข้อมูลและจุดรั่วไหลของข้อมูลอย่างเร่งด่วน

มีกระบวนการภายในของบริษัทที่เหมาะสมหรือไม่ ?

- ส่งข้อมูลส่วนบุคคลผ่าน LINE ไม่สอดคล้องตามมาตรการรักษาความปลอดภัยข้อมูล และเป็นการเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ
- บริษัทยังไม่มีการแต่งตั้ง DPO รับผิดชอบเรื่องข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

DPO คือใคร

DPO (Data Protection Officer)
คือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ตามมาตรา 42 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สแกน

พ.ร.บ. คุ้มครองข้อมูล
ส่วนบุคคล พ.ศ. 2562

มีหน้าที่ ดังนี้

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตาม พ.ร.บ. นี้

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

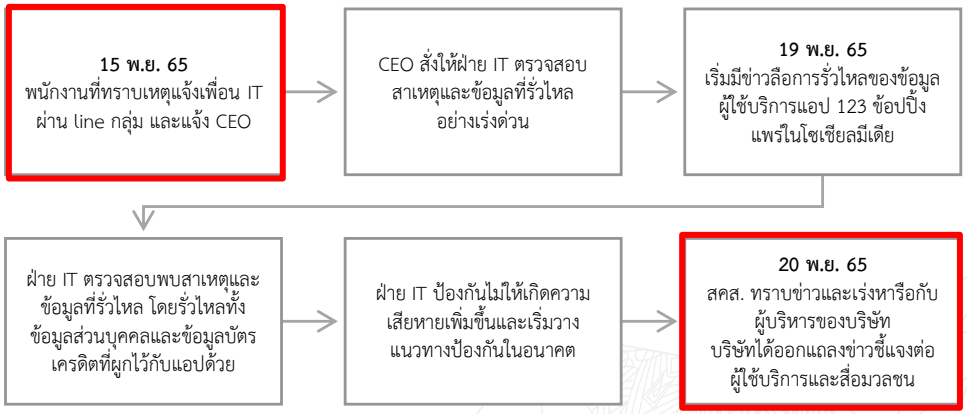
ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.07
V2

2 กรณีศึกษาเกี่ยวกับ **การดำเนินการรองรับเหตุละเมิด**



จาก flow ที่บริษัทดำเนินการ เหมาะสมแล้วหรือไม่ มีอะไรที่ต้องทำเพิ่มเติมบ้าง?

บริษัทยังขาดขั้นตอนการประเมินความเสี่ยงที่จะกระทบต่อลูกค้า

การแจ้งเหตุละเมิดอยู่ในเวลาที่กำหนดหรือไม่

เหตุละเมิดต้องรีบแจ้งภายใน 72 ชั่วโมง
วันที่ 15-20 พ.ย. เกิน 72 ชม. แล้ว

20 พฤศจิกายน 2565

หนังสือชี้แจง
กรณีข่าวการรั่วไหลของข้อมูลผู้ใช้บริการแอปพลิเคชัน 123 ช้อปปิ้ง

ตามที่มีการรายงานข่าวการรั่วไหลของข้อมูลผู้ใช้บริการแอปพลิเคชันของบริษัท 123 ช้อปปิ้ง จำกัด (บริษัทฯ) ส่งผลกระทบต่อผู้ใช้บริการมากกว่า 1 ล้านราย ปรากฏในข่าวลือในโซเชียลมีเดียหลายช่องทางในช่วงหลายวันที่ผ่านมา ขอเรียนชี้แจงว่า บริษัทฯ ได้ทำการตรวจสอบสาเหตุแล้วพบว่า ข่าวการรั่วไหลข้อมูลของผู้ใช้บริการกว่า 1 ล้านรายไม่เป็นความจริง อย่างไรก็ดี มีการรั่วไหลของข้อมูลผู้ใช้บริการเพียงบางส่วนจริงแต่ไม่เกิน 1,000 ราย ซึ่งคิดเป็น 0.1% เทียบกับฐานข้อมูลผู้ใช้บริการทั้งหมดของบริษัท ซึ่งบริษัทได้ดำเนินการแก้ไขและป้องกันไม่ให้เกิดความเสียหายมากกว่าที่ปรากฏในข่าว พร้อมทั้งประสานแจ้งหน่วยงานที่เกี่ยวข้องรับทราบเรียบร้อยแล้ว

ทั้งนี้ ขอยืนยันว่าบริษัทฯ ให้ความสำคัญในการป้องกันข้อมูลและความเป็นส่วนตัวของลูกค้าเป็นสำคัญ และจะเร่งดำเนินการวางแนวทางป้องกันที่รัดกุม เพื่อป้องกันเหตุการณ์ดังกล่าวในอนาคต เพื่อรักษาความเชื่อมั่นของการใช้บริการของบริษัทฯ ต่อไป

กรณีต้องการทราบข้อมูลเพิ่มเติม กรุณาติดต่อ

ฝ่ายประชาสัมพันธ์ บริษัท 123 ช้อปปิ้ง จำกัด
โทรศัพท์ 02-123-xxxx

จากหนังสือชี้แจง เหมาะสมแล้วหรือไม่ ยังขาดข้อมูลอะไรบ้างไหม ?

เหตุการณ์ที่เกิดขึ้นเป็นกรณีเสี่ยงสูง บริษัทไม่แจ้งแนวทางเยียวยาแก่เจ้าของข้อมูลส่วนบุคคล และไม่ได้แนะนำแนวทางป้องให้แก่ตัวลูกค้าผู้ใช้บริการ เช่น ให้ตั้งค่า password ใหม่ หรือเปลี่ยนข้อมูลบัตรที่ผูกไว้

หนังสือชี้แจงควรระบุข้อมูลต่อไปนี้ด้วย

- ประเภทและรายละเอียดข้อมูลที่รั่วไหล
- รายละเอียดและช่องทางการติดต่อ DPO

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เมื่อเกิดเหตุ การละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ควรทำอย่างไร?

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล เช่น เหตุที่ส่งผลกระทบต่อมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล เป็นต้น

ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่...

แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่...

แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

หมายเหตุ
ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ที่มา : มาตรา 37 (4) และ มาตรา 40 (2) พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.25
V2

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ต้องทำอย่างไร เมื่อมีการ ละเมิดข้อมูลส่วนบุคคล?

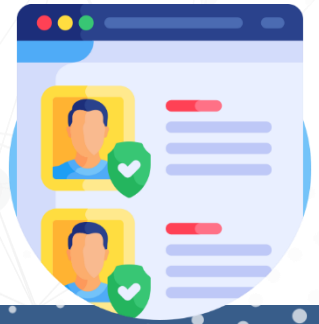
การแจ้ง \ ความเสี่ยง	ไม่มีความเสี่ยงฯ	มีความเสี่ยงฯ	มีความเสี่ยงสูงฯ
ไม่ต้องแจ้ง	✓	✗	✗
เจ้าของข้อมูลส่วนบุคคล	✗	✗	✓
สคส.	✗	✓	✓

- ความเสี่ยง : ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานฯ โดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เท่าที่จะสามารถกระทำได้
- แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ที่มา : มาตรา 37 (4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND



3 กรณีศึกษาเกี่ยวกับ
การขอใช้สิทธิของเจ้าของข้อมูล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

3 กรณีศึกษาเกี่ยวกับ **การขอใช้สิทธิของเจ้าของข้อมูล**

วันที่ 1 มิถุนายน 2565 ที่ผ่านมา นายสองได้ยินข่าวเกี่ยวกับการบังคับใช้ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งให้สิทธิเจ้าของข้อมูลในเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่จัดเก็บไว้และยกเลิกความยินยอมการใช้ข้อมูลส่วนบุคคลได้ จึงเดินทางไปที่ธนาคาร DEF สาขาหนึ่ง เพื่อขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนที่ธนาคาร DEF จัดเก็บไว้ เพื่อนำมาพิจารณาก่อนว่าธนาคารจัดเก็บข้อมูลอะไรบ้างก่อนที่จะทำการยกเลิกความยินยอม โดยธนาคารให้นายสองกรอกแบบฟอร์มแสดงความจำนงค์ขอใช้สิทธิเข้าถึงข้อมูลไว้ และจะติดต่อนายสองอีกครั้งเมื่อเอกสารข้อมูลดังกล่าวเสร็จสมบูรณ์

นายสองได้ติดตามการขอเข้าถึงข้อมูลส่วนบุคคลอย่างต่อเนื่อง แต่พนักงานแจ้งว่าเรื่องดังกล่าวอยู่ระหว่างดำเนินการ จนเวลาผ่านไปถึงวันที่ 4 กรกฎาคม 2565 ธนาคาร DEF ยังไม่ส่งรายละเอียดข้อมูลส่วนบุคคลของนายสองที่ธนาคารจัดเก็บไว้ให้สักที นายสองจึงเดินทางไปที่สาขาธนาคารอีกครั้ง เพื่อขอใช้สิทธิยกเลิกความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์ทางการตลาด แต่พนักงานสาขาดังกล่าวแจ้งว่า การยกเลิกความยินยอมสามารถทำได้เมื่อผ่านไป 180 วันนับจากวันที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ

การใช้เวลาดำเนินการตามคำขอใช้สิทธิเข้าถึงข้อมูลของลูกค้าเหมาะสมหรือไม่

ธนาคารต้องดำเนินการตามคำขอใช้สิทธิเข้าถึงข้อมูลโดยไม่ชักช้า และไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ วันที่ 1 มิ.ย.–4 ก.ค. เกิน 30 วันแล้ว

การมีระยะเวลารอเพื่อใช้สิทธิถอนความยินยอม ถูกต้องแล้วหรือไม่

เจ้าของข้อมูลมีสิทธิถอนความยินยอมเมื่อไหร่ก็ได้

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

3 กรณีศึกษาเกี่ยวกับ **การขอใช้สิทธิของเจ้าของข้อมูล**

แบบฟอร์มคำขอใช้สิทธิถอนความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)	
วันที่.....4 มกราคม 2566.....	
ชื่อ-นามสกุล..... นายสอง	
เลขประจำตัวประชาชน.....12345678xxxxx.....หนังสือเดินทางเลขที่ (กรณีคนต่างด้าว).....	
มีความประสงค์ขอใช้สิทธิถอนความยินยอมเกี่ยวกับข้อมูล ดังต่อไปนี้	
ส่วนที่ 1 การถอนความยินยอมเพื่อวัตถุประสงค์ทางการตลาด	ถอนความยินยอม
1.1 ถอนความยินยอมให้ ธนาคาร DEF เก็บรวบรวมข้อมูลของคุณ ใช้ และเปิดเผยข้อมูลของคุณให้แก่ บริษัทในเครือธนาคาร DEF เพื่อการวิเคราะห์ การส่งเสริมการขาย หรือการประชาสัมพันธ์ผลิตภัณฑ์และบริการ รวมถึงสิทธิพิเศษที่เป็นประโยชน์	☑
1.2 ถอนความยินยอมให้ ธนาคาร DEF เก็บรวบรวมข้อมูลของคุณ ใช้ และเปิดเผยข้อมูลของคุณให้แก่พันธมิตรของธนาคาร DEF รวมทั้งยินยอมให้ผู้รับข้อมูลดังกล่าว เก็บรวบรวมและใช้ข้อมูลของคุณ เพื่อการวิเคราะห์ การส่งเสริมการขาย หรือการประชาสัมพันธ์ผลิตภัณฑ์และบริการ รวมถึงสิทธิพิเศษที่เป็นประโยชน์	☑
ส่วนที่ 2 การถอนความยินยอมเพื่อวัตถุประสงค์อื่นที่ไม่ใช่ทางการตลาด	ถอนความยินยอม
2.1 ถอนความยินยอมให้ ธนาคาร DEF เก็บรวบรวมข้อมูลชีวภาพของคุณ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ เพื่อการระบุและพิสูจน์ตัวตนทางอิเล็กทรอนิกส์ จากการสมัครหรือใช้ผลิตภัณฑ์หรือบริการของธนาคาร DEF	☑
2.2 ถอนความยินยอมให้ ธนาคาร DEF เก็บรวบรวม ใช้ และ/หรือ เปิดเผยข้อมูลของคุณเกี่ยวกับศาสนา ซึ่งปรากฏอยู่ในสำเนาหรือรูปถ่ายของบัตรประชาชนในขั้นตอนกระบวนการแสดง ระบุ ยืนยันและพิสูจน์ตัวตนต่อธนาคาร DEF	☑
2.3 ถอนความยินยอมให้ ธนาคาร DEF เปิดเผย ส่งหรือโอนข้อมูลของคุณไปยังต่างประเทศ	☑
2.4 ถอนความยินยอมให้ ธนาคาร DEF เปิดเผยข้อมูลของคุณเพื่อประโยชน์ในการทำวิจัยหรือการจัดทำข้อมูลสถิติ	☑
ข้าพเจ้าให้ความยินยอมในการถอนความยินยอมตามที่ระบุข้างต้น	
ลงชื่อ .....นายสอง..... เจ้าของข้อมูลส่วนบุคคล (.....นายสอง.....)	

ธนาคารมีกระบวนการภายในรองรับการจัดการถอนความยินยอมที่เหมาะสมแล้วหรือไม่ ?
หากไม่เหมาะสม มีประเด็นใดบ้าง ?

นายสองไม่ให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลเพื่อวัตถุประสงค์ทางการตลาดแล้ว
แต่ยังได้รับข้อเสนอจากธนาคาร แสดงว่าไม่ได้มีการเพิกถอนความยินยอมทั้งหมด

ไม่แจ้งผลกระทบจากการขอถอนความยินยอมให้ชัดเจน

3 กรณีศึกษาเกี่ยวกับ **การขอใช้สิทธิของเจ้าของข้อมูล**

ผ่านไป 2 เดือน นายสองได้รับโทรศัพท์จากพนักงาน DEF อีกครั้งแจ้งว่านายสองเป็นลูกค้าชั้นดีของธนาคาร จึงขอเสนอบริการทำประกันภัยกับบริษัทในเครือด้วยค่าเบี้ยทำประกันอัตราที่ถูกกว่าอัตราปกติ แต่นายสองทำประกันกับบริษัทประกันอื่นไว้แล้ว จึงปฏิเสธข้อเสนอดังกล่าว ต่อมานายสองได้รับการติดต่อขอยืมเงินจากเพื่อนสมัยประถมรายหนึ่ง ซึ่งเพื่อนรายดังกล่าวทำงานในแผนกจัดซื้อของธนาคาร DEF และเห็นข้อมูลยอดเงินบัญชีเงินฝากของนายสองจากฐานข้อมูลลูกค้าธนาคาร จากเหตุการณ์ต่าง ๆ ที่ผ่านมา ทำให้นายสองรู้สึกไม่พอใจกับการดำเนินการและการแก้ไขปัญหาของธนาคาร DEF จึงไปถอนเงินทั้งหมดออกบัญชีและย้ายไปใช้บริการธนาคารอื่นแทน

ตัวอย่างสถานการณ์ที่ยกมา ยังมีกรณีใดที่ธนาคารดำเนินการไม่เหมาะสมอีกหรือไม่

ผู้ไม่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

แนวทางในการดำเนินการขอความยินยอม

มีการขอความยินยอมก่อน หรือในขณะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์และรายละเอียดของการขอความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ (informed) ก่อนจะให้ความยินยอม

การให้ความยินยอมต้องไม่มีลักษณะที่เป็นเงื่อนไขที่บังคับก่อนการเข้าทำสัญญาหรือการให้บริการใด ๆ ที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาหรือการให้บริการนั้น ๆ

ต้องระบุวัตถุประสงค์ในการให้ความยินยอมอย่างเฉพาะเจาะจง (specific) ไม่ใช่ระบุวัตถุประสงค์อย่างกว้าง ๆ เป็นการทั่วไป

เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยสมัครใจและอิสระ (freely given) โดยปราศจากกลฉ้อฉล หลอกลวง ข่มขู่ หรือสำคัญผิด

ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์

เนื่องจากความยินยอมมีเงื่อนไขหลายประการที่ต้องปฏิบัติให้สอดคล้องตามมาตรา 19 ดังนั้น จึงควรพิจารณาเลือกใช้ความยินยอมเป็นฐานทางกฎหมายสุดท้าย

ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ หากมีฐานทางกฎหมาย (Lawful Basis) ตามมาตรา 24 หรือมาตรา 26

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.64
V0.2

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล ที่เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล

ใครขอใช้สิทธิได้บ้าง

1. เจ้าของข้อมูลส่วนบุคคล
2. ผู้มีอำนาจกระทำการแทนตามกฎหมาย
3. ผู้มีอำนาจกระทำการแทนผู้เยาว์ / คนไร้ความสามารถ / คนเสมือนไร้ความสามารถ ตามมาตรา 20

ขออะไรได้บ้าง

1. ขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน
2. ขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน
3. ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าว ที่ตนไม่ได้ให้ความยินยอม

ขอที่ใคร

ยื่นคำขอได้ที่ผู้ควบคุมข้อมูลส่วนบุคคล

การดำเนินการตามคำขอ

ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ

ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอได้ เมื่อ...

1. เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล
2. การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคล
ต้องบันทึกการปฏิเสธคำขอดังกล่าว
พร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 39

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 30

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.78
V0.1

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 กรณีศึกษาเกี่ยวกับ
การประมวลผลข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 กรณีศึกษาเกี่ยวกับ **การประมวลผลข้อมูลส่วนบุคคล**

เนื่องจากการเติบโตอย่างต่อเนื่องของการธนาคารดิจิทัล (digital banking) ธนาคาร JKL จึงมีการเพิ่มช่องทางการขอสินเชื่อเพื่อเพิ่มความสะดวกรวดเร็วให้แก่ลูกค้าได้มากขึ้น โดยลูกค้าสามารถขอสินเชื่อผ่านทางร้านสะดวกซื้อทั่วไปได้

ในการนี้ ธนาคาร JKL ได้ไปติดต่อร้านสะดวกซื้อเพื่อดำเนินการรับคำขอของลูกค้าดังกล่าว โดยร้านสะดวกซื้อจะทำหน้าที่รับคำขอของลูกค้าโดยจัดการให้ลูกค้ากรอกแบบฟอร์มการขอสินเชื่อของธนาคาร JKL สแกนแบบฟอร์มและเอกสารที่เกี่ยวข้องของลูกค้าเข้าระบบของร้านสะดวกซื้อไว้เป็นหลักฐานเพื่อให้ธนาคาร JKL สามารถตรวจสอบได้ แล้วจึงนำส่งเอกสารตัวจริงให้แก่ธนาคาร JKL เพื่อให้ธนาคาร JKL ทำการพิจารณาตามขั้นตอนปกติต่อไป แต่ธนาคารยังไม่ได้มีการทำสัญญากับร้านสะดวกซื้ออย่างเป็นทางการ

นางสาวสวยเป็นลูกค้าบัญชีเงินฝากของธนาคาร JKL และมีอาชีพขายของออนไลน์ มีความต้องการขยายธุรกิจ เมื่อเห็นป้ายโฆษณาในร้านสะดวกซื้อ จึงสนใจอยากจะขอสินเชื่อกับธนาคาร JKL นางสาวสวยจึงได้จัดการกรอกแบบฟอร์มการขอสินเชื่อและนำส่งเอกสารที่เกี่ยวข้อง ซึ่งรวมถึงสำเนาบัตรประชาชนรุ่นเก่าที่มีข้อมูลศาสนา สำเนาทะเบียนบ้าน และรายการเดินบัญชีที่ใช้รับเงินค่าขายของออนไลน์ ให้แก่ร้านสะดวกซื้อ โดยพนักงานร้านสะดวกซื้อเห็นรายรับแต่ละเดือนของนางสาวสวยค่อนข้างต่ำมาก พนักงานจึงคิดเองว่านางสาวสวยอาจจะไม่สามารถจ่ายคืนได้ จึงได้แจ้งปฏิเสธการขอสินเชื่อให้นางสาวสวยทราบ แต่ก็ได้เก็บรวบรวมแบบฟอร์มการขอสินเชื่อ แบบฟอร์มขอความยินยอม สำเนาบัตรประชาชน สำเนาทะเบียนบ้าน และรายการเดินบัญชีที่นางสาวสวยส่งให้ สแกนเอกสารเข้าเครื่องคอมพิวเตอร์ทันทีโดยไม่ได้ตรวจสอบข้อมูลในสำเนาที่ขอจากนางสาวสวย และนำเอกสารตัวจริงใส่แฟ้มเพื่อจัดส่งให้ธนาคาร JKL ต่อไป

จากตัวอย่างสถานการณ์ที่ยกมานี้
ใครเป็น**ผู้ประมวลผลข้อมูล** ?
และมีจุดที่ดำเนินการไม่เหมาะสมหรือไม่ ?

ร้านสะดวกซื้อมีสถานะเป็นผู้ประมวลผลข้อมูล
ดังนั้น ธนาคารจะต้องทำสัญญาประมวลผลข้อมูลส่วนบุคคลกับร้านสะดวกซื้อด้วย

พนักงานร้านสะดวกซื้อไม่มีสิทธิปฏิเสธการให้สินเชื่อ เนื่องจากเป็นเพียงผู้ประมวลผลตามคำสั่งธนาคาร

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ใครเป็นใครใน PDPA

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ประชาชนทุกคน
หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsource ด้วย
กล่าวอีกนัยคือเป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมถึงคนตายและนิติบุคคล
*ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

หน่วยงาน / องค์กร / สถาบัน ที่กำหนดวัตถุประสงค์
วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล
บุคคลธรรมดาก็อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
โดยหลักคือ Outsource ที่รับจ้าง
*ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน / องค์กร / สถาบัน

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ
หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ
หน่วยงาน / องค์กร / สถาบัน ให้เป็นไปตามกฎหมาย

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

หน้าที่ ผู้ประมวลผลข้อมูลส่วนบุคคล

Responsibilities of a Data Processor

กฎหมายกำหนดหน้าที่เฉพาะสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 มาตรา 40 ดังนี้

1. ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. นี้

2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

3. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

4. จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเฉพาะเมื่อเข้าเงื่อนไขที่มาตรา 41 กำหนด

หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตาม ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ข้อตกลงการประมวลผล หรือ DPA คืออะไร?

ข้อตกลงการประมวลผล หรือ Data Processing Agreement (DPA)

คือข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบด้วยเงื่อนไขอย่างน้อยดังต่อไปนี้

1 ต้องมีข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

3 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

4 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อกำหนดทั้ง 4 ข้อเป็นกรอบเงื่อนไขเบื้องต้นที่ควรกำหนดไว้ ซึ่งรายละเอียดของข้อสัญญาและข้อตกลงอื่นๆ เป็นเรื่องที่คู่สัญญาควรตกลงกันให้สอดคล้องกับกิจกรรมการประมวลผลและความเสี่ยงที่เกี่ยวข้องกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ที่มา : มาตรา 40 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.21
V2

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

4 กรณีศึกษาเกี่ยวกับ **การประมวลผลข้อมูลส่วนบุคคล**

จากสถานการณ์ที่ยกมา มีจุดที่ไม่เหมาะสมอีกหรือไม่ ?

...แต่ก็ได้เก็บรวบรวมแบบฟอร์มการขอสินเชื่อ แบบฟอร์มขอความยินยอม สำเนาบัตรประชาชน สำเนาทะเบียนบ้าน และรายการเดินบัญชีที่นางสาวสวยส่งให้ สแกนเอกสารเข้าเครื่องคอมพิวเตอร์ทันทีโดยไม่ได้ตรวจสอบข้อมูลในสำเนาที่ขอจากนางสาวสวย และนำเอกสารตัวจริงใส่แฟ้มเพื่อจัดส่งให้ธนาคาร JKL ต่อไป

หนึ่งสัปดาห์ต่อมา ธนาคาร JKL อนุมัติสินเชื่อให้แก่นางสาวสวย จึงมีจดหมายแจ้งอนุมัติสินเชื่อไปยังอีเมลที่นางสาวสวยแจ้งไว้ โดยพนักงานธนาคารที่รับผิดชอบมีการส่งอีเมลที่ encrypt ข้อมูลไว้ และแจ้งรหัสผ่านไว้ให้เห็นชัดเจนที่ด้านล่างของอีเมลนั้น พร้อมทั้ง cc เจ้าหน้าที่ร้านสะดวกซื้อทั้งหมดด้วยในอีเมลเดียวกันเพื่อประหยัดเวลาในการแจ้งเจ้าหน้าที่ที่เกี่ยวข้อง

ควรเก็บข้อมูลเท่าที่จำเป็น จึงต้องตรวจสอบและขีดฆ่าข้อมูลอ่อนไหวที่อยู่ในสำเนาบัตรประชาชน

ตามมาตรฐานการรักษาความปลอดภัย ไม่ควรส่งรหัสผ่านไปในอีเมลฉบับเดียวกัน และไม่ควรส่งอีเมลถึงผู้ที่ไม่เกี่ยวข้องกับกระบวนการ

หากลูกค้าถอนความยินยอมทางการตลาดแล้ว ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลต่อไปได้ไหม ? ใช้เพื่อวัตถุประสงค์อะไรได้บ้าง ?

การแจ้งไม่ประสงค์จะได้รับการติดต่อเสนอขายทางการตลาด ไม่รวมถึงการได้รับแจ้งการเปลี่ยนแปลงเงื่อนไขการให้บริการ ดังนั้น**ธนาคารยังใช้ข้อมูลเพื่อวัตถุประสงค์ในการปฏิบัติตามสัญญาสินเชื่อ**ได้

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5

กรณีศึกษาเกี่ยวกับ
การจัดการข้อมูลก่อน PDPA บังคับใช้ และมาตรการรักษาความปลอดภัยของข้อมูล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5 กรณีศึกษาเกี่ยวกับ **การจัดการข้อมูลก่อน PDPA บังคับใช้ และมาตรการรักษาความปลอดภัยของข้อมูล**

ข้อมูลลูกค้าก่อนวันที่ 1 มิ.ย. 65 ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลได้แค่ไหน ? และหากธนาคารมีการประมวลผลต้องแจ้งสิ่งใดเพิ่มเติมให้ลูกค้าทราบด้วยหรือไม่ ?

สามารถประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์เดิมที่เคยแจ้งต่อลูกค้าหรือตามความคาดหมายเดิมของลูกค้า แต่จะต้องแจ้งถึงวิธีการยกเลิกความยินยอมให้ลูกค้าทราบด้วย

นอกจากนี้ ต้องคำนึงถึงเกณฑ์ที่เกี่ยวข้อง เช่น กรณีผู้ประกอบธุรกิจภายใต้การกำกับ ธปท. ต้องมีการเช็ค do-not-contact ตามเกณฑ์ Market Conduct ของ ธปท. ไม่ว่าจะเป็นกรณีประมวลผลข้อมูลที่มีอยู่ก่อนหรือหลังวันที่ 1 มิ.ย. 65

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5 กรณีศึกษาเกี่ยวกับ **การจัดการข้อมูลก่อน PDPA บังคับใช้ และมาตรการรักษาความปลอดภัยของข้อมูล**

การขอความยินยอมจากลูกค้าทางโทรศัพท์ในการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าให้แก่ vendor ที่ให้บริการ ออกบัตรและพิมพ์ข้อมูลบนหน้าบัตรเครดิตจำเป็นต้องขอความยินยอม ใช่หรือไม่ ?

การเปิดเผยข้อมูลให้กับ vendor ที่ให้บริการออกบัตรและพิมพ์ข้อมูลบนหน้าบัตรเครดิต ธนาคารควรใช้**ฐานสัญญา**ในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้บริการแก่ลูกค้าตามข้อกำหนดและเงื่อนไขการให้บริการ เนื่องจากเป็นความจำเป็นในการให้บริการ ไม่ควรขอความยินยอมลูกค้าอีก

วันที่ 10 ตุลาคม 2565 นายบุญได้โทรหาลูกค้าเพื่อเสนอขายผลิตภัณฑ์บัตรเครดิตตามปกติ และได้ขอความยินยอมจากลูกค้าทางโทรศัพท์ในการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าให้แก่ vendor ที่ให้บริการ emboss ออกบัตรและพิมพ์ข้อมูลบนหน้าบัตรเครดิต และขอความยินยอมการใช้ข้อมูลเพื่อนำเสนอผลิตภัณฑ์ที่เหมาะสมกับลูกค้าในอนาคตโดยที่ไม่ได้แจ้งประกาศความเป็นส่วนตัวในตอนนั้นเนื่องจากลูกค้าไม่ได้สอบถามแต่สัญญาว่าจะส่งรายละเอียดให้ลูกค้าอ่านอีกครั้งหลังจากวางสายโทรศัพท์

การดำเนินการขอความยินยอมจากสถานการณ์ที่ยกมานี้เหมาะสมหรือไม่

กรณีที่จะต้องขอความยินยอม พนักงานจะต้องแจ้ง privacy notice ให้แก่ลูกค้าทราบก่อนหรือในขณะการขอความยินยอม

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ความแตกต่างระหว่าง การใช้ฐานสัญญา และการขอความยินยอมจากลูกค้า เป็นอย่างไร ?

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติตามสัญญา ไม่ต้องขอความยินยอม
Contract

เฉพาะข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหวไม่สามารถใช้ฐานสัญญาได้*

เมื่อไม่ใช่เรื่องความยินยอม จึงไม่อาจถอนความยินยอมได้ เป็นเรื่องของนิติสัมพันธ์ตามสัญญา

จำกัดเฉพาะข้อมูลของเจ้าของข้อมูลผู้เป็นคู่สัญญาเท่านั้น

ภายใต้ขอบเขตของสัญญาตามที่ตกลงกัน

ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่จำเป็นในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา หรือเพื่อปฏิบัติตามสัญญา ก็ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลเพิ่มเติมอีก

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3)
*การปฏิบัติตามสัญญาไม่เพียงพอที่จะนำไปเก็บรวบรวม ใช้ หรือเปิดเผยสำหรับข้อมูลอ่อนไหว เว้นแต่เป็นกรณีสัญญาให้บริการทางการแพทย์ที่เข้าเงื่อนไขตามกฎหมายตามมาตรา 26(5)(ก)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

กรณีความยินยอม
Consent

ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง

คำนึงถึงความเป็นอิสระของเจ้าของข้อมูล

ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

รูปแบบการขอความยินยอมแต่ละองค์กรควรปรับให้เหมาะสมกับกิจกรรมการประมวลผลของตน

ทำโดยชัดแจ้งเป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์ก็ได้

เจ้าของข้อมูลมีสิทธิถอนเมื่อใดก็ได้

ขอความยินยอมเท่าที่จำเป็นเฉพาะกรณีไม่มีฐานการประมวลผลอื่น

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 และ 24 วรรคหนึ่ง
*ฐานการประมวลผล หมายถึง การเก็บรวบรวมข้อมูลที่ได้รับยกเว้นตามมาตรา 24 และ 26

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

5 กรณีศึกษาเกี่ยวกับ การจัดการข้อมูลก่อน PDPA บังคับใช้ และมาตรการรักษาความปลอดภัยของข้อมูล

การเข้าถึงระบบข้อมูลส่วนบุคคลของลูกค้า ควรมีมาตรการรักษาความปลอดภัยข้อมูลอย่างไร ? การดำเนินการที่ยกมานี้เหมาะสมหรือไม่ ?

ต่อมาวันที่ 20 ตุลาคม 2565 ธนาคาร MNO ได้อนุมัติบัตรเครดิตให้แก่ลูกค้า แต่นายชู พนักงานที่มีหน้าที่รับผิดชอบในการโทรแจ้งผลการอนุมัติลาพักร้อน จึงได้ขอให้เพื่อนพนักงานดำเนินการแทนโดยการให้ username และ password ในการเข้าไปดูรายละเอียดของลูกค้ารายดังกล่าว นายชูกำชับเพื่อนพนักงานคนดังกล่าวว่าอย่ามอบ username และ password ให้พนักงานฝ่ายอื่นต่อเด็ดขาด พนักงานคนดังกล่าวจึงได้แจ้งผลการอนุมัติให้แก่ลูกค้าเรียบร้อยตามกำหนดเวลา

เมื่อพนักงานคนดังกล่าวเห็นข้อมูลลูกค้าจำนวนมาก ก็เกิดความคิดจะนำข้อมูลลูกค้าไปแบ่งปันให้แก่เพื่อนที่ทำงานอยู่บริษัทประกันภัย เนื่องจากพนักงานคนดังกล่าวคิดว่าเป็นโอกาสที่ลูกค้าจะได้รับการเสนอบริการต่าง ๆ จากบริษัทที่หลากหลาย และทราบมาว่ามีการแบ่งปันซื้อขายข้อมูลส่วนบุคคลจำนวนมากจากข้อมูลของหน่วยงานภาครัฐและเอกชน จึงไม่ได้มองว่าการดำเนินการดังกล่าวเป็นเรื่องไม่ถูกต้อง

การมอบ username และ password ให้แก่พนักงานคนอื่น ถือเป็นการละเมิดความปลอดภัยของข้อมูลในแง่ของการรักษาความลับของข้อมูล (confidentiality)

การนำข้อมูลส่วนบุคคลของลูกค้าไปเผยแพร่ต่อภายนอกเป็นการกระทำที่ไม่ถูกต้อง

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

หลักการสำคัญเกี่ยวกับ
มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี
มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

โดยเน้นเรื่อง...

1. ต้องมีมาตรการ security ไม่ว่าจะเก็บข้อมูลในรูปแบบกระดาษหรืออิเล็กทรอนิกส์ หรือรูปแบบอื่นก็ตาม
   - การรักษาความลับของข้อมูล (confidentiality)
   - คงความถูกต้องครบถ้วน (integrity)
   - และทำให้ข้อมูลพร้อมใช้งาน (availability)
   - ต้องป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ
2. ต้องทบทวนมาตรการเมื่อมีความจำเป็น เช่นเมื่อมีเหตุการละเมิดเกิดขึ้น

3. ต้องประกอบด้วย มาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) โดยอาจรวมถึงมาตรการทางกายภาพ (physical measures)
4. จัดมาตรการป้องกันเท่าที่จำเป็นเหมาะสม โดยคำนึงถึงระดับความเสี่ยงขององค์กร ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

ที่มา : ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 มีผลบังคับใช้วันที่ 21 มิถุนายน 2565

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Key takeaways

- แจ้งให้ลูกค้าทราบถึงนโยบายขององค์กร ด้านการคุ้มครองข้อมูลส่วนบุคคล
- การเก็บ ใช้ เปิดเผยข้อมูล ให้พิจารณาว่ากรณีใดต้องขอความยินยอมจากลูกค้า
- เมื่อเกิดเหตุข้อมูลรั่วไหล ต้องรีบแจ้งตามกระบวนการที่องค์กรกำหนด เพื่อสามารถแจ้งต่อ สคส. ภายใน 72 ชม.
- ต้องมีความเข้าใจในกระบวนการภายใน เพื่อแจ้งต่อลูกค้า เมื่อมาขอใช้สิทธิ
- การรักษาความมั่นคงปลอดภัยต้องอยู่ในชีวิตประจำวันของทุกคน

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ปัญหา อุปสรรคที่พบ และการแก้ไขหลัง PDPA บังคับใช้

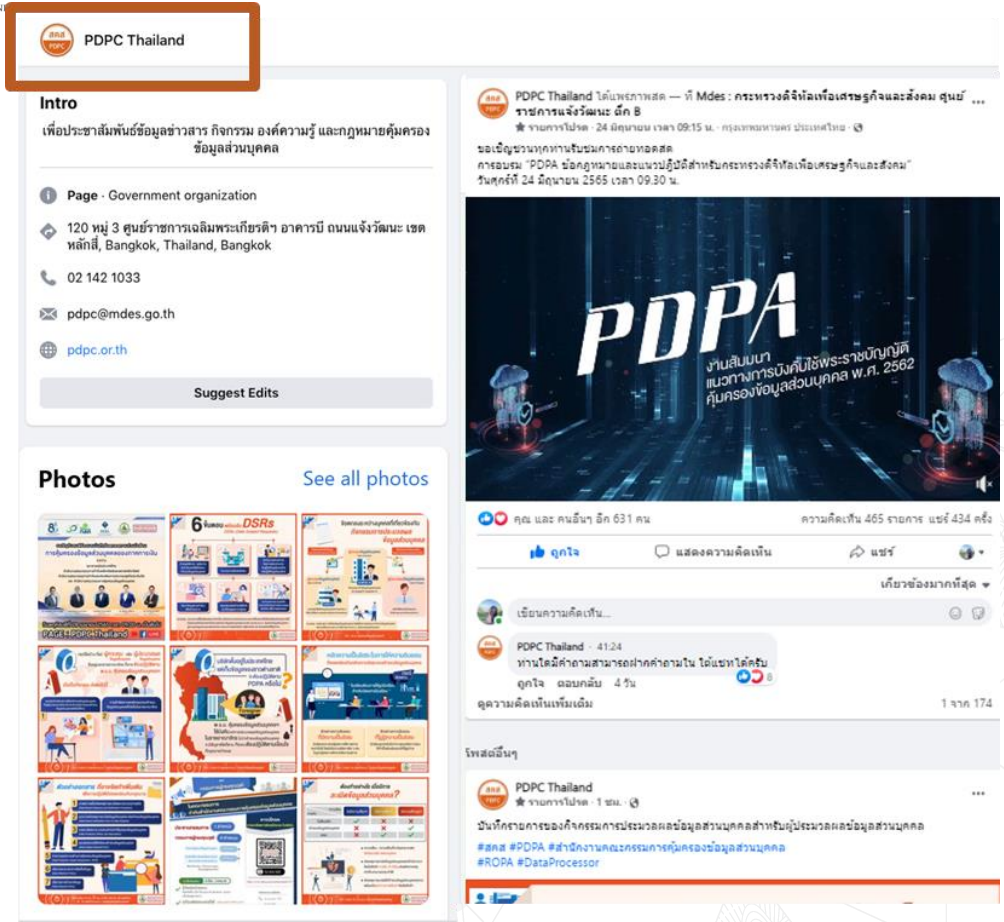
ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

แบบประเมินผลการจัดงาน workshop

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ช่องทางติดตามข่าวสาร สคส.



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

www.pdpc.or.th

PDPC Thailand

pdpc@mdes.go.th

1111 หรือ

0 2142 1033

เปลี่ยนแปลงเพื่อยืนหยัดดูแลเศรษฐกิจไทย