การเสวนา
เรื่อง การคุ้มครองข้อมูลส่วนบุคคล
วันพฤหัสบดีที่ 19 ธันวาคม พ.ศ. 2562

ณ ห้องประชุมออดิทอเรียม สำนักงานใหญ่
บริษัท การบินไทย จำกัด (มหาชน)

สุรางคณา วายุภาพ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

www.ETDA.OR.TH
Facebook: ETDA Thailand
Facebook: Surangkana Wayuparb

หัวข้อ

1. พัฒนาการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2. ข้อมูลส่วนบุคคลคืออะไร ?
3. PDPA
4. แนวปฏิบัติสากลที่เกี่ยวข้อ
5. Challenges

1 พัฒนาการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ต้องให้ความสำคัญเพราะ เมื่อโอนข้อมูลส่วนบุคคลไปต่างประเทศ ประเทศปลายทางที่รับข้อมูล ต้องมี**มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ**

2548

- APEC Privacy Framework

2556

- OECD : Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Information Security Management 27001/2013

2559

- ASEAN Framework on Personal Data Protection
- EU : General Data Protection Regulation (GDPR)

2562

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- **กฎหมายอื่น** ที่มีหลักเกณฑ์รองรับ Data Protection
- ISO/IEC **27701**:2019
- **NIST** Privacy Framework (Preliminary Draft)

2 ข้อมูลส่วนบุคคล คืออะไร ?

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ **ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม** แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลที่จะต้องดูแลเป็นพิเศษ ตามมาตรา 26 (Sensitive Data)

ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ฯลฯ

ความสัมพันธ์ระหว่าง

ความเป็นส่วนตัว
และ ข้อมูลส่วนบุคคล

ความเป็นส่วนตัว

เช่น สิทธิที่จะอยู่โดยลำพัง
(The right to be let alone)

ข้อมูลส่วนบุคคล

Examples

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

European Commission, *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en*

ตัวอย่างข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับธุรกิจการบิน

- ☑ ข้อมูลพนักงาน
- ☑ ข้อมูลลูกค้า (name, contact details, passport number and payment detail including sensitive data)
- ☑ ข้อมูลคู่ค้า

PDPA มาเสริมหลักเกณฑ์ Data Protection ใน กฎหมายอื่น ที่มีอยู่เดิม

PAYMENT

พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต
ปกป้องข้อมูลเครดิตที่ครอบคลุม
ข้อมูลส่วนบุคคล
(เป็นข้อยกเว้นของ PDPA)

ประกาศ ธปท. เรื่อง หลักเกณฑ์ทั่วไป ในการกำกับดูแลการประกอบธุรกิจ ระบบการชำระเงินภายใต้การกำกับ
กำหนดมาตรการดูแลการเก็บข้อมูลส่วนบุคคล

TELECOM

พ.ร.บ. กสทช.
กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล
ของผู้ใช้บริการโทรคมนาคม

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคม เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล สิทธิเจ้าของข้อมูล
และหน้าที่ผู้ให้บริการ

INSURANCE

ประกาศ คปภ. เรื่อง หลักเกณฑ์ วิธีการ ออก และการเสนอขายกรมธรรม์
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล

รัฐธรรมนูญ 2560

สิทธิในความเป็นส่วนตัว
และข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562

GOVERNMENT

พ.ร.บ. ข้อมูลข่าวสารราชการ
กำหนดมาตรการดูแลข้อมูลส่วนบุคคลที่รัฐดูแล

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
กำหนดธรรมาภิบาลข้อมูลภาครัฐ
ที่ครอบคลุมการดูแลข้อมูลส่วนบุคคล

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
ดูแลธุรกรรมออนไลน์ภาครัฐ เน้นสร้างความปลอดภัย
ลดความเสี่ยงต่อข้อมูลส่วนบุคคล & ระบบ

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ
แนวปฏิบัติดูแลข้อมูลส่วนบุคคลในการทำ
ธุรกรรมออนไลน์ภาครัฐ

HEALTHCARE

พ.ร.บ. สุขภาพแห่งชาติ
ปกป้องข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล
กำหนดเงื่อนไขการเปิดเผยข้อมูลสุขภาพ
พร้อมมาตการดูแล

การคุ้มครองข้อมูลส่วนบุคคลภาครัฐ มีหน่วยงานที่ผ่าน แต่ยังมีความท้าทายที่ต้องผลักดัน

ปัจจุบันมี **21** หน่วยงานของรัฐ **Pass!**

12 ใน 120 หน่วยงาน CI ที่ คธอ.ประกาศ (10%)

ทำแนวนโยบาย/แนวปฏิบัติ DP (ม.35) และ มี 75 ใน 120 หน่วยงาน CI (62.5%) ผ่าน Security Policy

ข้อจำกัดทางปฏิบัติ

1. ต้องผ่าน Security Policy ก่อน จึงจะทำ DP Policy ได้
2. ทางปฏิบัติยังมีความเข้าใจว่าตนเองไม่มีข้อมูลดังกล่าว
3. แม้มี ตัวอย่าง Template & เกณฑ์การตรวจ แต่รูปแบบการทำงาน/ข้อมูลของแต่ละหน่วยงาน ทำให้เกิดความเข้าใจไม่ตรงกัน

ความสอดคล้อง ม. 35 กับ หลักกฎหมายกลาง PDPA 2019

ความจำเป็นที่ต้องมีการปรับแก้เพื่อให้สอดคล้องกฎหมาย

เนื่องจากจะมีการดูแล **Digital ID & e-Signature** ที่เชื่อมโยงตัวบุคคล การดูแลข้อมูลส่วนบุคคลจึงสำคัญ

ความท้าทายกับสิ่งที่ต้องผลักดัน

- Encourage ให้หน่วยงานรัฐทำ **DP Policy** มากขึ้น
- ต้องช่วยให้ 120 หน่วยงาน CI มี SP Policy และ DP Policy ครบ
- ปรับปรุงแนวปฏิบัติ DP ให้สอดคล้องกับ กฎหมาย DP & กฎหมายอื่นๆ ที่เกี่ยวข้อง
- มี Format &Template ชัดเจน&ง่ายต่อการจัดทำมากขึ้น

“ข้อมูลส่วนบุคคล” มีความเสี่ยงอะไรบ้าง?

Cloud | Machine Learning
IoT | Cyber Attack
AI | Big Data & Data Analytic

Identity theft

“ถูกขโมยตัวตน”

เพื่อใช้ก่ออาชญกรรม และ
โจรกรรมข้อมูลทางการเงิน

SPAM

เช่น เบอร์โทรศัพท์,
email เป็นต้น

Tracking
Stalking

**“ติดตาม
สะกดรอย
สอดแนม”**

Profiling

**“ประมวลข้อมูล
เพื่อใช้กำหนด Profile”**

เพื่อเจาะโฆษณาหาประโยชน์
ทางการเมือง / การตลาด

Misuse

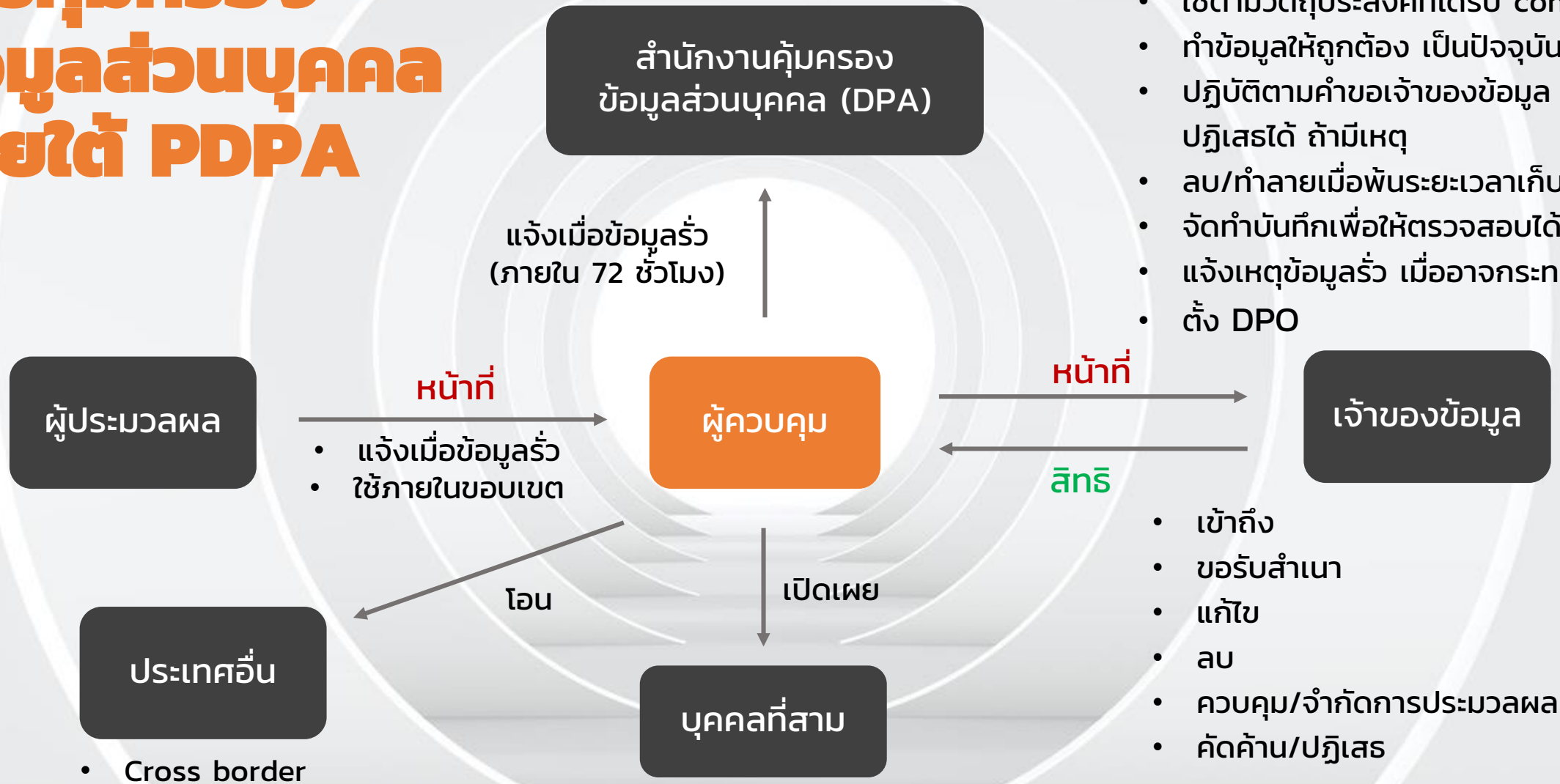
**“ข้อมูลถูกขาย
ให้บุคคลที่ 3”**

เพื่อใช้ประโยชน์ทางการตลาด
เช่น กรณีของ Facebook
และ Cambridge Analytica

3 PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การคุ้มครองข้อมูลส่วนบุคคลภายใต้ PDPA



- เก็บเท่าที่จำเป็น และมีฐานตามกฎหมาย
- ใช้ตามวัตถุประสงค์ที่ได้รับ consent
- ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน
- ปฏิบัติตามคำขอเจ้าของข้อมูล ปฏิเสธได้ ถ้ามีเหตุ
- ลบ/ทำลายเมื่อพ้นระยะเวลาเก็บ
- จัดทำบันทึกเพื่อให้ตรวจสอบได้
- แจ้งเหตุข้อมูลรั่ว เมื่ออาจกระทบ
- ตั้ง DPO

- เข้าถึง
- ขอรับสำเนา
- แก้ไข
- ลบ
- ควบคุม/จำกัดการประมวลผล
- คัดค้าน/ปฏิเสธ

ใคร
ที่มีสิทธิ & หน้าที่ ทำอะไร เก็บรวบรวม, ใช้, เปิดเผย

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

- ให้**ความยินยอม** เท่าที่เหมาะสม
- รับทราบและใช้สิทธิที่มี

ผู้ควบคุมข้อมูลส่วนบุคคล (Controller)

- มีมาตรการดูแล Security ที่เหมาะสม และทบทวนสม่ำเสมอ
- ลบ ทำลายข้อมูล เมื่อพ้นระยะเวลาเก็บรักษา
- แจ้งเหตุละเมิด ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ
- ถ้าเป็น บจก. ตปท. ต้องแต่งตั้งตัวแทน และตั้ง **DPO**
- จัดทำ + เก็บรักษาบันทึกรายงาน

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor)

- เก็บ ใช้ เปิดเผยตามคำสั่ง
- จัดให้มีมาตรการดูแล Security ที่เหมาะสม
- แจ้งเหตุละเมิดให้ Controller ทราบ
- จัดทำ + เก็บรักษาบันทึกรายงาน

คณะกรรมการ
ที่ดูแล Law Compliance ตาม PDPA

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- จัดทำแผนแม่บท และแผนระดับชาติ
- กำหนดมาตรการและแนวทางการดำเนินงานเกี่ยวกับ DP
- ออกประกาศหลักเกณฑ์/มาตรการ
- วินิจฉัยชี้ขาด
- ส่งเสริมและสนับสนุนด้าน DP

คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียน
- ตรวจสอบการดำเนินการของผู้ที่เกี่ยวข้อง
- ไกล่เกลี่ยข้อพิพาท

Law Compliance ตามกฎหมายอื่น
ที่มีลักษณะเฉพาะ ลงลึก และ based on minimum requirement ของ PDPA พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

RIGHTS OF DATA SUBJECT

ความแตกต่างกันของ GDPR & PDPA

= สิทธิในการได้รับแจ้งข้อมูล

= สิทธิในการเข้าถึงข้อมูล

= สิทธิในการแก้ไขข้อมูลให้ถูกต้อง

= สิทธิในการลบ

= สิทธิในการจำกัดการประมวลผลข้อมูล

= สิทธิในการโอนย้ายข้อมูล

= สิทธิในการคัดค้าน

≠ สิทธิในการคัดค้านการตัดสินใจแทนโดยอัตโนมัติ

- **Data Controller**
- **Data Processor**

สำรวจตนเอง

จัดทำ DP policy กำหนดเป้าหมาย การเก็บรวมรวบ การใช้ การเปิดเผย สร้างความโปร่งใส

ศึกษาข้อมูล DP policy ให้มั่นใจใน กระบวนการ คุ้มครองข้อมูล ส่วนบุคคล

แต่งตั้ง DPO

เมื่อ :
- Controller, Processor เป็น หน่วยงานของรัฐ
- มีการเก็บ ใช้ เปิดเผยข้อมูล จำนวนมาก
- มีกิจกรรมหลักเป็น การเก็บ ใช้ เปิดเผย Sensitive Data

DPO มีหน้าที่
- ให้คำแนะนำ
- ตรวจสอบการ ดำเนินการที่เกี่ยวกับ การเก็บ ใช้ เปิดเผย
- ประสานงานกับ สนง.เมื่อมีปัญหา
- รักษาความลับ

มี Contract point ที่เป็น DPO กรณีมี ปัญหาเกิดขึ้น

การเก็บรวบรวม

ขอความยินยอมที่ชัดเจน เข้าใจง่าย มีหลักฐานเป็น doc หรือ e-document

แจ้งวัตถุประสงค์ เช่น
- การใช้
- การเปิดเผย
- ระยะเวลาการจัดเก็บ
- แจ้งสิทธิต่าง ๆ แก่เจ้าของข้อมูล

การเก็บรวมรวมต้องทำ เท่าที่จำเป็นเหมาะสม

รู้วัตถุประสงค์ ข้อมูล ส่วนบุคคลที่จัดเก็บ และ สิทธิของตนเอง

ให้ความยินยอมตาม ความจำเป็น เหมาะสม

ถ้าเป็นเด็ก ให้ผู้มีอำนาจ ปกครองให้ความยินยอม

ถ้าเป็นคนไร้ฯ คนเสมือน ไร้ฯ ให้ผู้อนุบาล / ผู้พิทักษ์ความยินยอม

การใช้ การเปิดเผยข้อมูล

ใช้ เปิดเผยตาม วัตถุประสงค์

ทำสัญญากับ Third Party กำหนดหน้าที่ดูแล หากมีการประมวลผล ข้อมูล

โอนข้อมูลไปต่างประเทศได้ เมื่อหน่วยงาน / องค์กร มาตรฐานที่เพียงพอ

โอนข้อมูลไปต่างประเทศ ในเครือเดียวกันได้ หาก DP Policy ได้รับการ รับรองจาก สนง..

ตรวจสอบข้อมูลว่า
- ได้ใช้ / เปิดเผย ตาม วัตถุประสงค์หรือไม่
- ใช้ / เปิดเผย นอกเหนือจาก วัตถุประสงค์หรือไม่

สิทธิและหน้าที่

ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน

ต้องปฏิบัติตามคำขอเจ้าของข้อมูล

ปฏิเสธคำขอได้ ถ้ามีกฎหมาย คำสั่งศาล กำหนดไว้ หรือกระทบต่อสิทธิ เสรีภาพ ของผู้อื่น และต้องบันทึกเหตุผลด้วย

ลบ ทำลายข้อมูลเมื่อพ้นระยะเวลาเก็บ

หากได้รับคำขอให้ลบ ทำลาย หรือ Anonymous ต้องรับผิดชอบทั้ง ทางเทคโนโลยีและค่าใช้จ่ายตามคำขอนั้น

กรณีให้ข้อมูลแก่คนอื่น ต้องป้องกัน ไม่ให้ผู้อื่นใช้ /เปิดเผย ข้อมูลโดยไม่ชอบ

จัดทำบันทึกเกี่ยวกับข้อมูล เพื่อให้ ตรวจสอบได้.

ได้รับสิทธิต่าง ๆ เพื่อดูแลข้อมูลตัวเอง
- เข้าถึง
- รับสำเนา
- ให้เปิดเผยแหล่งที่มากรณี ที่ไม่ได้ให้ความยินยอม
- ส่ง / โอน / ย้ายข้อมูล
- คัดค้าน
- ลบ / ขอทำลาย / ขอ Anonymous
- ขอให้ระงับการประมวลผล
- ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน

สามารถร้องเรียนต่อ คกก.ผู้เชี่ยวชา
หากผู้ควบคุมไม่ดำเนินการตามที่ร้อง

Data Breach

จัดให้มีมาตรการ Incident response

แจ้งเหตุแก่ สนง. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

แจ้งแหตุแก่เจ้าของข้อมูล + แนวทางเยียวยาโดย ไม่ชักช้า

ได้รู้ถึงสาเหตุ + แนวทางการการเยียวยา

ถอนความยินยอม

จัดทำช่องทาง การถอนที่ง่าย เหมือนตอน ขอความยินยอม

แจ้งผลกระทบ การขอยกเลิก

รับทราบ ผลกระทบของ การยกเลิก

Security

จัดให้มีมาตรการ Security

ทบทวนมาตรการ Security เมื่อจำเป็นหรือ เทคโนโลยี เปลี่ยนแปลงไป

มั่นใจในความ มั่นคงปลอดภัย

Data subject

ประเภทของ Data Breach

หรือการละเมิดข้อมูลส่วนบุคคล

การละเมิดความพร้อมใช้ของข้อมูล (Availability Breach)

การทำลายข้อมูลส่วนบุคคลที่ไม่ไปเป็นตามกฎหมายหรือเกิดเหตุสุดวิสัย ทำให้ข้อมูลเสียหาย

การละเมิดความครบถ้วนสมบูรณ์ของข้อมูล (Integrity Breach)

การเปลี่ยนแปลงข้อมูลส่วนบุคคล

การละเมิดความลับของข้อมูล (Confidentiality Breach)

การเปิดเผยหรือเข้าถึงโดยไม่มีสิทธิของข้อมูลส่วนบุคคล

4ขั้นตอน PDPA

เพื่อเตรียมพร้อม Comply ตาม Personal Data Protection Act

มีกระบวนการประเมินความเสี่ยง
เพื่อให้แน่ใจว่าการออกแบบและกระบวนการถูกต้องเหมาะสม

บริหาร Law Compliance
ให้มีประสิทธิภาพ

มีข้อมูลอะไร ข้อมูลอยู่ที่ไหน ใครเข้าถึงได้บ้าง สิทธิและหน้าที่ความรับผิดที่เกิดขึ้น โดยคำนึงถึง governance

รับมือ และ response
ต่อภัยคุกคามที่ส่งผลกระทบให้ข้อมูลรั่วไหล และการบริหารจัดการเมื่อมีข้อมูลรั่วไหล

Source: RSAConference 2018

สิ่งที่ควรเตรียมพร้อม

ก่อน PDPA ใช้บังคับ

Key to Success

1. **ตั้งงบประมาณ** และได้การสนับสนุนจากผู้บริหาร
2. **แต่งตั้ง Working Group** หรือ **DPO** ในองค์กร
3. **กำหนดประเภทของข้อมูล และวัตถุประสงค์ความจำเป็น**
4. **ทบทวน Data Protection Policy** เช่น บริหารจัดการ การเข้าถึงข้อมูล life-cycle ของข้อมูล
5. **จัดเตรียมข้อกำหนดหรือแนวปฏิบัติ** การคุ้มครองข้อมูลส่วนบุคคล
6. **จัดทำเอกสารมาตรการ Security**
7. **พัฒนากระบวนการแจ้งเตือน** (Breach Notification)
8. **สร้างความตระหนักและ training** ให้กับบุคลากร พนักงาน เจ้าหน้าที่ และลูกค้า
9. **พัฒนาทักษะ** และกระบวน Audit
10. **Privacy by Design & Security by Design**

Source: RSAConference 2018

Privacy by Design and Default

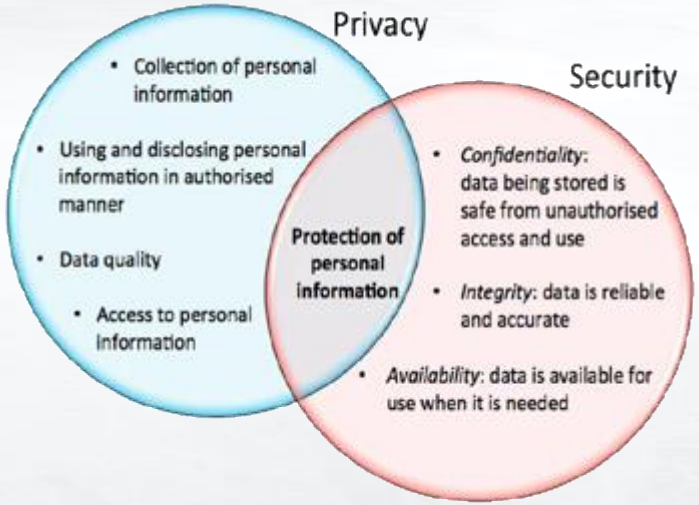
Ref: ISO/IEC 27701 Annex. A.7.4, B.8.4

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- จำกัดการประมวลผลข้อมูล เช่น การจัดเก็บ การแสดงผล เฉพาะที่จำเป็นเท่านั้น (need-to-know)
- มีกลไกการยืนยันความถูกต้องของข้อมูลที่จัดเก็บและประมวลผล
- มีกลไกการลดข้อมูลที่จะนำมาใช้ในการเชื่อมโยงตัวบุคคล
- มีการจำกัดช่วงเวลาของการเก็บข้อมูล
- มีกลไกการทำลายข้อมูลทั้งในรูปแบบของข้อมูลดิบและข้อมูลบ่งชี้ (metadata)
- มีกลไกการควบคุมการส่งข้อมูลไปยังผู้รับปลายทาง เพื่อให้แน่ใจว่าข้อมูลไม่สามารถเข้าถึงได้โดยบุคคลอื่น

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- มีกลไกการทำลายข้อมูลของระบบหรือแอปพลิเคชันที่เกิดขึ้นระหว่างการประมวลผล (Temporary File)
- มีกระบวนการเพื่อให้ผู้เกี่ยวข้อง เช่น ลูกค้า มั่นใจได้ว่าข้อมูลที่ประมวลผลจะถูก ส่งคืน ถ่ายโอน และทำลาย
- มีกลไกการควบคุมการส่งข้อมูลไปยังผู้รับปลายทาง เพื่อให้แน่ใจว่าข้อมูลไม่ถูกเปลี่ยนแปลงก่อนถึงผู้รับ



17

4. แนวปฏิบัติสากลที่เกี่ยวข้อง

แนวปฏิบัติสากล
ที่อาจนำมาปรับใช้ในระหว่างรอหลักเกณฑ์
DATA PRIVACY& PROTECTION

ISO/IEC 27701:2019

Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information Management – Requirements and guidelines

ISACA Privacy Principles

The COBIT Framework

Data Relevant Business Objectives and Governance Objectives

Preliminary Draft

NIST Privacy Framework

แนวปฏิบัติสำหรับ information security standards และ information security management

ISO/IEC 27001:2013

+

ISO/IEC 27002:2013

+

ISO/IEC 27701:2019

แนวทางในการดูแล Personal data ขององค์กร
NIST Privacy Framework

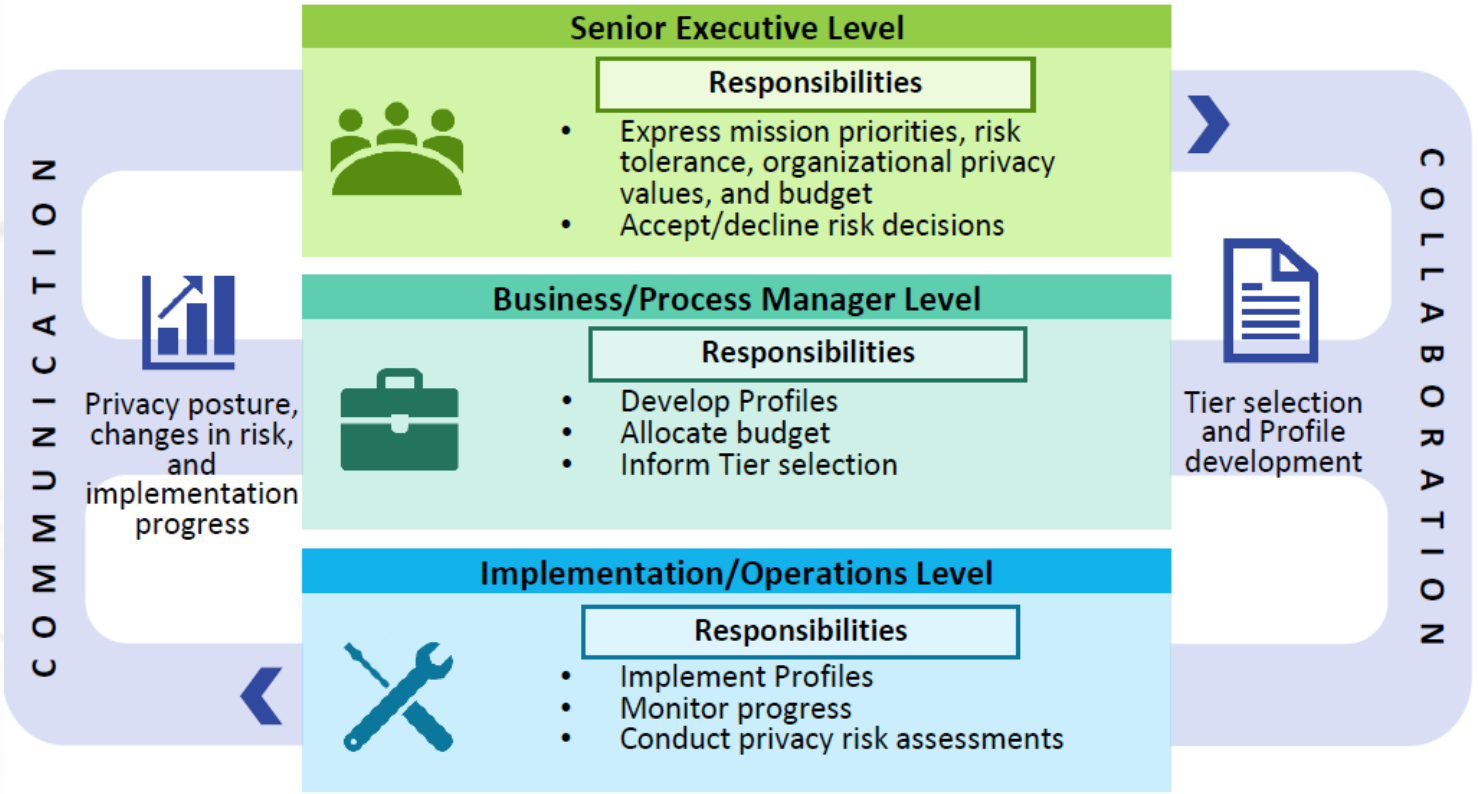


Figure 6: Notional Collaboration and Communication Flows Within an Organization

Source: Preliminary Draft NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework)

5. Challenges

ข้อกำหนดในการโอนและประมวลผลข้อมูลส่วนบุคคลที่แตกต่างกันในแต่ละประเทศ

จะทำอย่างไรให้ได้รับประโยชน์จาก big data และการประมวลผลข้อมูลในขณะที่ปฏิบัติตามกฎหมายเหล่านี้

ผลกระทบกับภาคธุรกิจ

non-compliance

สูญเสีย**ความน่าเชื่อถือ**

ถูก**ดำเนินคดี**ทางกฎหมาย
จ่ายค่าเสียหาย/จำคุก

เกิด**ค่าเสียโอกาส**
และเพิ่มต้นทุนค่าใช้จ่าย

เสียเปรียบในการแข่งขัน**ทางการค้า**

(effective) compliance

ความเชื่อมั่นและไว้วางใจ
จากลูกค้า/ลูกจ้าง/คู่ค้า

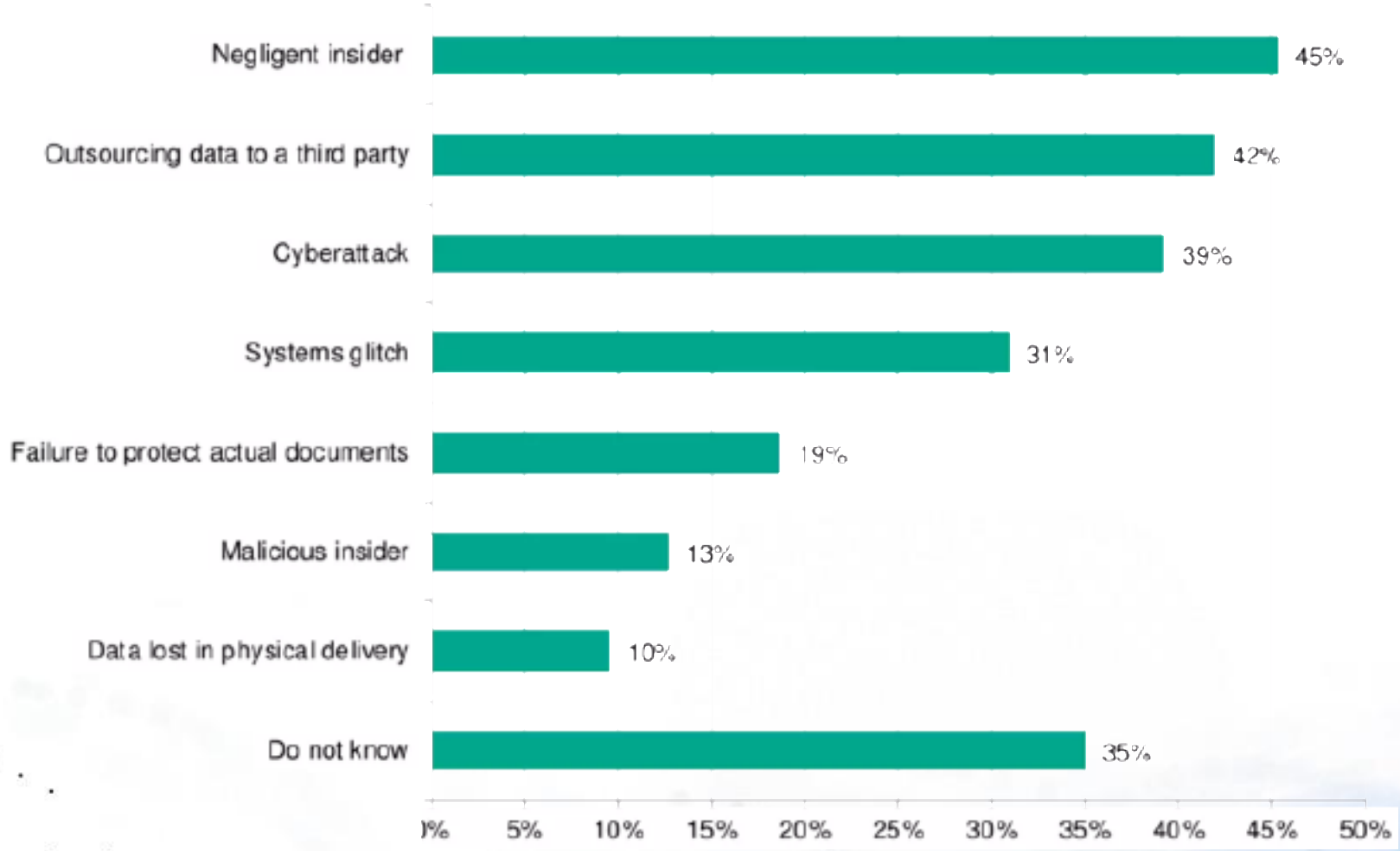
ใช้ข้อมูลเพื่อ**ทำแคมเปญการตลาด**
ให้ดึงดูดใจลูกค้า

เกิดอะไร หลัง GDPR ใช้บังคับมา 1 ปีกว่า

- 1 ใน 4 ของบริษัทที่ตอบแบบสอบถาม เชื่อมั่นใน**ระดับต่ำ**ว่าพร้อมและสามารถตอบสนองเมื่อเกิดเหตุ data breach ได้ตามที่ GDPR กำหนด
- มีเพียง 18% ที่มั่นใจใน**ระดับสูง**ว่าสามารถแจ้งเหตุ data breach แก่หน่วยงานได้ทันภายใน 72 ชั่วโมง
- กว่าครึ่งเชื่อว่าการดำเนินการตาม GDPR ใช้เวลา**มากกว่าที่คาดการณ์**ไว้
- เกือบครึ่งพบว่ามี**ประมาณ 2 เหตุ** data breach ที่ต้องรายงาน นับแต่ GDPR ใช้บังคับ

Source: www.digitalguardian.com/blog/survey-gdpr-compliance-still-lagging

ผลสำรวจพบว่าสาเหตุส่วนใหญ่ของ **Data Breach** เกิดจากการ**ละเลย**ของคนทำงาน หรือการ**ส่งต่อ**ข้อมูลไปให้บุคคลที่สาม



*สามารถตอบได้มากกว่าหนึ่งข้อ

Source: www.digitalguardian.com/blog/survey-gdpr-compliance-still-lagging