กฎหมายคุ้มครอง
ข้อมูลส่วนบุคคล
กับบริบท การคุ้มครองข้อมูลส่วนบุคคลในกฎหมายฉบับอื่น ๆ

สุรางคณา วายุภาพ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

www.ETDA.OR.TH

Facebook: ETDA Thailand

Facebook: Surangkana Wayuparb

กฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับสากล

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
- กฎหมายอื่นๆ ที่มีหลักเกณฑ์รองรับ Data Protection
- ISO/IEC 27701:2019
- Preliminary Draft-NIST Privacy Framework

DATA PRIVACY & PROTECTION
Law Landscape

รัฐธรรมนูญ 2560
ความเป็นส่วนตัวข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562

PAYMENT
พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต
ปกป้องข้อมูลเครดิตที่ครอบคลุมข้อมูลส่วนบุคคล
(เป็นข้อยกเว้นของ PDPA)

ประกาศ ธปท. เรื่อง หลักเกณฑ์ทั่วไปในการกำกับดูแลการประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ
กำหนดมาตรการดูแลการเก็บข้อมูลส่วนบุคคล

INSURANCE
ประกาศ คปภ. เรื่อง หลักเกณฑ์ วิธีการออก และการเสนอขายกรมธรรม์
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล

TELECOM
พ.ร.บ. กสทช.
กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการโทรคมนาคม

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคม เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล สิทธิเจ้าของข้อมูล และหน้าที่ผู้ให้บริการ

GOVERNMENT
พ.ร.บ. ข้อมูลข่าวสารราชการ
กำหนดมาตรการดูแลข้อมูลส่วนบุคคลที่รัฐดูแล

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
กำหนดธรรมาภิบาลข้อมูลภาครัฐ ที่ครอบคลุมการดูแลข้อมูลส่วนบุคคล

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

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ
แนวปฏิบัติดูแลข้อมูลส่วนบุคคลในการทำธุรกรรมออนไลน์ภาครัฐ

HEALTHCARE
พ.ร.บ. สุขภาพแห่งชาติ
ปกป้องข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล
กำหนดเงื่อนไขการเปิดเผยข้อมูลสุขภาพ พร้อมมาตการดูแล

DATA PRIVACY& PROTECTION
Mapping

● มี แต่อาจมีรายละเอียดที่แตกต่าง
● ไม่มี

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	Personnel Data	Consent	Right of Data Subject	Data Security	Data Breach Notification	Sanction
พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต	●	●	●	●	●	●
พ.ร.บ. กสทช. & ประกาศ	●	●	●	●	●	●
พ.ร.บ. สุขภาพแห่งชาติ & ประกาศ	●	●	●	●	●	●
พ.ร.บ. ข้อมูลข่าวสารราชการ	●	●	●	●	●	●
พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล	●	●	●	●	●	●
พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์	●	●	●	●	●	●

สามารถระบุ/เชื่อมโยงเจ้าของข้อมูลได้ทั้งทางตรงทางอ้อม

โยงมายัง PDPA

ไม่กำหนดนิยามเพื่อรองรับกฎหมายที่ไปเสริม

แนวนโยบาย/แนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลภาครัฐ

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

12 ใน 120 หน่วยงาน CI ที่ ครอ.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

ต้องผลักดัน

- 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
- อาจปรับแนวทางให้ประกาศได้เลย โดยไม่ต้องตรวจก่อน แต่เน้นการตรวจ Comply ตาม ม. 35

ข้อมูลส่วนบุคคล คืออะไร ?

"ข้อมูลส่วนบุคคล" หมายความว่า

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ
ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

แต่ไม่รวมถึงข้อมูลของ
ผู้ถึงแก่กรรมโดยเฉพาะ

: *พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*

"personal data" means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

: General Data Protection Regulation (GDPR), EU

Examples of personal data

- 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

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

สรุปภาพรวม PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562

ขอบเขตการบังคับใช้

- ใช้บังคับทั้งใน และนอกราชอาณาจักร กรณี :
  - เสนอขายสินค้า หรือบริการ
  - เฝ้าติดตามพฤติกรรม
- ใช้เป็นกฎหมายกลาง
- ไม่ใช้บังคับ :
  - เพื่อประโยชน์ส่วนตัวโดยแท้
  - การดำเนินการของรัฐ
  - เพื่อการสื่อสารมวลชนฯ
  - สส. / สว.
  - การพิจารณาคดี
  - ตาม Cybersecurity act

สนง. คกก.

- ตั้งสำนักงานชั่วคราว
- ตั้งสำนักงาน (ภายใน 1 ปี)
- คกก. (ภายใน 90 วัน)
- มีเลขาธิการ (90 วันนับแต่ตั้ง สนง.)

บังคับใช้ทันที

- คกก.
- สำนักงาน

ครบ 1 ปี

- ความยินยอม
- การคุ้มครองข้อมูล
- หน้าที่ผู้เกี่ยวข้อง
- การตั้ง DPO
- หน้าที่ DPO
- สิทธิของเจ้าของข้อมูลฯ
- การร้องเรียน
- การลงโทษ

ขอยินยอม

- เก็บ ใช้ เปิดเผย ต้องขอความยินยอม + แจ้งวัตถุประสงค์ก่อน
- ความยินยอมต้องชัดแจ้ง เข้าใจง่าย เป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์
- ขอถอนคำยินยอมได้

คุ้มครองข้อมูล

- เก็บรวมรวมเท่าที่จำเป็น
- เก็บจากเจ้าของโดยตรง
- ไม่เป็น Sensitive Data
- ใช้ และเปิดเผยได้ตามวัตถุประสงค์ที่ขอไว้
- โอนข้อมูลไป ตปท. ต้องมีมาตรฐานคุ้มครองที่เพียงพอ
- โอนข้อมูลไป ตปท. ภายในเครือ Privacy Policy ต้องได้รับตรวจสอบ + รับรองจาก สนง.

หน้าที่ผู้เกี่ยวข้อง

- Controller มีหน้าที่
  - จัดให้มี Security
  - มีระบบรองรับการลบ ทำลายแจ้งเหตุละเมิดแก่ สนง. ภายใน 72 ชั่วโมง
  - ถ้าเป็น บจก. .ตปท. ต้องแต่งตั้งตัวแทน
  - บันทึกรายการเป็นหนังสือ หรือ e-doc
- Processor มีหน้าที่
  - เก็บ ใช้ เปิดเผย ตามคำสั่งที่ได้รับ
  - จัดให้มี Security
  - แจ้งเหตุละเมิดให้ Controller ทราบ
  - จัดทำบันทึกเป็นหนังสือ หรือ e-doc

การตั้ง DPO

- ให้ตั้ง DPO ถ้าเป็นกรณี :
  - Controller และ Processor เป็นหน่วยงานของรัฐ
  - มีข้อมูลที่เก็บ ใช้ เปิดเผย เป็นจำนวนมาก จำเป็นต้องตรวจสอบข้อมูลและระบบอย่างสม่ำเสมอ
  - กิจกรรมหลักเป็นการเก็บ ใช้ เปิดเผยข้อมูล Sensitive Data
- ถ้า Controller และ Processor เป็นเครือกิจการเดียวกัน ตั้ง DPO ร่วมกันได้

หน้าที่ DPO

- ให้คำแนะนำ
- ตรวจสอบการดำเนินการที่เกี่ยวกับการเก็บใช้เปิดเผย
- ประสานงานกับ สนง. เมื่อมีปัญหา
- รักษาความลับ

สิทธิของเจ้าของข้อมูล

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

การร้องเรียน

- ร้องเรียนไปที่ คกก. ผู้เชี่ยวชาญ / สนง. ตามแบบที่ประกาศกำหนด
- คกก. พิจารณาโดยไกล่เกลี่ย / มีคำสั่งให้แก้ไข ถ้าไม่ดำเนินการ สามารถ ยึด อายัด ขายทอดตลาดซึ่งทรัพย์สินได้

บทลงโทษ

- แพ่ง (ชดใช้เงิน)
- ปกครอง (ปรับ)
- อาญา (จำคุก / ปรับ)

หมายเหตุ : ประกาศ ระเบียบที่คกก. ควรออกภายใน 1 ปีนับแต่ พ.ร.บ.ใช้บังคับ ไม่ทันให้รายงาน ครม. ทราบ

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

สำรวจตนเอง	แต่งตั้ง DPO	การเก็บรวบรวม	การใช้ การเปิดเผยข้อมูล	สิทธิและหน้าที่	Data Breach	ถอนความยินยอม	Security
จัดทำ DP policy กำหนดเป้าหมาย การเก็บรวมรวบ การใช้ การเปิดเผย สร้างความโปร่งใส	เมื่อ : • Controller, Processor เป็นหน่วยงานของรัฐ • มีการเก็บ ใช้ เปิดเผยข้อมูลจำนวนมาก • มีกิจกรรมหลักเป็นการเก็บ ใช้ เปิดเผย Sensitive Data DPO มีหน้าที่ • ให้คำแนะนำ • ตรวจสอบการดำเนินการที่เกี่ยวกับการเก็บ ใช้ เปิดเผย • ประสานงานกับ สนง.เมื่อมีปัญหา • รักษาความลับ	ขอความยินยอมที่ชัดเจน เข้าใจง่าย มีหลักฐานเป็น doc หรือ e-document แจ้งวัตถุประสงค์ เช่น • การใช้ • การเปิดเผย • ระยะเวลาการจัดเก็บ • แจ้งสิทธิต่าง ๆ แก่เจ้าของข้อมูล การเก็บรวมรวมต้องทำเท่าที่จำเป็นเหมาะสม	ใช้ เปิดเผยตามวัตถุประสงค์ ทำสัญญากับ Third Party กำหนดหน้าที่ดูแลหากมีการประมวลผลข้อมูล โอนข้อมูลไปต่างประเทศได้เมื่อหน่วยงาน / องค์กร มาตรฐานที่เพียงพอ โอนข้อมูลไปต่างประเทศในเครือเดียวกันได้ หาก DP Policy ได้รับการรับรองจาก สนง..	ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน ต้องปฏิบัติตามคำขอเจ้าของข้อมูล ปฏิเสธคำขอได้ ถ้ามีกฎหมาย คำสั่งศาล กำหนดไว้ หรือกระทบต่อสิทธิ เสรีภาพของผู้อื่น และต้องบันทึกเหตุผลด้วย ลบ ทำลายข้อมูลเมื่อพ้นระยะเวลาเก็บ หากได้รับคำขอให้ลบ ทำลาย หรือ Anonymous ต้องรับผิดชอบทั้งทางเทคโนโลยีและค่าใช้จ่ายตามคำขอนั้ กรณีให้ข้อมูลแก่คนอื่น ต้องป้องกันไม่ให้ผู้อื่นใช้ /เปิดเผย ข้อมูลโดยไม่ชอบ จัดทำบันทึกเกี่ยวกับข้อมูล เพื่อให้ตรวจสอบได้.	จัดให้มีมาตรการ Incident response แจ้งเหตุแก่ สนง. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ แจ้งแหตุแก่เจ้าของข้อมูล + แนวทางเยียวยาโดยไม่ชักช้า	จัดทำช่องทางการถอนที่ง่าย เหมือนตอนขอความยินยอม แจ้งผลกระทบการขอยกเลิก	จัดให้มีมาตรการ Security ทบทวนมาตรการ Security เมื่อจำเป็นหรือเทคโนโลยีเปลี่ยนแปลงไป
ศึกษาข้อมูล DP policy ให้มั่นใจในกระบวนการคุ้มครองข้อมูลส่วนบุคคล	มี Contract point ที่เป็น DPO กรณีมีปัญหาเกิดขึ้น	รู้วัตถุประสงค์ ข้อมูลส่วนบุคคลที่จัดเก็บ และสิทธิของตนเอง ให้ความยินยอมตามความจำเป็น เหมาะสม ถ้าเป็นเด็ก ให้ผู้มีอำนาจปกครองให้ความยินยอม ถ้าเป็นคนไร้ฯ คนเสมือนไร้ฯ ให้ผู้อนุบาล / ผู้พิทักษ์ความยินยอม	ตรวจสอบข้อมูลว่า • ได้ใช้ / เปิดเผย ตามวัตถุประสงค์หรือไม่ • ใช้ / เปิดเผย นอกเหนือจากวัตถุประสงค์หรือไม่	ได้รับสิทธิต่าง ๆ เพื่อดูแลข้อมูลตัวเอง • เข้าถึง • รับสำเนา • ให้เปิดเผยแหล่งที่มากรณีที่ไม่ได้ให้ความยินยอม • ส่ง / โอน / ย้ายข้อมูล • คัดค้าน • ลบ / ขอทำลาย / ขอ Anonymous • ขอให้ระงับการประมวลผล • ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน สามารถร้องเรียนต่อ คกก.ผู้เชี่ยวชาญ หากผู้ควบคุมไม่ดำเนินการตามที่ร้องขอ	ได้รู้ถึงสาเหตุ + แนวทางการการเยียวยา	รับทราบผลกระทบของการยกเลิก	มั่นใจในความมั่นคงปลอดภัย

- **Data subject**

4 ขั้นตอน PDPA

เพื่อเตรียมพร้อม Comply ตาม Personal Data Protection Act

มีกระบวนการประเมินความเสี่ยง
เพื่อให้แน่ใจว่าการออกแบบและกระบวนการถูกต้องเหมาะสม

บริหาร Law Compliance
ให้มีประสิทธิภาพ

1. การประเมินความเสี่ยง
(Risk Assessment)

2. ธรรมาภิบาลข้อมูล
(Data Governance)

3. การบริหารเพื่อให้มีการปฏิบัติตามกฎเกณฑ์
(Compliance Management)

4. มาตรการรับมือเมื่อข้อมูลรั่วไหล
(Breach Response)

มีข้อมูลอะไร ข้อมูลอยู่ที่ไหน
ใครเข้าถึงได้บ้าง สิทธิและหน้าที่
ความรับผิดที่เกิดขึ้น
โดยคำนึงถึง governance

รับมือ และ response
ต่อภัยคุกคามที่ส่งผลกระทบ
ให้ข้อมูลรั่วไหล และการบริหารจัดการ
เมื่อมีข้อมูลรั่วไหล

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

Best Practice ที่ควรใช้ประกอบการจัดทำ

ข้อปฏิบัติในการดูแลข้อมูลส่วนบุคคล

Critical Data Protection Program

- ระบุและกำหนดข้อมูลส่วนบุคคล กำหนดมาตรการรักษาความมั่นคงปลอดภัย
- วิเคราะห์และจำแนกมิติที่สำคัญที่สุดของสภาพแวดล้อมข้อมูล
- ทำ GAP Analysis ของกระบวนการและมาตรการควบคุมความมั่นคงปลอดภัยข้อมูลสำคัญ
- ทำแผนการลดความเสี่ยงเพื่อจัดลำดับความสำคัญและทดสอบแนวทางแก้ไข
- ตรวจสอบกรอบการรักษาความมั่นคงปลอดภัย

Define

ข้อมูลส่วนบุคคลอะไร

- ทำความเข้าใจกลยุทธ์โดยรวมการรักษาความมั่นคงปลอดภัยข้อมูล
- กำหนดเป้าหมายการปกป้อง
- พัฒนาโครงสร้างโมเดลข้อมูล/อนุกรมวิธาน

Discover

ข้อมูลอะไรมีการใช้งานอย่างไร

- ทำความเข้าใจสภาพแวดล้อมข้อมูล โครงสร้าง และ lifecycle
- ดำเนินการตรวจค้น วิเคราะห์ และจำแนกอย่างต่อเนื่อง

Baseline

มีข้อกำหนดอะไรในการปกป้องข้อมูลสำคัญ

- ทำ baseline ความต้องการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ประเมินกระบวนการและมาตรการควบคุมความมั่นคงปลอดภัยข้อมูล
- ตรวจสอบ GAP และกำหนดแนวทางแก้ไข

Secure

จะวางแผน ออกแบบ และดำเนินการอย่างไร

- วางแผนและกำหนดลำดับความสำคัญของกระบวนการ Transformation ทางเทคนิคและกระบวนการทางธุรกิจ
- ออกแบบและดำเนินการเพื่อปกป้องข้อมูลสำคัญ ทำให้เข้าถึง และสอดคล้องกับเป้าหมายเติบโตทางธุรกิจ

Monitor

จะจัดการการปกป้องข้อมูลสำคัญอย่างไร

- พัฒนากรอบธรรมาภิบาล Risk metrics และกระบวนการเฝ้าระวัง
- ตรวจสอบกลยุทธ์และวิธีการในการปกป้องข้อมูลอย่างสม่ำเสมอ

DATA PRIVACY& PROTECTION

Implementation

แนวปฏิบัติสากล ที่อาจนำมาปรับใช้ในระหว่างรอหลักเกณฑ์

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

ISO/IEC 27701:2019

แนวปฏิบัติสำหรับ information security standards และ information security management

กำหนดความต้องการสำหรับ Information Security Management System (ISMS)

- เป็นส่วนเสริมของ ISO/IEC 27001 และ ISO/IEC 27002
- กำหนดแนวปฏิบัติของระบบการบริหารจัดการข้อมูลความเป็นส่วนตัว (PIMS) ซึ่งเกี่ยวข้องกับการประมวลผลข้อมูลที่สามารถระบุตัวบุคคลได้ (PII)
- Mapping กับ ISO/IEC 29001, 27018, 29151 รวมไปถึง GDPR

ISO/IEC 27001:2013
Information security Management System - Requirements

+

ISO/IEC 27002:2013
Code of practice for information security control

+

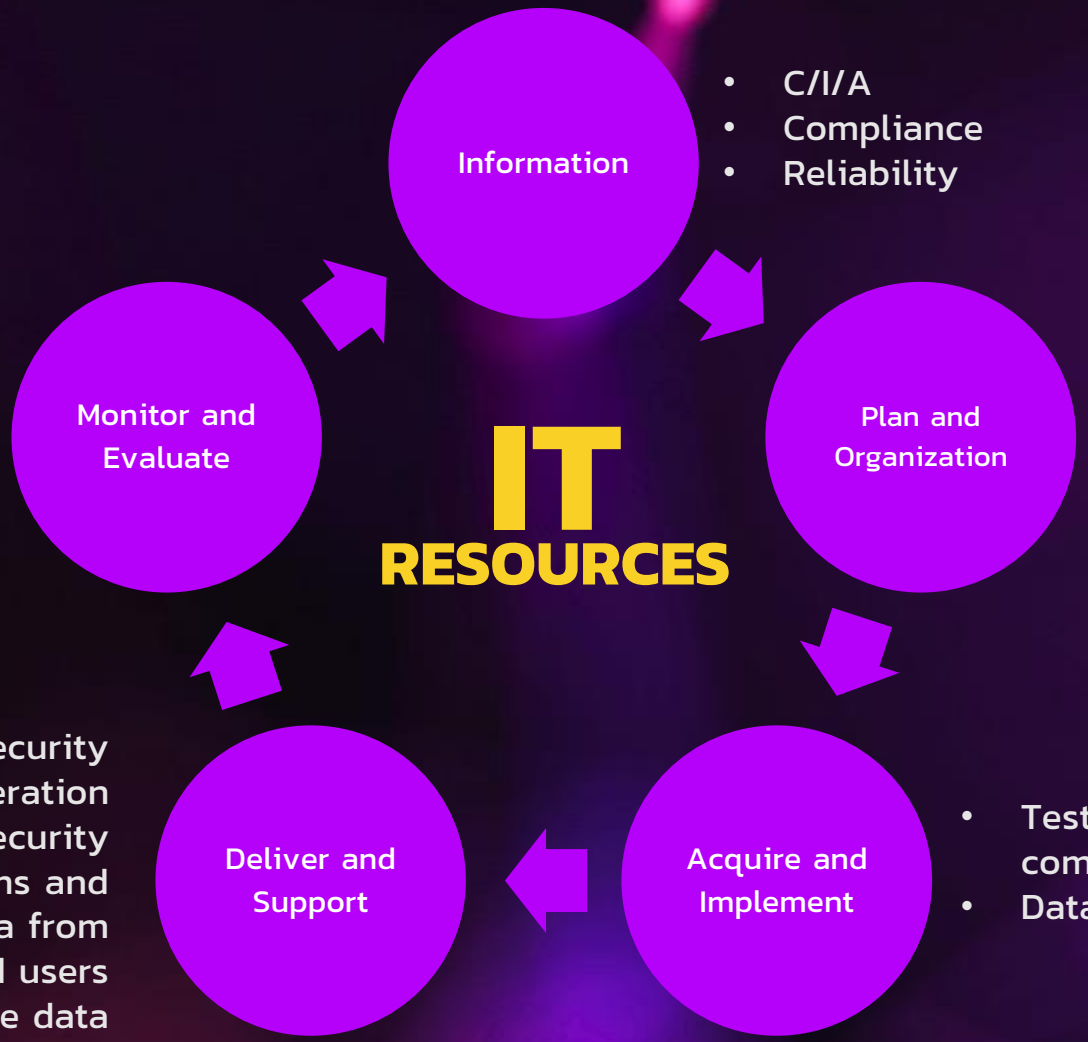
ISO/IEC 27701:2019
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information Management – Requirements and guidelines

แนะนำหัวข้อสำคัญที่ควรรู้

- 5 PIMS-specific requirements related to ISO/IEC 27001
- 6 PIMS-specific guidance related to ISO/IEC 27002
- 7 Additional ISO/IEC 27002 guidance for PII controllers
- 8 Additional ISO/IEC 27002 guidance for PII processor

The COBIT Framework : Data Relevant

Business Objectives and Governance Objectives



- C/I/A
- Compliance
- Reliability

- Assess and manage risks
- Data classification
- Define use of data/Data owner
- Data Retention
- Manage data quality

- Test data misused and compromising corporate security
- Data integrity

- Data privacy and security consideration
- Ensure system security
- Protection of IT systems and confidential data from unauthorized users
- Exchange of sensitive data

- Ensure regulatory compliance
- IT governance

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management

The Core

A set of privacy protection activities and outcomes.

Profiles

Assess current state and set the stage of "desired

Tiers

Provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk

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

Preliminary Draft
NIST Privacy Framework

Balance

<u>deriving</u>
benefits from data

<u>managing</u>
risks to individual's privacy

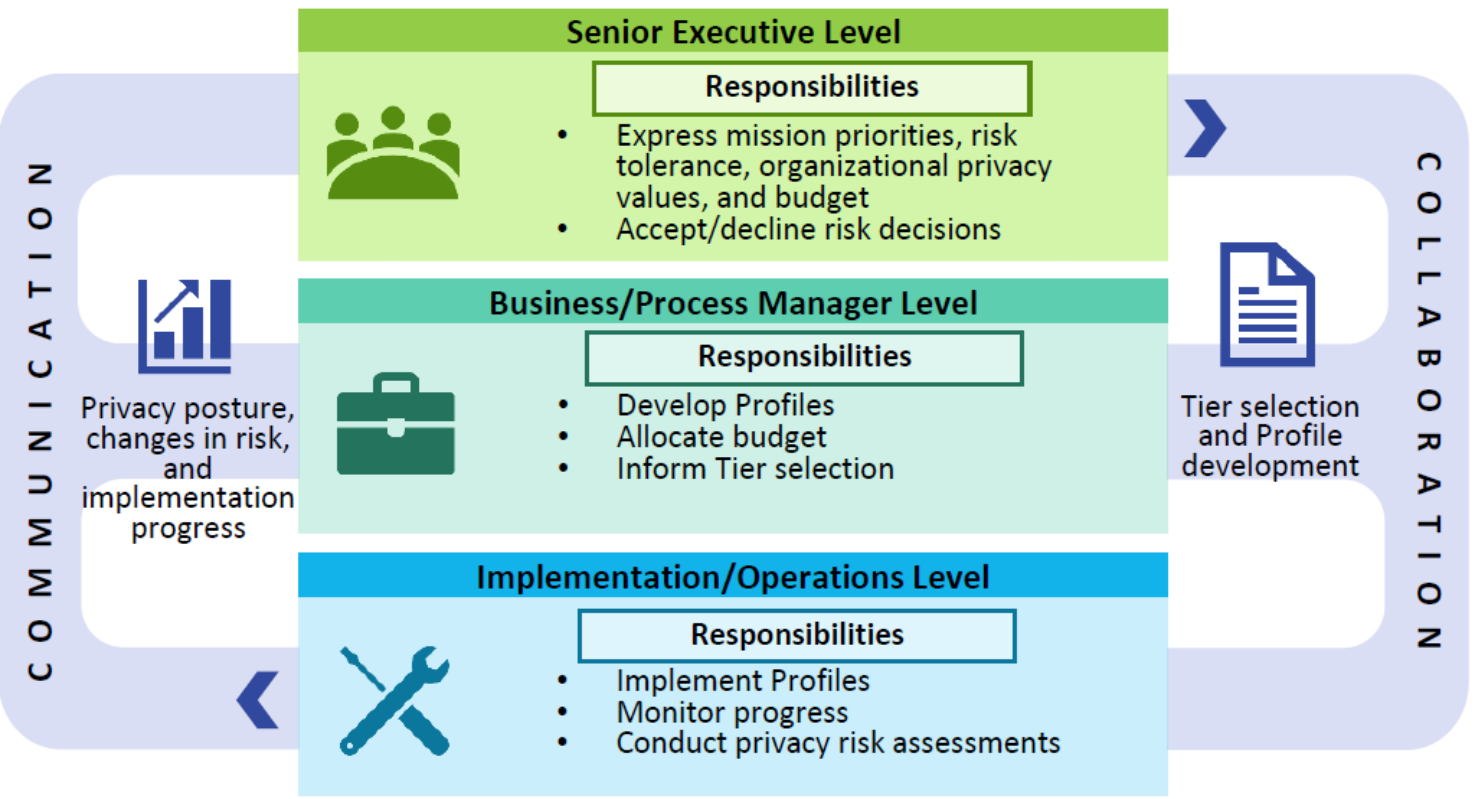
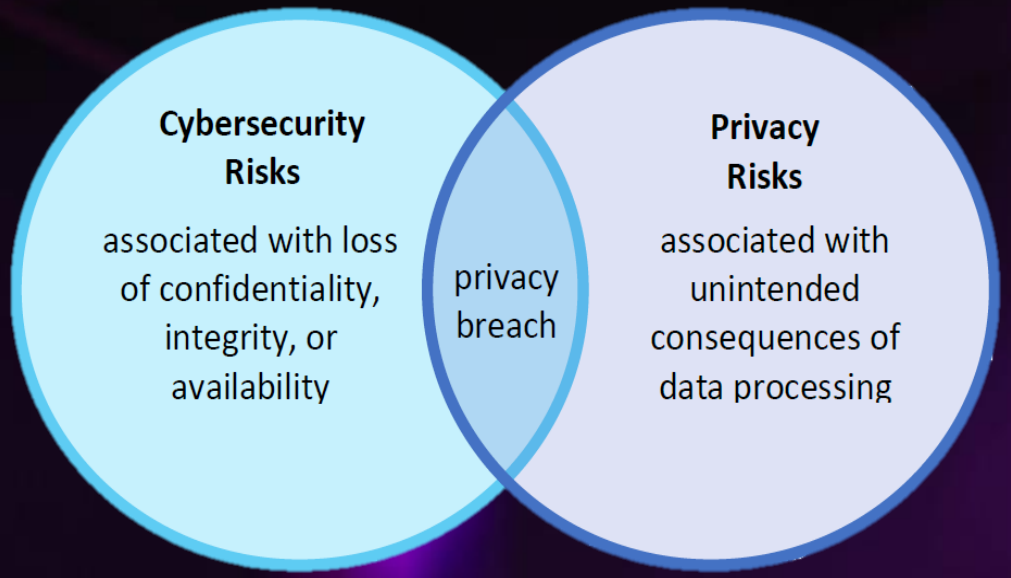


Figure 6: Notional Collaboration and Communication Flows Within an Organization

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

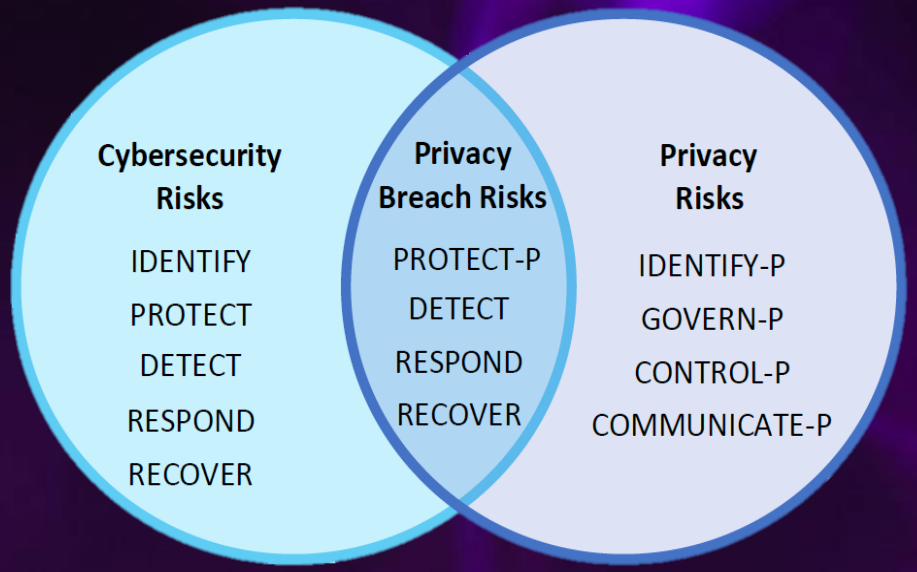
Cybersecurity and Privacy Risk Management Relationship

Cybersecurity Risk = Likelihood x Impact



Privacy Risk = Problematic Data Action x Likelihood x Impact

NIST Cybersecurity Framework



NIST Privacy Framework

Privacy risks can arise outside the scope of cybersecurity risks.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
		CT.DM-P	Data Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.DP-P	Data Protection Policies, Processes, and Procedures
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis

18 ACTIVITIES

Identify-p (id-p): develop the organizational understanding to manage privacy risk for individuals arising from data processing.

Govern-p (gv-p): develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

Control-p (ct-p): develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Communicate-p (cm-p): develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.

Protect-p (pr-p): develop and implement appropriate data processing safeguards.

Privacy by Design and Default

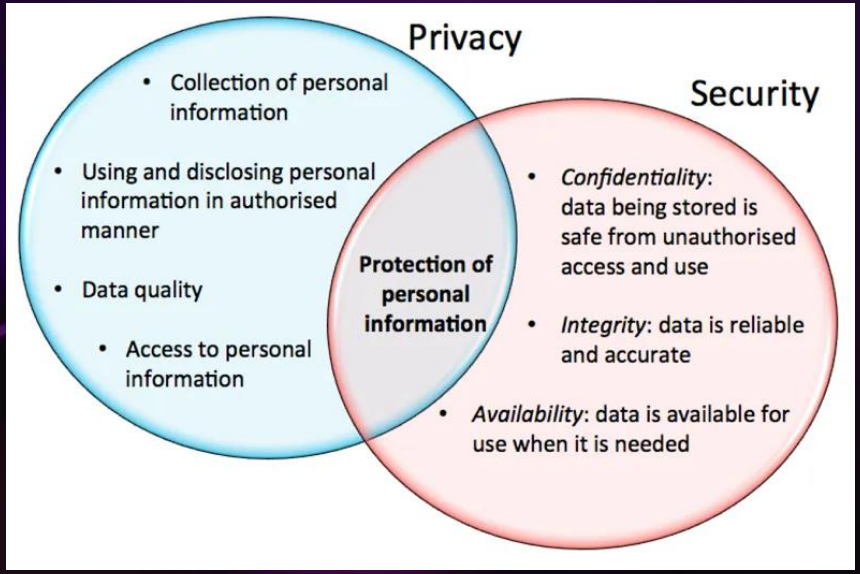
Ref: ISO/IEC 27701 Annex. A.7.4, B.8.4

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

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

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

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



ISACA Privacy Principles

ISACA Privacy Principles establish a uniform set of practical principles to give guidance on planning, implementing and maintaining a comprehensive privacy management program in the context of the wide range of enterprises.

Principle 1: Choice and Consent
Principle 2: Legitimate Purpose Specification and Use Limitation
Principle 3: Personal information and Sensitive Information Life Cycle
Principle 4: Accuracy and Quality
Principle 5: Openness, Transparency and Notice
Principle 6: Individual Participation
Principle 7: Accountability
Principle 8: Security Safeguards
Principle 9: Monitoring, Measuring and Reporting
Principle 10: Preventing Harm
Principle 11: Third Party/Vendor Management
Principle 12: Breach Management
Principle 13: Security and Privacy by Design
Principle 14: Free flow of information and legitimate restriction

ISACA Privacy Principles

ISACA Privacy Principles establish a uniform set of practical principles to give guidance on planning, implementing and maintaining a comprehensive privacy management program in the context of the wide range of enterprises.

Principle 1	**Choice and Consent**	The data controller should: ▪ Obtain implicit or explicit consent, as appropriate and according to the corresponding regulation. ▪ Ensure that appropriate and necessary consents have been obtained: • Prior to commencing collection activities • Prior to using the personal information for other purposes • Prior to the transfer of personal information to third parties
Principle 2	**Legitimate Purpose Specification and Use Limitation**	The data controller should: ▪ Describe and specify the purpose(s) for which personal information is collected in the privacy notice or other means of communication. ▪ Align the subsequent uses of the personal information with the purpose(s) provided, as well as with the consents obtained, and be in compliance with legal requirements for use limitation.
Principle 3	**Personal information and Sensitive Information Life Cycle**	The data controller should: ▪ Limit the collection, derivation, use, disclosure, transfer and retention and disposal of personal information throughout the entire information lifecycle. ▪ Minimize the personal information that is processed to only necessary for the purposes. ▪ Retain personal information for only as long as necessary to fulfill the purposes or as required by law.
Principle 4	**Accuracy and Quality**	▪ The data controller should implement practices and processes to ensure that personal information is as accurate, complete and up to date to the extent necessary for the purposes of use. ▪ Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date.

Principle 5	**Openness, Transparency and Notice**	The data controller should provide the following information to data subjects: ▪ Clear and easily accessible information about its privacy management program, policies and practices. ▪ Accurate details in the privacy notice about the personal information. ▪ Ensure that the privacy notice is provided either before or at the time of collection of personal information where practical.
Principle 6	**Individual Participation**	The data controller should provide data subjects the following rights and capabilities: ▪ A process to request confirmation from the data controller about whether or not the data controller has personal information relating to the data subjects. ▪ A process to provide data subjects with access to their personal information in an easy to understand format. ▪ A method to validate the identity of the individual. ▪ A process to provide the data subject with the opportunity to challenge the accuracy or use of personal information relating to him/her.
Principle 7	**Accountability**	The data controller should: ▪ Identify privacy stakeholders and applicable legal requirements, and implement privacy frameworks to support risk mitigation and legal compliance. ▪ Analyze, assess and manage privacy risk throughout the enterprise. ▪ Assign roles, responsibility, accountability and authority for performing privacy risk management processes. ▪ Identify and inventory personal information and business processes that involve such information.
Principle 8	**Security Safeguards**	The data controller should: ▪ Identify appropriate security safeguards, based upon identification of privacy risks, which align with all existing information security policies and applicable laws and regulations. ▪ Establish security safeguards that include administrative, technical and physical security controls and that address confidentiality, integrity and availability of information.

Principle 9	**Monitoring, Measuring and Reporting**	The data controller should: ▪ Establish a framework for measuring and monitoring the following: • Effectiveness of the privacy management program • Level of compliance with applicable policies, standards and legal requirements • Use and implementation of privacy tools • Types and numbers of privacy breaches that occur • Privacy risk areas within the data controller • Third parties that have access to personal information and the associated risk levels ▪ Report compliance with privacy policies, applicable standards and laws to key stakeholders. ▪ Integrate internationally accepted privacy practices into business practices.
Principle 10	**Preventing Harm**	The data controller should: ▪ Design the implementation of controls for personal information to prevent misuse of that information, which can result in harm to the individuals. ▪ Establish processes to mitigate any personal harms that occur to data subjects as a result of privacy breaches.
Principle 11	**Third Party / Vendor Management**	The data controller should: ▪ Implement governance and risk management processes and apply contractual, administrative and audit measures to ensure the protections and use of personal information by all associated third parties. ▪ Require all third parties with any type of access to personal information to report personal information breaches in a timely manner to the data controller.

Principle 12	**Breach Management**	The data controller should: ▪ Establish a policy and procedure for identifying, escalating and reporting incidents of personal information breaches to data subjects and relevant authorities, as necessary, in a timely manner. ▪ Maintain records of all personal information breaches, remediation and monitoring the progress until the incident is closed. ▪ Implement remediation actions to prevent reoccurrence of personal information breaches of a similar nature.
Principle 13	**Security and Privacy by Design**	The data controller should: ▪ Establish an enterprise privacy policy describing the privacy philosophy for the data controller to ensure the evaluation of the impact to the security and privacy of personal information. ▪ Communicate executive support for the privacy enterprise-wide roles and responsibilities during the implementation of IT systems and launch of enterprise programs and operations.
Principle 14	**Free flow of information and legitimate restriction**	The data controller should: ▪ Establish a framework to govern the transfer of personal and sensitive information outside of the jurisdiction of the data controller to ensure the level of security and privacy protections. ▪ Document the security and privacy protection requirements for the data processor to implement within other jurisdictions. ▪ Maintain records of all personal information transferred into and out of the data controller's jurisdiction.

Phase	Assess	Design	Transform	Operate	Conform
Activity	• ประเมินความเสี่ยงและความพร้อมในการดูแลข้อมูลส่วนบุคคล • แผนเตรียมพร้อมตาม GDPR • ระบุข้อที่อยู่ของข้อมูลส่วนบุคคล **IBM Case Study**	• วางแผนการอบรม แผนการสื่อสารและมาตรฐานที่เกี่ยวข้อง • กำหนดมาตรฐานการจัดการข้อมูลและบริหารความมั่นคงปลอดภัยของข้อมูล	• พัฒนาขั้นตอนการปฏิบัติและเครื่องมือที่จำเป็น • จัดอบรม GDPR • พัฒนาระบบในลักษณะ Privacy by Design และ Security by Design	• นำไปปฏิบัติกับธุรกิจที่เกี่ยวข้อง • เฝ้าระวังด้านความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคลด้วยมาตรการทางเทคนิคและการจัดการ (TOMs) • จัดการความยินยอมและสิทธิในการเข้าถึงข้อมูล	• เฝ้าระวัง ประเมิน ตรวจสอบ รายงานความสอดคล้องกับ GDPR
Outcome	**Assessments and roadmap**	**Defined implementation plan**	**Process enhancements completed**	**Operational framework in place**	**Ongoing monitoring and reporting**
	ระบุผลกระทบจาก GDPR และวางแผนมาตรการทางเทคนิคและการจัดการ (Technical and Organizational Measures: TOMs)	มาตรการคุ้มครองข้อมูลส่วนบุคคล ที่ต้องปฏิบัติ	TOMs : การระบุข้อมูลส่วนบุคคล การจัดแบ่งประเภท และการจัดการและอภิบาลข้อมูล	เริ่มใช้ขั้นตอนการปฏิบัติใหม่ตาม GDPR	เฝ้าระวังการปฏิบัติตาม GDPR และรายงานผลการปฏิบัติให้ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกรับทราบ

Source: IBM's GDPR Readiness, Data Responsibility

WORKING TO A PLAN

คุณได้รับผลหรือไม่

→ **องค์กรได้มีการประมวลผล การจัดเก็บ** และการจัดการข้อมูลที่สามารถระบุตัวบุคคลได้ หรือข้อมูลส่วนบุคคล (หรือมีแผน) หรือไม่

NO → **หยุด** (แล้วแต่กรณี)

YES → **ข้อมูลที่สามารถระบุตัวบุคคลได้**ดังกล่าวเป็นของคนที่มีถิ่นพำนักใน EU ซึ่งรวมถึงลูกค้าและ/หรือลูกจ้าง ใช่หรือไม่

YES → **คุณได้เริ่มการคุ้มครองข้อมูลส่วนบุคคล**ตาม GDPR แล้วหรือไม่

NO → **ให้ความรู้** เกี่ยวกับ GDPR

YES → **คุณได้ประเมินความเสี่ยง** หรือวิเคราะห์เกี่ยวกับ GDPR แล้วหรือไม่

→ **ประเด็นที่คุณกังวลมากที่สุด**

กำหนดแผนของท่าน

- **การตอบสนองเมื่อเกิดเหตุการณ์ละเมิด** (Breach Response)
  - คุณจัดการความเสี่ยงจากภัยคุกคามหรือการโจมตีทางไซเบอร์ขั้นสูงอย่างไร
    - กลยุทธ์ใดของท่านที่ใช้ในการระบุและตอบสนองเมื่อเกิด data breach
      - ขั้นตอนอัตโนมัติที่ใช้ในการลดระยะเวลาที่ breach exposure
- **Data Governance**
  - คุณมีรายการการประมวลผลข้อมูลที่ถูกต้องหรือไม่
    - กลยุทธ์ใดของท่านที่ใช้ยืนยันว่าการเข้าถึงข้อมูลส่วนบุคคลมีความเหมาะสมและอยู่ภายใต้การควบคุม
      - คุณกำหนดนโยบายเกี่ยวกับ Data Governance อย่างไร
- **การประเมินความเสี่ยง** (Risk Assessment)
  - ในกรณีปกติ องค์กรของท่านจัดการกับการประเมินความเสี่ยงอย่างไร
    - องค์กรของท่านมีกลยุทธ์ในการบริหารจัดการความเสี่ยงที่ครอบคลุมหรือไม่
      - การคุ้มครองข้อมูลส่วนบุคคลอยู่ภายในขอบเขตของกลยุทธ์ในการบริหารจัดการความเสี่ยงส่วนใด
- **การบริหารจัดการการปฏิบัติตามกฎระเบียบ** (Compliance Management)
  - ในกรณีปกติ องค์กรของท่านจัดการกับการปฏิบัติตามกฎระเบียบอย่างไร
    - ท่านมีวิธีการระบุ จัดลำดับความสำคัญ และติดตามการปฏิบัติตามกฎระเบียบอย่างไร
      - ท่านมีวิธีจัดรายการข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้อง รวมทั้งข้อกำหนดตามกฎระเบียบอย่างไร

Source: RSAConference 2018

ตัวอย่าง Transparency

Implement

(PDPA ม. 23) (GDPR Art 12 Transparency) (ISO 27701:2019 “7.3.3”)

วิธีการแจ้งข้อมูล

- ใช้ถ้อยคำกระชับ ชัดเจน เข้าใจง่าย
- ครบถ้วน โปร่งใส และ up to date
- รูปแบบเข้าถึงง่าย ระยะเวลาเหมาะสม
- แจ้งก่อน หรือขณะเก็บข้อมูล

ตัวอย่างข้อมูลที่แจ้ง

- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล
- สิทธิเจ้าของข้อมูล
- หน้าที่ของผู้ควบคุมข้อมูล
- ข้อมูลเกี่ยวกับการประมวลผล

ตัวอย่าง Checklist Assessment

- **Organization data**
  - บันทึกรายการข้อมูลต่าง ๆ เช่น การได้มาซึ่งข้อมูล หมวดหมู่ของข้อมูล วัตถุประสงค์การประมวล
  - ตรวจสอบและจัดทำเอกสาร เช่น Form การขอคำยินยอม
  - จัดทำ DP Policy และมีการทบทวน
- **Employee data**
  - HR มีนโยบายและวิธีการบริหารจัดการข้อมูลพนักงาน
  - มีขั้นตอน และนโยบายเกี่ยวกับวิธีการจัดการข้อมูลของลูกค้าให้พนักงานทราบ

- **Customer data**
  - เผยแพร่ Privacy Policy
  - มีนโยบายและกระบวนการต่าง ๆ เช่น customer marketing protocols / consents / Cooking / online tracking / Data Subject right
- **Privacy by design**
  - มีการออกแบบตาม guidance principles

Data transfers to third parties

- มีนโยบายและกระบวนการต่าง ๆ เช่น data sharing to other controller & processor

ตัวอย่าง Data Breach

Implement

(PDPA มาตรา 37 (4) การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล)
(GDPR Art 33 การแจ้ง Supervisory Authority, 34 การแจ้งเจ้าของข้อมูล)
(ISO/IEC 27701:2019 "**7.3.3**")

แนวทางการรับมือภัยคุกคาม Incident Management เช่น

1. แต่งตั้ง **"ผู้รับผิดชอบ"** และกำหนด **"กระบวนการ"** เกี่ยวกับ
   - 1.1 การวินิจฉัยเหตุการละเมิดข้อมูล PII
   - 1.2 การจัดทำบันทึกเหตุการละเมิดข้อมูล PII
   - 1.3 การแจ้งเตือนผู้ที่เกี่ยวข้อง
   - 1.4 การเปิดเผยข้อมูลต่อ authorities

2. **ตอบสนอง**เหตุการละเมิดข้อมูล PII ในฐานะ <u>ผู้ควบคุมข้อมูล</u>และ<u>ผู้ประมวลผลข้อมูล</u>
   - 2.1 ตรวจสอบเหตุคุกคามว่าเกี่ยวกับการละเมิดข้อมูล PII หรือไม่
   - 2.2 หากเกี่ยวกับการละเมิดข้อมูล PII ให้ดำเนินการ
     - **2.2.1 แจ้งเตือน**
     - **2.2.2 จัดทำบันทึกเหตุละเมิดข้อมูล PII**

ตัวอย่าง Checklist Assessment

- จัดทำและบังคับใช้กระบวนการ Data Breach เช่น ทำรายงาน การจัดการ การแก้ไขปัญหา
- มีขั้นตอนในการรายงาน Data Breach ให้หน่วยงานกำกับดูแล ภายใน 72 ชั่วนับแต่ทราบเหตุ
- มีขั้นตอนการเก็บรักษาและจัดทำรายงาน Data Breach
- กำหนดขั้นตอนการรายงาน Data Breach ภายในองค์กร

ตัวอย่างแนวปฏิบัติ

ของ 4 บริษัทยักษ์ใหญ่

Microsoft

facebook

aws

Google

Microsoft

วิธีการรับมือ GDPR ของ Microsoft

1 ระบุขอบเขตที่แน่ชัดของ GDPR

- **ออก a self-service privacy portal** สำหรับลูกค้าเพื่อขอสำเนาและลบข้อมูลส่วนบุคคลที่ใช้สำหรับบริการ Cloud
- **สร้าง Data Inventory** ข้อมูลส่วนบุคคล
- **ใช้โครงสร้างพื้นฐานเพื่อสร้าง data schema** ให้เป็นมาตรฐาน, ทำให้เป็นอัตโนมัติและบังคับใช้นโยบายความเป็นส่วนตัว
- **ทบทวนและกำหนดมาตรฐานนโยบายการเก็บรักษาข้อมูล**ในธุรกิจระบบและพันธมิตร / ซัพพลายเออร์
- **อัปเดตเอกสารต่าง ๆ ที่เกี่ยวข้อง** เช่น เอกสารทางเทคนิค สัญญาการให้บริการต่าง ๆ ให้สอดคล้องตาม GDPR
- **ตรวจสอบข้อกำหนด**ความเป็นส่วนตัวของข้อมูลและการสร้างข้อกำหนดในการปฏิบัติตาม กระบวนการจัดซื้อ

2 จัด Training และ Workshop ให้กับทีมงาน

- **จัดการสัมมนา, workshop** ออนไลน์ เพื่ออบรมพนักงานเจ้าหน้าที่ภายในบริษัท คู่ค้า และ Vendors
- **จัด Train-the-trainer programs** เพื่อเพิ่มขีดความสามารถให้กับผู้เชี่ยวชาญเฉพาะด้าน
- **จัดทำเอกสารรายละเอียด**แนะนำการใช้งานผลิตภัณฑ์และบริการ เพื่อการปฏิบัติตาม GDPR

3 ปรับปรุงข้อกำหนดของกฎความเป็นส่วนตัว

- ✓ ตั้ง “ทีมกลาง” ที่ประกอบทั้ง ระดับผู้บริหาร, เจ้าของโปรแกรม Privacy ผู้จัดการด้าน Privacy และฝ่ายวิศวกรรม เพื่อทำ framework ที่ครอบคุลมนโยบาย, กระบวนการทางเทคนิค, โครงสร้างพื้นฐานและประสบการณ์ของลูกค้า (Customer Experiences)

4 ลงทุนกับเทคโนโลยีใหม่

- ✓ สร้างระบบอัตโนมัติ เพื่อเป็นมาตรฐานให้กับข้อมูล นำไปสู่การกำกับดูแลง่ายขึ้น

ตัวอย่างการทำงาน

- **ใช้โปรแกรม** Power BI เพื่อควบคุม GDPR Workstream Dashboard เพื่อให้การทำงานของทีมเชื่อมโยงกัน

- **อัพเดตเอกสารทางเทคนิค**ใน Service Trust Portal เพื่อให้คำแนะนำเกี่ยวกับวิธีการจัดการข้อมูลส่วนบุคคลบนคลาวด์ และความรู้เรื่องมาตราฐานความปลอดภัย ที่สอดคล้องกับการใช้งาน Microsoft ให้กับลูกค้า

Facebook

วิธีการรับมือ GDPR ของ Facebook

1. **ทำงานร่วมกับผู้เชี่ยวชาญ**เพื่อออกแบบ Privacy ผลิตภัณฑ์ของบริษัท (Privacy by Design)
   - **มีทีมงานด้าน Privacy** ที่ประกอบด้วย ผู้เชี่ยวชาญด้านต่าง ๆ ทำงานประจำ
     เช่น หน่วยงานกำกับ (regulator), policymakers, ผู้เชี่ยวชาญด้านความเป็นส่วนตัว (privacy experts) และ นักวิชาการจากทั่วโลก เพื่อให้ผู้เชี่ยวชาญทุกกลุ่มทราบถึงขั้นตอนการดำเนินการของบริษัท รวมถึงรับข้อเสนอแนะและนำมาพัฒนาเรื่องการปกป้องข้อมูลส่วนบุคคล
   - **พัฒนาการ control และ design privacy** ตลอดเวลา
     โดยลงทุนทำการศึกษาวิจัยและทำงานร่วมกับผู้เชี่ยวชาญ
     ทั้ง designers, developers, privacy professionals และ regulators.
   - **พัฒนา design privacy กับผลิตภัณฑ์ของบริษัท ตั้งแต่ขั้นตอนแรกตามคำแนะนำของผู้เชี่ยวชาญด้านต่าง ๆ**
     เช่น Data Protection, Privacy Law, Security, Interface design, engineering, product management และ public policy โดยทีม privacy ของบริษัทได้มีการทำงานในหลากหลายมิติเหล่านี้ในทุกขั้นตอนของการพัฒนาผลิตภัณฑ์

Facebook

วิธีการรับมือ GDPR ของ Facebook

2. ปรับปรุงข้อกำหนดของความเป็นส่วนตัว

- **กำหนด Privacy Principles** เพื่อชี้แจงให้ผู้ใช้งานได้ทราบถึงข้อกำหนดความเป็นส่วนตัวและการนำข้อมูลของผู้ใช้งานไปใช้งาน
  เพื่อให้ทราบว่า Facebook เข้าถึงความเป็นส่วนตัวของผู้ใช้งานอย่างไร
- **ให้สิทธิในการควบคุม**ความเป็นส่วนตัวแก่ผู้ใช้งาน
- **ออกแบบความเป็นส่วนตัว**ในผลิตภัณฑ์ของบริษัทตั้งแต่ขั้นตอนแรก
- ผู้ใช้งานสามารถลบข้อมูลของตัวเองได้
- มีการปรับปรุงข้อกำหนดตลอดเวลา ให้ทันสมัย สอดคล้องกับ GDPR
- แสดงให้เห็นว่า มีการทำ privacy policy ที่เชื่อถือได้

Amazon : AWS (Amazon Web Service)

บฏิบัติตาม **GDPR, EU-US Privacy Shield และยังทำตามข้อกำหนดอื่น** เช่น **หลักจรรยาบรรณของ CISPE** (Cloud Infrastructure Services Providers in EU) เพื่อรับรองว่า สินค้าบริการของ AWS สอดคล้องกับ GDPR และข้อปฏิบัติอื่น ๆ อีกด้วย เช่น **ISO 27017 ปลอดภัยของคลาวด์, ISO 27018 ความเป็นส่วนตัวในระบบคลาวด์**

ขั้นตอนที่ AWS มีการ Comply ตาม GDPR

- การระบุขอบเขต ความรับผิดชอบของผู้ให้บริการ (บริการโครงสร้างพื้นฐานระบบคลาวด์)
- ตรวจสอบมาตรการทางเทคนิค และปรับแก้ให้ทันสมัยอย่างสม่ำเสมอ
- การเสนอบริการให้ลูกค้า – เพื่อให้สอดคล้องกับ GDPR :
  - ควบคุมการเข้าถึง : ผู้ดูแลระบบ ผู้ใช้ Application ที่เข้าถึง
  - ติดตามและบันทึกการเปลี่ยนแปลง
  - เข้ารหัส (การเข้ารหัสข้อมูลบน AWS)
  - จัดให้มี Framework การปฏิบัติตามข้อกำหนดและมาตรฐานด้านความปลอดภัย เช่น ISO 27001/9001, 27017/27018, C5, AWS TüV TRUST IT

- ระบุ**สิทธิของเจ้าของข้อมูล**
- **แจ้งเตือนการรั่วไหลของข้อมูล (Data Breach Notification)** มีวิธีการควบคุมการรั่วไหล, ต้องทำภายใน 72 ชม., การกำหนดแนวทางว่าต้องแจ้งหน่วยงานกำกับ, คนที่ได้รับผลกระทบ
- แต่งตั้ง**เจ้าหน้าที่ฝ่ายปกป้องข้อมูล (DPO)**
- **ประเมินผลกระทบของการปกป้องข้อมูล (APIA)**
- กำหนด**ข้อตกลงการประมวลผลข้อมูล (DPA)** โดยเฉพาะการโอนข้อมูลส่วนบุคคลไปภายนอกเขตเศรษฐกิจยุโรป

วิธีการรับมือ GDPR ของ Google

1. อัพเดต terms และ contractual protections
2. ทำ Client Checklist
3. เสริมสร้างการทำ Safeguards ให้แข็งแรงมากขึ้น
4. มี Incident Response ที่รองรับเวลาเกิดเหตุ ภัยคุกคาม
5. สร้างความโปร่งใสในการใช้ข้อมูลของผู้ใช้ (User Transparency)
6. รับการรับรองตาม Privacy Shield ระดับสากล เช่น EU-US Shield และมาตรฐานสากลอื่น ๆ

1 อัพเดต terms และ contractual protections

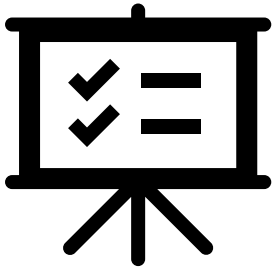
- อัพเดต terms ให้สอดคล้องกับกฎเกณฑ์และข้อบังคับ ให้เป็นปัจจุบัน เพื่อให้การให้บริการ สินค้าและบริการต่าง ๆ ของ Google มีความทันสมัย

- Publisher และ Advertiser ต้องปฏิบัติตามหลักเกณฑ์ที่ Google กำหนด เช่น การให้ความยินยอมตาม EU User Consent Policy ของ Google และการขอความยินยอมจากผู้ใช้ EEA สำหรับการโฆษณาและการใช้ cookies บนเว็บไซต์และ Application

2 ทำ Client Checklist

key area ที่ต้องคำนึงถึงในการทำ Checklist เช่น

- หน่วยงานของท่านมี**การรับรองความโปร่งใสของผู้ใช้ (User Transparency)** และการควบคุมการใช้ข้อมูลอย่างไร ท่านได้อธิบายประเภทของข้อมูลที่เก็บหรือไม่ และเก็บไปเพื่ออะไร
- องค์กรของท่านใช้วิธีการ**ให้ความยินยอมที่ถูกต้อง (Right consents)** หรือไม่ (ตาม GDPR, Google EU User Consent Policy)
- **การบันทึกการตั้งค่าของผู้ใช้ (User preference)** และการให้ความยินยอม ทำเป็นระบบถูกต้องหรือไม่
- มี**วิธีการแสดงให้หน่วยงานกำกับตามกฎหมาย และ Partners** ของท่านเห็นได้อย่างไร ว่าท่านเป็นหน่วยงานที่น่าเชื่อถือและได้ปฏิบัติตาม GDPR



3 เสริมสร้างการทำ Safeguards ให้แข็งแรงมากขึ้น

จัดให้มีการรักษาความปลอดภัย :

- ป้องกันความปลอดภัยของข้อมูลครอบคลุมองค์กร
- แต่งตั้งทีมรักษาความปลอดภัยโดยเฉพาะและทีมรักษาความเป็นส่วนตัว
- จัดให้มีการ audit อย่างสม่ำเสมอ, เป็นประจำปี โดยผู้ตรวจสอบภายนอก (3rd Party Auditor)

4 มีการทำ Incident Response

- เตรียมการ Advanced Threat Detection และ Avoidance Technology
- จัดให้มีโปรแกรมการจัดการตอบสนองต่อเหตุการณ์ และภัยคุกคามต่าง ๆ

5 สร้างความโปร่งใสในการใช้ข้อมูลของผู้ใช้งาน (User Transparency)

Google

- สร้างความโปร่งใสเกี่ยวกับการใช้ข้อมูลในสินค้าโฆษณา
- โดย Google ขออนุญาต (permission) เมื่อมีการใช้ข้อมูลเพื่อการโฆษณาและแสดงความโปร่งใสแบบ real-time ผ่าน “Why This Ad”
- Google จะแจ้งผู้ใช้งานผ่าน Google Account ว่า มีการบันทึกข้อมูลของผู้ใช้อะไรบ้าง (ผู้ใช้จะสามารถควบคุมการใช้ข้อมูลสำหรับการโฆษณาได้)

6 รับรองตาม Privacy Shield ระดับสากลอื่น ๆ อีก

เช่น การรับรองภายใต้ EU-US และ Swiss-US Privacy shield

และยังทำตามมาตรฐานอื่น ๆ เช่น
ISO 27001 (Information Security Management)
ISO 27017 (Cloud Security)
ISO 27018 (Cloud Privacy)
SSAE16 / ISAE 3402
FedRAMP
PCI DSS (Payment Card Industry Data Security Standard)

การเตรียมความพร้อมรองรับการบังคับใช้ PDPA รวมทั้ง Law com ภายใต้กฎหมายฉบับอื่น

เจ้าของข้อมูล	ตระหนักในสิทธิของตัวเอง
ผู้ประกอบการรายเล็ก	• คำนึงถึงบทบาทหน้าที่ของผู้ที่เกี่ยวข้อง • จัดทำแนวปฏิบัติตามข้อกำหนดเท่าที่จำเป็น
ผู้ประกอบการรายใหญ่	• comply ตาม best practice ที่ควรจะเป็น • มีทั้ง internal audit และ external audit
ภาครัฐ	คำนึงถึงกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่ง • กม.ธุรกรรมฯ ที่ต้องแก้ไขให้สอดคล้อง • Data governance ภายใต้ กม.สพร. • การเปิดเผยข้อมูลตาม กม.ข้อมูลข่าวสารฯ
บริการที่ถูกกำกับดูแล	• ปฏิบัติตามกฎหมายอย่างเคร่งครัด • meet International Standard

การทำงานอย่าง**ใกล้ชิดระหว่าง Regulator** ที่เกี่ยวข้อง เป็นสิ่ง**สำคัญและจำเป็น** เพื่อสร้างความชัดเจน และความสอดคล้อง

Law enforcement ต้องแน่ใจว่าเป็นไปเพื่อ **คุ้มครองสิทธิขั้นพื้นฐาน** ของประชาชน ไม่เป็นภาระเกินสมควร และ **ไม่ก่อให้เกิดข้อจำกัด ต่อการเติบโตของ Technology และ Innovation**

THANK YOU

www.ETDA.OR.TH

Facebook: ETDA Thailand

Facebook: Surangkana Wayuparb