การสัมมนา
เรื่องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสำหรับสหกรณ์
27 พฤษภาคม 2565
โรงแรมลองบีช ชะอำ จังหวัดเพชรบุรี
เวลา 9:00-12:00 น.

บรรยายโดย ดร.ดวงกมล ทรัพย์พิทยากร
Senior IT Security Specialist
บริษัท ที-เน็ต จำกัด

แนะนำตัวผู้บรรยาย

บจ. ที-เน็ต จำกัด

ดร.ดวงกมล ทรัพย์พิทยากร

ชื่อเล่น: เกด

- ตำแหน่งปัจจุบัน Senior IT Security Specialist
  บจ. ที-เน็ต จำกัด
- ใบประกาศ, วุฒิบัตร (CERTIFICATE)
- CISA (Certified Information Systems Auditor)
- EXIN Privacy and Data Protection Foundation
- EXIN Information Security Foundation based on ISO/IEC 27001
- ISO/IEC 27701, PIMS Implementer
- ISO/IEC 27001 ISMS Lead Auditor
- ISO/IEC 20000 SMS Lead Auditor
- ISO/IEC 22301 BCMS Lead Auditor
- CompTIA Security +
- บทบาทหน้าที่ในปัจจุบัน เป็นที่ปรึกษาด้าน Information Security และด้าน PDPA ให้กับองค์กรชั้นนำทั้งภาครัฐและเอกชน และหน่วยงานกำกับดูแล

วัตถุประสงค์การอบรม

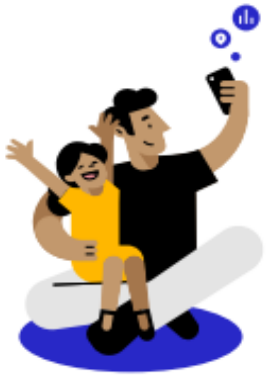
- เพื่อให้บุคลากรของชุมนุมสหกรณ์ออมทรัพย์ประเทศไทยมีความรู้ความเข้าใจในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรอบรู้ถึงภัยคุกคามทางไซเบอร์ที่อาจส่งผลต่อการละเมิดข้อมูลส่วนบุคคล รวมถึงมาตรการรักษาความมั่นคงปลอดภัยที่จำเป็น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ๒๕๖๒

Personal Data Protection Act B.E. 2019 (PDPA)

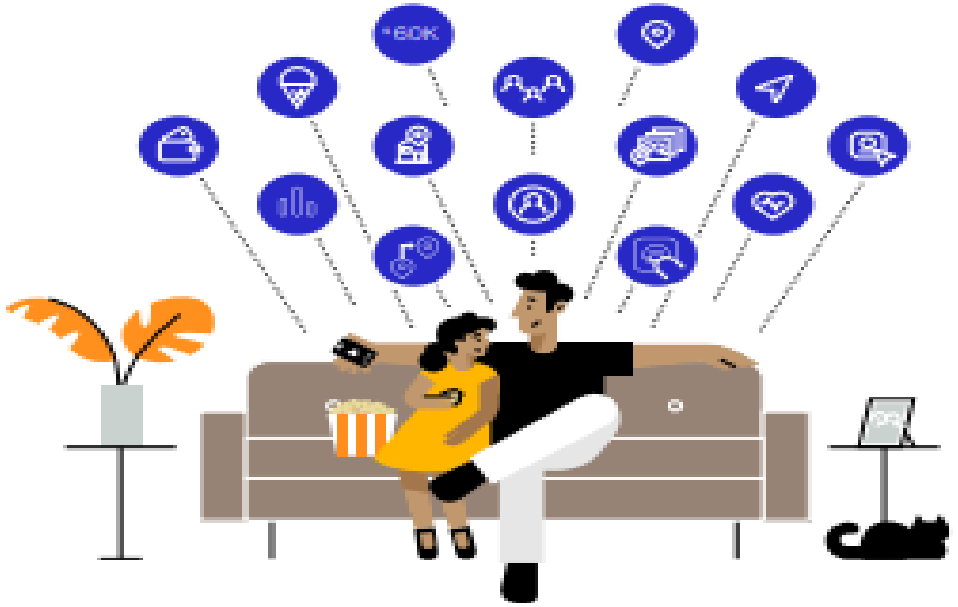
Last update: 30 Mar. 2022



ในหนึ่งวันเกิดอะไรขึ้นกับข้อมูลของคุณบ้าง

หนึ่งวันของคุณพ่อและลูกสาวที่สนามเด็กเล่

เมษายน 2021



"ผมเชื่อว่าคนเราฉลาด และบางคนก็อยากแชร์ข้อมูลมากกว่าคนอื่นๆ ดังนั้นเราจึงควรถามถามทุกครั้ง จนกว่าพวกเขาจะเบื่อกับการถูกถามและบอกให้คุณหยุด บอกให้พวกเขารู้อย่างตรงไปตรงมาว่าคุณกำลังจะทำอะไรกับข้อมูลของพวกเขาบ้าง"

Steve Jobs

การประชุม All Things Digital ปี 2010

เมื่อจบวัน หลายบริษัททั่วโลกที่ John ไม่เคยโต้ตอบด้วยเลยต่างก็พากันอัปเดตข้อมูลในโปรไฟล์เกี่ยวกับตัวเขาและลูกสาว กลายเป็นว่าบริษัทเหล่านี้รู้ทั้งตำแหน่งที่อยู่บ้านของครอบครัว สวนสาธารณะที่พวกเขาไป เว็บไซต์ข่าวที่อ่าน ผลิตภัณฑ์ที่เลือกชม โฆษณาที่ดู ลักษณะนิสัยในการซื้อสินค้า และร้านที่ไป[3,4] เพราะข้อมูลเหล่านี้ถูกเก็บและติดตามข้ามแอปต่างๆ ที่ John และลูกสาวใช้งานตลอดทั้งวัน รวมถึงจากแหล่งอื่นๆ ด้วย โดยที่ John ไม่รู้เลยว่ามีการเก็บข้อมูลไปมากแค่ไหนตลอดวันนั้น อีกทั้งยังไม่สามารถควบคุมเรื่องนี้ได้ทุกครั้ง หรือไม่รู้ตัวเลยด้วยซ้ำว่าเคยอนุญาตไปเมื่อไหร่[5,6] ซึ่งเมื่อสองพ่อลูกกลับมาพักผ่อนที่บ้านในตอนเย็นแล้วค้นหาภาพยนตร์สำหรับเด็กในแอปบนสมาร์ททีวี วงจรการติดตาม การแลกเปลี่ยนข้อมูล การประมูล และการย้ำกลุ่มเป้าหมายนั้นก็ยังคงวนเวียนต่อไปไม่จบสิ้น[7,8]

https://www.apple.com/th/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf?fbclid=IwAR2XxKkHbXYj5722EGyJLLyPBR75hbe22gEI5FZ3lJnpeavYBeyHGTs_CqM

Privacy Note ได้ศึกษาข้อมูล จากฐานข้อมูลการละเมิดกฎหมายข้อมูลส่วนบุคคลของกลุ่มธุรกิจสื่อสารจำนวน 180 รายการ พบสาเหตุหลายประการที่เป็นเหตุทำให้เกิดการละเมิด ซึ่งเป็นกรณีศึกษาที่ ธุรกิจสื่อสารควรตระหนักเพื่อป้องกันไม่ให้เกิดขึ้นกับธุรกิจของตนดังนี้

1.ถูกแอบอ้างชื่อไปใช้ในการเปิดบริการเบอร์โทรศัพท์จำนวนหลายเบอร์แล้วถูกเรียกเก็บเงิน

2.ถูกโอนสายอัตโนมัติไปให้ผู้อื่น โดยที่เจ้าของเบอร์ไม่ได้อนุญาต

3.ส่งอีเมลผิดส่งหรือส่งใบแจ้งหนี้ไปผิดที่อยู่ ....

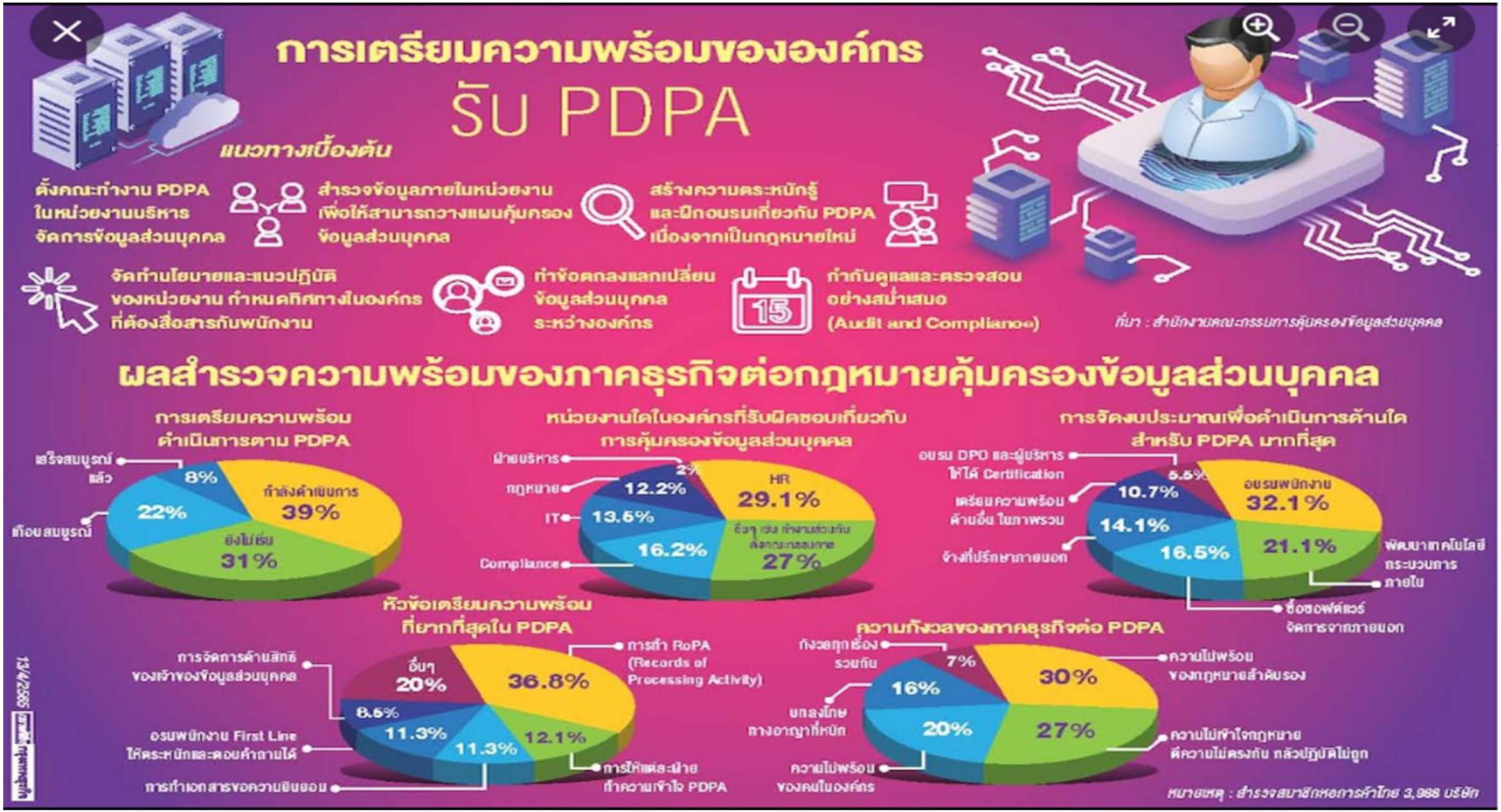
ที่มา : https://www.enforcementtracker.com

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสาธารณรัฐเฮลเลนิก ซึ่งเป็นประเทศที่ตั้งอยู่ทางตะวันออกเฉียงใต้ของทวีปยุโรป สั่งปรับเจ้าของโรงเรียนสอนภาษาจำนวน 2000 ยูโร หรือประมาณ 7.3 หมื่นบาท

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประเทศอิตาลี สั่งปรับบริษัท ClearView AI ซึ่งเป็นบริษัทเทคโนโลยี AI ในประเทศสหรัฐอเมริกาจำนวน 20,000,000 ยูโร หรือประมาณ 738 ล้านบาท หลังจากพบว่า บริษัทดังกล่าวได้มีการนำเอาเทคโนโลยีตรวจจับทางชีวมิติ (Biometric) มาใช้ในประเทศอิตาลี

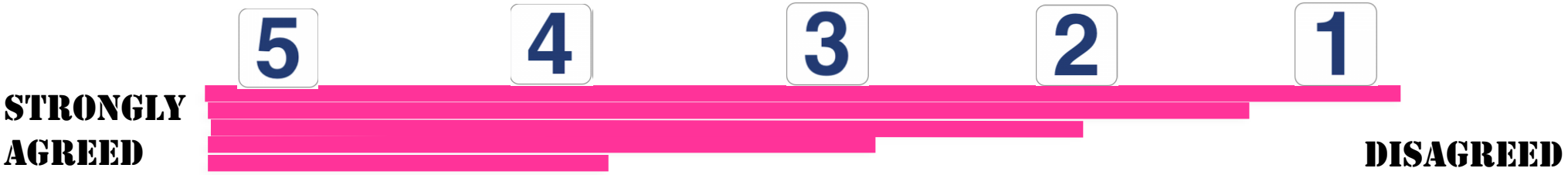
https://www.gpdp.it/.../-/docweb-display/docweb/9751323

Case Study
credit: #PrivacyNote



WWW.MENTI.COM

- หน่วยงานของท่านมีนโยบายที่เกี่ยวกับ PDPA ที่ชัดเจนครบถ้วน
- หน่วยงานของท่านมีขั้นตอนปฏิบัติหรือแนวทางปฏิบัติที่จัดทำไว้ให้กับพนักงานสามารถทำไปปฏิบัติได้อย่างชัดเจนและครบถ้วน
- หน่วยงานของท่านมีการกำหนดบทบาทหน้าที่และความรับผิดชอบ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และทุกคนเข้าใจในบทบาทหน้าที่ของตน
- หน่วยงานของท่านมีการกำหนดบทลงโทษสำหรับการละเมิดหรือละเลยบทบาทหน้าที่ในการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล อย่างชัดเจน
- หน่วยงานของท่านมีระบบงานสนับสนุนการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ตลอดวงจรชีวิตของข้อมูลส่วนบุคคล (เก็บรวบรวม ใช้ เปิดเผย ทำลาย)
- หน่วยงานของท่านมีการจัดทำ Data inventory ซึ่งสามารถทราบได้ว่าข้อมูลส่วนบุคคลมาจากไหน อยู่ที่ใด และส่งไปที่ไหนบ้าง
- หน่วยงานของท่านมีการสร้างความตระหนักเกี่ยวกับการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ให้กับทุกๆ บทบาท และพนักงานมีความพร้อมในการปฏิบัติตามหน้าที่ของตน



ทำไมต้องมี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ?

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

เนื่องจากสหภาพยุโรป (European Union: EU) ได้ออก GDPR (General Data Protection Regulation) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล บังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2561 ซึ่งนอกจากมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว ผู้ประกอบการในไทยที่ต้องติดต่อ รับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอด้วย

โครงสร้างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

บททั่วไป (มาตรา ๑ – มาตรา ๗)

หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๘ – มาตรา ๑๘)

หมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑ บททั่วไป (มาตรา ๑๙ – มาตรา ๒๑)

ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา ๒๒ – มาตรา ๒๖)

ส่วนที่ ๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา ๒๗ – มาตรา ๒๙)

หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา ๓๐ – มาตรา ๓๖)

หน้าที่ของผู้ควบคุมข้อมูล มาตรา ๓๗

หน้าที่ของผู้ประมวลผลข้อมูล มาตรา ๔๐

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา ๔๑ – มาตรา ๔๒

หมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา ๔๓ – มาตรา ๗๐)

หมวด ๕ การร้องเรียน (มาตรา ๗๑ – มาตรา ๗๖)

หมวด ๖ ความรับผิดทางแพ่ง (มาตรา ๗๗ - มาตรา ๗๘)

หมวด ๗ บทกำหนดโทษ

ส่วนที่ ๑ โทษอาญา (มาตรา ๗๙ – มาตรา ๘๑)

ส่วนที่ ๒ โทษทางปกครอง (มาตรา ๘๒ – มาตรา ๙๐)

บทเฉพาะกาล (มาตรา ๙๑ – มาตรา ๙๕)

การดำเนินการที่ได้รับยกเว้น (มาตรา 4)

เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวบุคคลเท่านั้น

การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

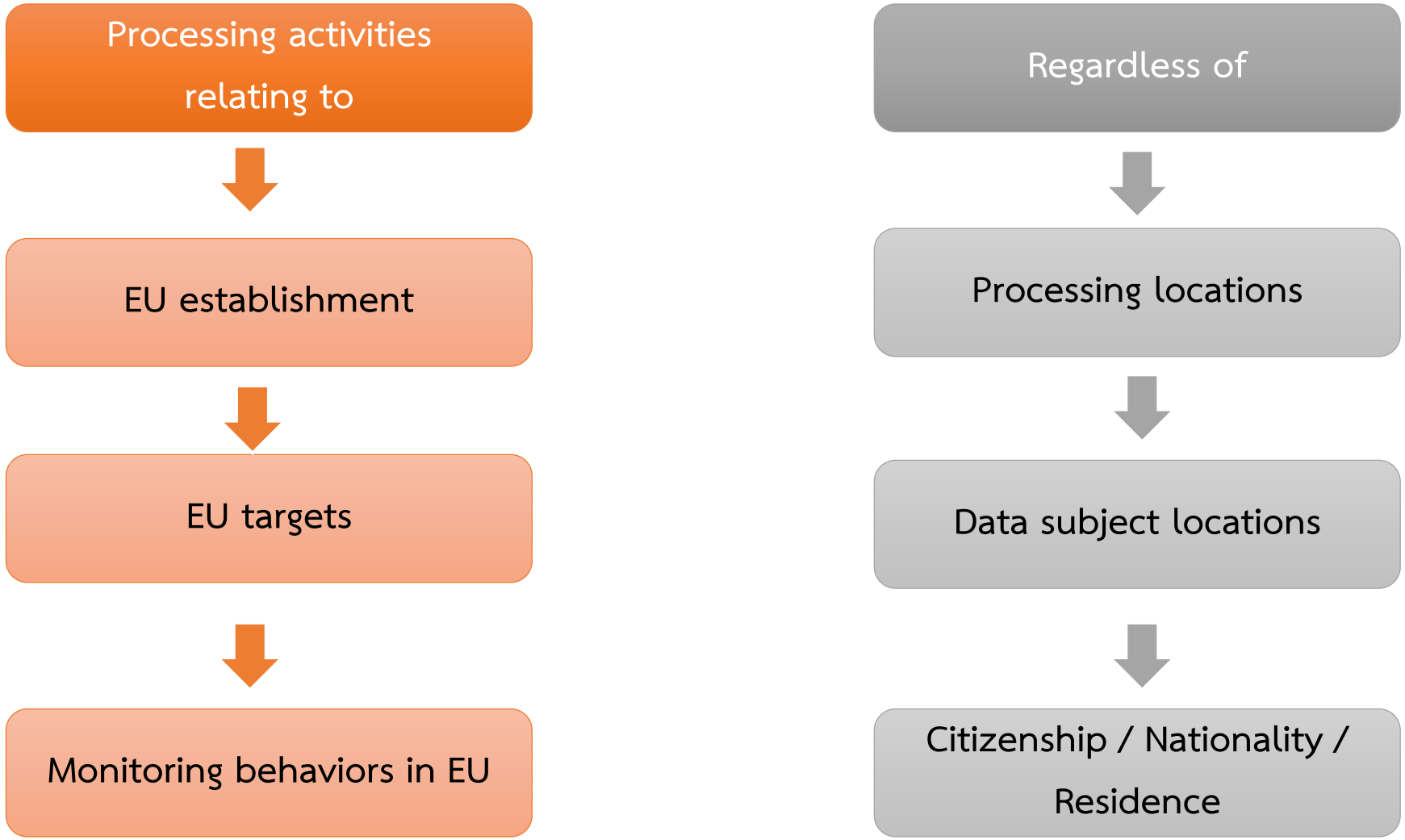
การพิจารณาตามหน้าที่และอำนาจสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

เพื่อกิจการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

หน้าที่ในการรักษาความมั่นคงของรัฐซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกัน และปราบปรามd การฟอกเงิน นิติวิทยาศาสตร์หรือการรักษาความมั่นคงปลอดภัยทางไซเบอร์

การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

GDPR's extraterritorial scope (Art.3)



ขอบเขตของการบังคับใช้

มาตรา ๕ พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(๑) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(๒) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

คำนิยาม PDPA

- “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
- “ผู้ควบคุมข้อมูลส่วนบุคคล” **(Data Controller)** หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- “ผู้ประมวลผลข้อมูลส่วนบุคคล” **(Data Processor)** หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
- **“เจ้าของข้อมูลส่วนบุคคล” (Data Subject)** ใน พ.ร.บ. ไม่ได้นิยามไว้

ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

GDPR

- **GDPR** ได้ให้คำจำกัดความและหน้าที่ของบทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูลหลักไว้ ๓ บทบาท ดังนี้
- ผู้ควบคุมข้อมูลส่วนบุคคล (**Controller**) คือ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการเว็บไซต์ต่าง ๆ
- ผู้ประมวลผลข้อมูลส่วนบุคคล (**Processor**) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้ อนึ่ง “การประมวลผลข้อมูล” (**Processing**) ตามกฎหมาย **GDPR** นั้น ไม่ใช่เพียงแค่การวิเคราะห์ หรือ จัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย
- เจ้าของข้อมูลส่วนบุคคล (**Data Subject**)

Example: Personal data, or not?

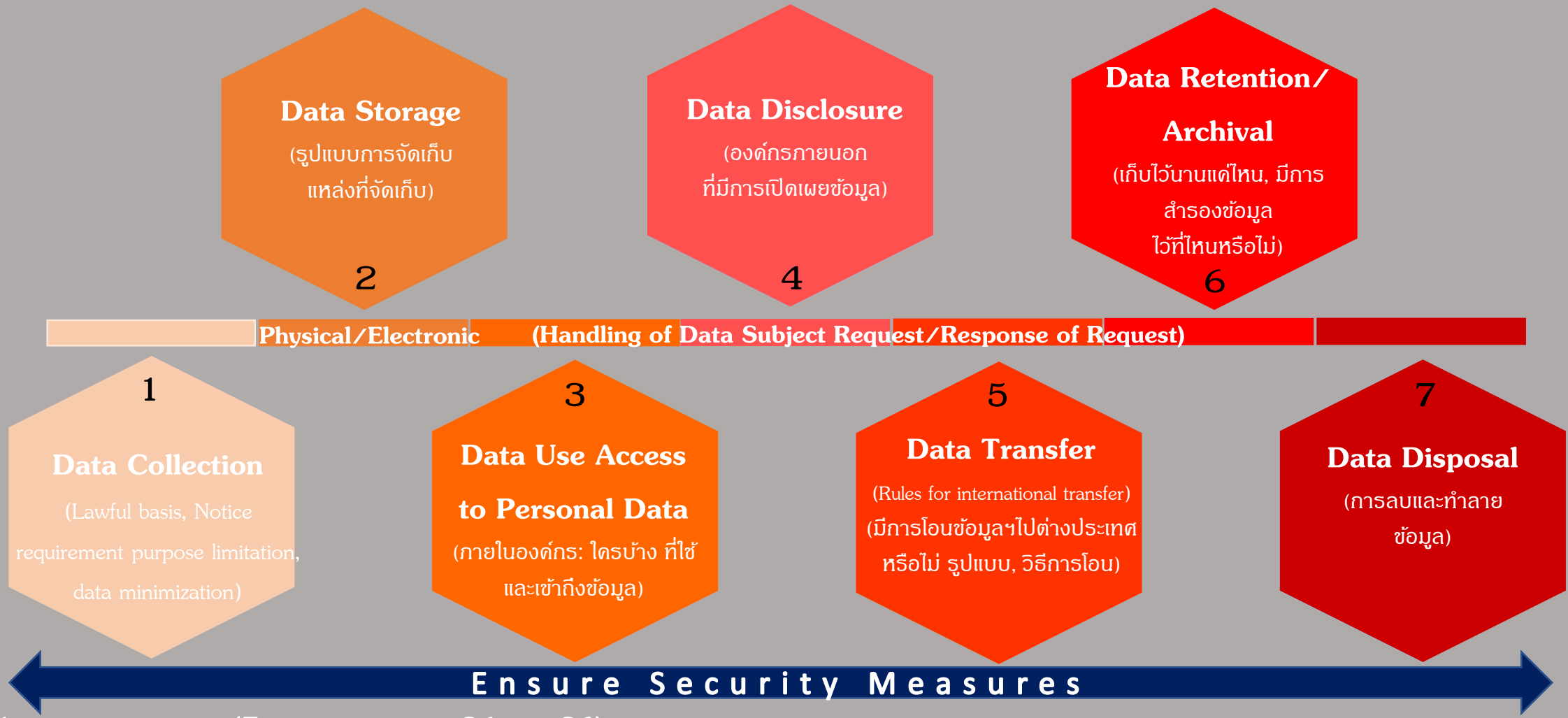
List	YES	NO
Jonathan Smith	YES	NO
Johathan.smith@company.com	YES	NO
Company Delta	YES	NO
Social Security Number	YES	NO
List of incoming call of a phone	YES	NO
Digital fingerprint	YES	NO
November 01, 2019	YES	NO
Minutes of meeting mentioning attendance of Jonathan Smith and his interventions	YES	NO
Geologicalised data of a company car	YES	NO
Credit card number	YES	NO
Oxford Street, 20, London	YES	NO
192.168.87.11 at internet cafe’	YES	NO
Car ID: 7465 PY 11	YES	NO
CCTV Surveillance	YES	NO

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

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

Article5 Principles relating to processing of personal data

Data minimization

Adequate, relevant and limited to what necessary in relation to the purpose

Storage limitation

Retained only for as long as necessary for achieving the purpose

Purpose limitation

Collected for specified explicit and legitimate purposes

Accuracy

Accuracy any, where necessary, kept up to date

7 Principles

Accountability

(Demonstrate Compliance)

Lawfulness, fairness and transparency

Integrity and Confidentiality

Processed in a manner to maintain security

การเก็บรวบรวมข้อมูลส่วนบุคคล มาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

การเก็บรวบรวมข้อมูลส่วนบุคคล มาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา ๒๑ และการแจ้งรายละเอียดตามมาตรา ๒๓ มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

ไม่เก็บรวบรวมเอง
ไปซื้อข้อมูลมาได้หรือไม่?

(๑) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๓) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา ๒๓ ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

20

ฐานการประมวลผล มาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

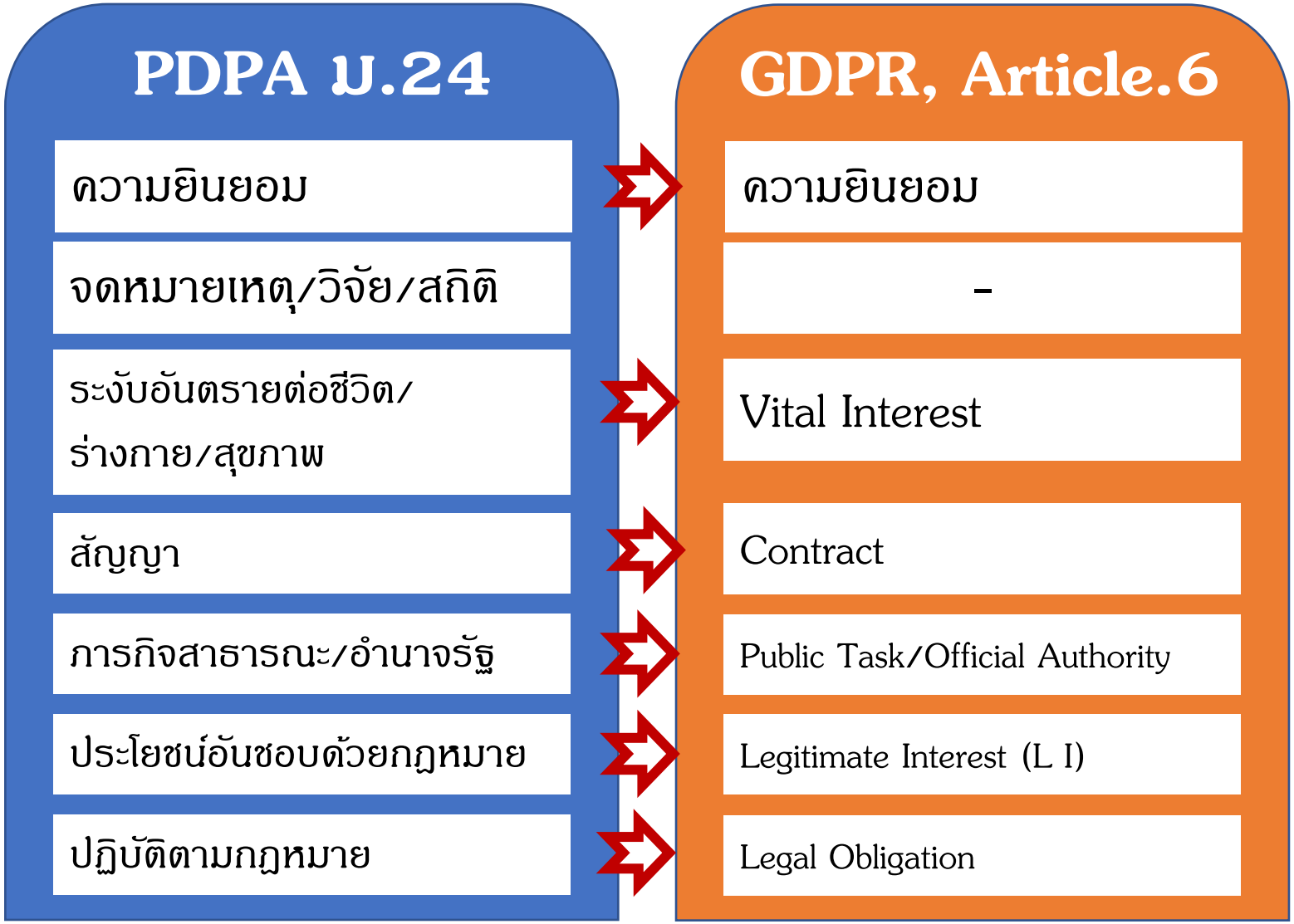
(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

PDPA

- ความยินยอม
- จดหมายเหตุ/วิจัย/สถิติ
- ระงับอันตรายต่อชีวิต/ร่างกาย/สุขภาพ
- สัญญา
- ภารกิจสาธารณะ/อำนาจรัฐ
- ประโยชน์อันชอบด้วยกฎหมาย
- ปฏิบัติตามกฎหมาย

21

ตารางเปรียบเทียบฐานการประมวลผลข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ GDPR



22

การประเมินฐานประโยชน์อันชอบด้วยกฎหมาย
Legitimate Interest Assessment (LIA)

Identify a legitimate interest

purpose

Necessary to meet the purposes

Legal basis

มีความจำเป็น และเป็นไปเพื่อประโยชน์อันชอบธรรม

Necessity test

Important?

No other way?

มีความจำเป็นต้องเก็บรวบรวม ไม่มีวิธีอื่นแล้วจริงๆ

Balancing test

Expectation of others

Value-added?

Negative Impact?

ไม่เกินไปจากความคาดหวังของเจ้าของข้อมูล เป็นประโยชน์เพิ่ม ไม่มีผลกระทบในทางลบ

การประกาศความเป็นส่วนตัว Privacy Notice

ม. 23 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

1. วัตถุประสงค์ของการเก็บรวบรวม และวัตถุประสงค์ตาม ม. 24 ที่ให้อำนาจในการเก็บรวบรวมได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา และแจ้งถึงผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล
3. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาได้ ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม
4. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
5. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ
6. สิทธิของเจ้าของข้อมูลส่วนบุคคล ได้แก่ สิทธิขอเข้าถึงและขอรับสำเนา สิทธิขอโอนข้อมูล สิทธิคัดค้าน สิทธิขอให้ลบหรือทำลาย สิทธิขอระงับการใช้ข้อมูล สิทธิขอให้ดำเนินการแก้ไขข้อมูลให้ถูกต้อง และสิทธิในการร้องเรียน

หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตาม ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท (ม. 82)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.20
V2

จุฬาฯ กับการคุ้มครองข้อมูลส่วนบุคคล ของนิสิต

Chula Chulalongkorn University

- นิสิตเป็นเจ้าของข้อมูลส่วนบุคคล จึงได้รับการคุ้มครองตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
- จุฬาฯ ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลและมีความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
- จุฬาฯ ประมวลผลข้อมูลส่วนบุคคลที่นิสิตให้ไว้ (ระเบียนประวัตินิสิต จท.20 และ จท.20/1 [ข้อมูลสุขภาพ]) เท่าที่จำเป็น เพื่อนำไปใช้ดำเนินการตามหน้าที่ของจุฬาฯ
- หากคณะ/หน่วยงานต้องการข้อมูลอื่นใด ต้องขอความยินยอมจากนิสิตเพิ่มเติม

ศึกษารายละเอียดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลได้ที่

จุฬาฯ เตรียมความพร้อมตั้งแต่มีการประกาศใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จึงมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- สำนักงานการทะเบียน https://www.reg.chula.ac.th และคณะที่นิสิตสังกัด
- เรียนรู้กฎหมายเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับ Chula MOOC https://mooc.chula.ac.th/courses/218

หากมีข้อสงสัย สอบถามได้ที่ สำนักยุทธศาสตร์และการขับเคลื่อน
E-mail : pichitchai.c@chula.ac.th

Chula Communication Center (CCC) | Chulalongkorn University

ตัวอย่าง

โปรดคำนึงอย่างจริงจัง
เรื่อง นโยบายความเป็นส่วนตัว

มหาวิทยาลัยธรรมศาสตร์ เห็นความสำคัญ ในการปกป้องข้อมูลส่วนบุคคล ของบุคลากร นักศึกษา และ อาจารย์ภายในมหาวิยาลัย เพื่อเป็นให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผู้ให้บริการให้มี สิทธิการเข้าถึงข้อมูล () (Personal Data Protection Act : PDPA)

สำคัญ

- ในการใช้บริการนี้ ผู้ใช้ต้องตรวจสอบว่าได้ดำเนินการผ่าน ผู้ให้บริการนี้ไม่ ต้องรับผิดชอบต่อความเสียหายใดๆ ที่เกิดจากการใช้บริการจาก แหล่งอื่นที่ไม่ใช่ผู้ให้บริการอย่างเป็นทางการ
- ข้อมูลส่วนบุคคลที่มอบให้แก่บริการนี้และข้อมูลส่วนบุคคลที่ รวบรวมใหม่จะถูกนำไปใช้ภายใต้ความรับผิดชอบของผู้ใช้บริการ นี้ โปรดตรวจสอบรายละเอียดในข้อกำหนดการใช้บริการและ นโยบายความเป็นส่วนตัวของผู้ให้บริการ
- ข้อมูลโปรไฟล์ประกอบด้วย ชื่อ-นามสกุล,วันเกิด ,อีเมลล์ ,เลขประจำตัวบัตรประชาชน หรือ พาสปอร์ต ,หน่วยงาน และองค์กร
- โปรดตรวจสอบว่า ชื่อ-นามสกุลของท่าน ไม่มีเนื้อหาที่ละเมิดในสิทธิ์ของผู้ใด เช่น ละเมิดลิขสิทธิ์ ละเมิดความเป็นส่วนตัว ตามที่ระบุในข้อกำหนดการใช้บริการ มหาวิทยาลัยธรรมศาสตร์

KU KASETSART UNIVERSITY

ประกาศมหาวิทยาลัยมหิดล
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

โดยที่มหาวิทยาลัยมหิดลมีการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลของบุคลากร นักศึกษา ผู้รับบริการ และบุคคลอื่น เพื่อการดำเนินงานด้านต่าง ๆ ของมหาวิทยาลัย จึงเป็นการสมควรที่มหาวิทยาลัยจะกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy) ให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินงานของมหาวิทยาลัยมหิดลเป็นไปอย่างเรียบร้อย มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและได้มาตรฐาน

อาศัยอำนาจตามความในมาตรา ๓๔ (๘) แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ คณะกรรมการประจำมหาวิทยาลัยมหิดล ในการประชุมครั้งที่ ๒๐/๒๕๖๓ เมื่อวันที่ ๒๘ ตุลาคม พ.ศ. ๒๕๖๓ อธิการบดีจึงกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ ดังต่อไปนี้

ข้อ ๑. ในประกาศนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคลากร นักศึกษา ผู้รับบริการ และผู้เข้าร่วมการวิจัย แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

มหาวิทยาลัยเกษตรศาสตร์ได้จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น

เพื่อคุ้มครองข้อมูลส่วนบุคคลของ ผู้ใช้บริการทุกท่าน (Personal Information) ที่ติดต่อเข้ามายังเว็บไซต์ของมหาวิทยาลัยเกษตรศาสตร์ ดังนี้

1. **การเก็บรวบรวมข้อมูลส่วนบุคคล**

เพื่อความสะดวกในการให้บริการแก่ผู้ใช้บริการทุกท่านที่เข้ามาใช้บริการเว็บไซต์ของมหาวิทยาลัยเกษตรศาสตร์ทางเว็บไซต์จึงได้จัดเก็บรวบรวมข้อมูลส่วนบุคคลของท่านไว้ เช่น อีเมล์แอดเดรส (Email Address) ชื่อ (Name) ที่อยู่หรือที่ทำงาน (Home or Work Address) เขตไปรษณีย์ (ZIP Code) หมายเลขโทรศัพท์ (Telephone Number) เป็นต้น ในกรณีที่ท่านสมัคร (Sign Up) เพื่อสมัครสมาชิกหรือเพื่อใช้บริการอย่างใดอย่างหนึ่ง มหาวิทยาลัยเกษตรศาสตร์จะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพิ่มเติม ได้แก่ เพศ (Sex) อายุ (Gender) สิ่งที่โปรดปราน/ความชอบ (Preferences/Favorites) ความสนใจ (Interests) หมายเลขบัตรเครดิต (Credit Card Number) และที่อยู่ในการแจ้งค่าใช้จ่าย (Billing Address) นอกจากนั้น เพื่อสำรวจความนิยมในการใช้บริการอันจะเป็นประโยชน์ ในการนำสถิติไปใช้ในการปรับปรุงคุณภาพ ในการให้บริการของมหาวิทยาลัยเกษตรศาสตร์จึงจำเป็นต้องจัดเก็บรวบรวมข้อมูลของท่านบางอย่างเพิ่มเติม ได้แก่ หมายเลขไอพี (IP Address) ชนิดของโปรแกรมค้นผ่าน (Browser Type) โดเมนเนม (Domain Name) บันทึกหน้าเว็บ (web page) ของเว็บไซต์ ที่ผู้ใช้เยี่ยมชม เวลาที่เยี่ยมชมเว็บไซต์ (Access Times) และเว็บไซต์ที่ผู้ใช้บริการเข้าถึงก่อนหน้านั้น (ReferringWebsite Addresses) มหาวิทยาลัยเกษตรศาสตร์ขอแนะนำให้ท่านตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของเว็บไซต์อื่นที่เชื่อมโยงจากเว็บไซต์นี้ เพื่อจะได้ทราบและเข้าใจว่าเว็บไซต์ดังกล่าวเก็บรวบรวมใช้ หรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านอย่างไร ทั้งนี้มหาวิทยาลัยเกษตรศาสตร์ ไม่สามารถรับรองข้อความ หรือรับรองการ ดำเนินการใดๆ ตามที่ได้มีการประกาศไว้ในเว็บไซต์ดังกล่าวได้และไม่ขอรับผิดชอบใดๆ หากเว็บไซต์เหล่านั้นไม่ได้ปฏิบัติการหรือดำเนินการใดๆ ตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่เว็บไซต์ดังกล่าวได้ประกาศไว้

2. **การใช้ข้อมูลส่วนบุคคล**

มหาวิทยาลัยเกษตรศาสตร์จะใช้ข้อมูลส่วนบุคคล ของท่านเพียงเท่าที่จำเป็น เช่น ชื่อ และ ที่อยู่ เพื่อใช้ในการติดต่อ ให้บริการประชาสัมพันธ์ หรือให้ข้อมูลข่าวสารต่างๆ รวมทั้งสำรวจความคิดเห็นของท่านในกิจการ หรือกิจกรรมของมหาวิทยาลัยเกษตรศาสตร์ท่านั้น มหาวิทยาลัยเกษตรศาสตร์ขอรับรองว่าจะไม่นำข้อมูลส่วนบุคคลของท่านที่มหาวิทยาลัยเกษตรศาสตร์ได้เก็บรวบรวมไว้ ไปขาย หรือเผยแพร่ให้กับบุคคลภายนอกโดยเด็ดขาดเว้นแต่จะได้รับอนุญาตจากท่านเท่านั้น
ในกรณีที่มหาวิทยาลัยเกษตรศาสตร์ ได้ว่าจ้างหน่วยงานอื่นเพื่อให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่าน เช่น การจัดส่งพัสดุไปรษณีย์ การวิเคราะห์เชิงสถิติในกิจการ หรือกิจกรรมของมหาวิทยาลัยเกษตรศาสตร์ เป็นต้น มหาวิทยาลัยเกษตรศาสตร์จะกำหนดให้หน่วยงานที่ได้ว่าจ้างให้ดำเนินการดังกล่าวเก็บรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลของท่านและกำหนดข้อห้ามมิให้มีการนำข้อมูลส่วนบุคคลดังกล่าวไปใช้นอกเหนือจากกิจกรรมหรือกิจการของมหาวิทยาลัยเกษตรศาสตร์

3. **สิทธิในการควบคุมข้อมูลส่วนบุคคลของท่าน**

เพื่อประโยชน์ในการรักษาความเป็นส่วนตัวของท่านๆ มีสิทธิเลือกที่จะให้มีการใช้หรือแชร์ข้อมูลส่วนบุคคลของ ท่าน หรืออาจ เลือกที่จะไม่รับข้อมูล หรือสื่อทางการตลาดใดๆจากมหาวิทยาลัยเกษตรศาสตร์ก็ได้ โดยเพียงแต่ท่านกรอกความจำนงดังกล่าวเพื่อแจ้งให้มหาวิทยาลัยเกษตรศาสตร์ทราบในหน้าเว็บ www.treasury.go.th

สำนักงาน ก.ล.ต. มีการแบ่งการประมวลผลข้อมูลส่วนบุคคลตามการดำเนินภารกิจของสำนักงาน ก.ล.ต. ซึ่งสามารถศึกษารายละเอียดได้ตาม link ด้านล่างนี้

- การใช้คุกกี้บนเว็บไซต์สำนักงาน
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับการระดมทุน
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับการจัดการลงทุน
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ประกอบธุรกิจ
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับการซื้อขายในตลาดรอง
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับงานบริหารงานภายใน (web สำนักงาน)
- การรับร้องเรียนและสอบถามข้อมูล

ตัวอย่าง

(เพื่อความสะดวกแก่หน่วยงาน และองค์กรนำไปพิจารณาใช้เป็นต้นแบบ)

(เวอร์ชั่นที่ทำกับ A.2.1)

DGA

นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

---

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (ต่อไปในนโยบายนี้เรียกว่า "**สพร.**" หรือ "**องค์กร**") ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่นอันเกี่ยวกับท่าน (รวมเรียกว่า "**ข้อมูล**") เพื่อให้ท่านมีความเชื่อมั่นได้ว่า สพร. มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ("**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**") รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ("**นโยบาย**") นี้จึงได้ถูกจัดทำขึ้นเพื่อชี้แจงแก่ท่านถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า "**ประมวลผล**") ข้อมูลส่วนบุคคลซึ่งดำเนินการโดย สพร. รวมถึงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องผู้ดำเนินการแทนหรือในนามของ สพร. โดยมีเนื้อหาสาระดังต่อไปนี้

2. ขอบเขตการบังคับใช้นโยบาย

นโยบายนี้ใช้บังคับกับ**ข้อมูลส่วนบุคคลของบุคคลซึ่งมีความสัมพันธ์กับ สพร.** ในปัจจุบันและที่อาจมีในอนาคต ซึ่งถูกประมวลผลข้อมูลส่วนบุคคลโดย สพร. เจ้าหน้าที่ พนักงาน ตามสัญญา หน่วยธุรกิจหรือหน่วยงานรูปแบบอื่นที่ดำเนินการโดย สพร. และรวมถึงคู่สัญญาหรือบุคคลภายนอกที่ประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของ สพร. ("**ผู้ประมวลผลข้อมูลส่วนบุคคล**") ภายใต้ผลิตภัณฑ์และบริการต่าง ๆ เช่น เว็บไซต์ ระบบ แอปพลิเคชัน เอกสาร หรือบริการในรูปแบบอื่นที่ควบคุมดูแลโดย สพร. (รวมเรียกว่า "**บริการ**")

บุคคลซึ่งมีความสัมพันธ์กับ สพร. ตามความในวรรคแรก รวมถึง

1) ลูกค้าบุคคลธรรมดา
2) เจ้าหน้าที่หรือผู้ปฏิบัติงาน ลูกจ้าง

3) คู่ค้าและผู้ให้บริการซึ่งเป็นบุคคลธรรมดา
4) กรรมการ ผู้รับมอบอำนาจ ผู้แทน ตัวแทน ผู้ถือหุ้น ลูกจ้าง หรือบุคคลอื่นที่มีความสัมพันธ์ในรูปแบบเดียวกันของนิติบุคคลที่มีความสัมพันธ์กับ สพร.
5) ผู้ใช้งานผลิตภัณฑ์หรือบริการของ สพร.
6) ผู้เข้าชมหรือใช้งานเว็บไซต์ www.dga.or.th รวมทั้งระบบ แอปพลิเคชัน อุปกรณ์ หรือช่องทางการสื่อสารอื่นซึ่งควบคุมดูแลโดย สพร.
7) บุคคลอื่นที่ สพร. เก็บรวบรวมข้อมูลส่วนบุคคล เช่น ผู้สมัครงาน ครอบครัวของเจ้าหน้าที่ ผู้ค้ำประกัน ผู้รับประโยชน์ในกรมธรรม์ประกันภัย เป็นต้น

ข้อ 1) ถึง 6) เรียกรวมกันว่า "**ท่าน**"

นอกจากนโยบายฉบับนี้แล้ว สพร. อาจกำหนดให้มีคำประกาศเกี่ยวกับความเป็นส่วนตัว ("**ประกาศ**") สำหรับผลิตภัณฑ์หรือบริการของ สพร. เพื่อชี้แจงให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้ใช้บริการได้ทราบถึงข้อมูลส่วนบุคคลที่ถูกประมวลผล วัตถุประสงค์และเหตุผลอันชอบด้วยกฎหมายในการประมวลผล ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล รวมถึงสิทธิในข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลที่มีในผลิตภัณฑ์หรือบริการนั้นเป็นการเฉพาะเจาะจง

ทั้งนี้ ในกรณีที่มีความขัดแย้งกันในสาระสำคัญระหว่างความในประกาศที่เกี่ยวกับความเป็นส่วนตัวและนโยบายนี้ ให้ถือตามความในประกาศที่เกี่ยวกับความเป็นส่วนตัวของบริการนั้น

3. คำนิยาม

- **สพร.** หมายถึง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
- **ข้อมูลส่วนบุคคลอ่อนไหว** หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลทางพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
- **การประมวลผลข้อมูลส่วนบุคคล** หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น เก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผย ส่งต่อ เผยแพร่ โอน รวม ลบ ทำลาย เป็นต้น
- **เจ้าของข้อมูลส่วนบุคคล** หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ สพร. เก็บรวบรวม ใช้ หรือเปิดเผย

https://www.dga.or.th/document-sharing/article/59030/

ตัวอย่าง

ข้อมูลต่อไปนี้ห้ามเก็บ (มาตรา 26)

Sensitive Data

01 Racial or Ethnic origin
เชื้อชาติ เผ่าพันธ์

02 Political opinion
ความคิดเห็นทางการเมือง

03 Religious or philosophical Beliefs
ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

04 Sexual orientation
พฤติกรรมทางเพศ

05 Criminal record
ประวัติอาชญากรรม

06 Health information
ข้อมูลสุขภาพ

07 Disability
ข้อมูลความพิการ

08 Trade union information
ข้อมูลสหภาพแรงงาน

09 Genetic data
ข้อมูลพันธุกรรม

10 Biometric data
ข้อมูลชีวภาพ

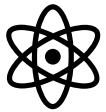
ข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลตามที่คณะกรรมการประกาศกำหนด
โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลฯ

ข้อยกเว้นตามมาตรา 26 สำหรับข้อมูลอ่อนไหว (Sensitive Personal Data)

วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์

ประโยชน์สาธารณะด้านสาธารณสุข

คุ้มครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ)



ศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

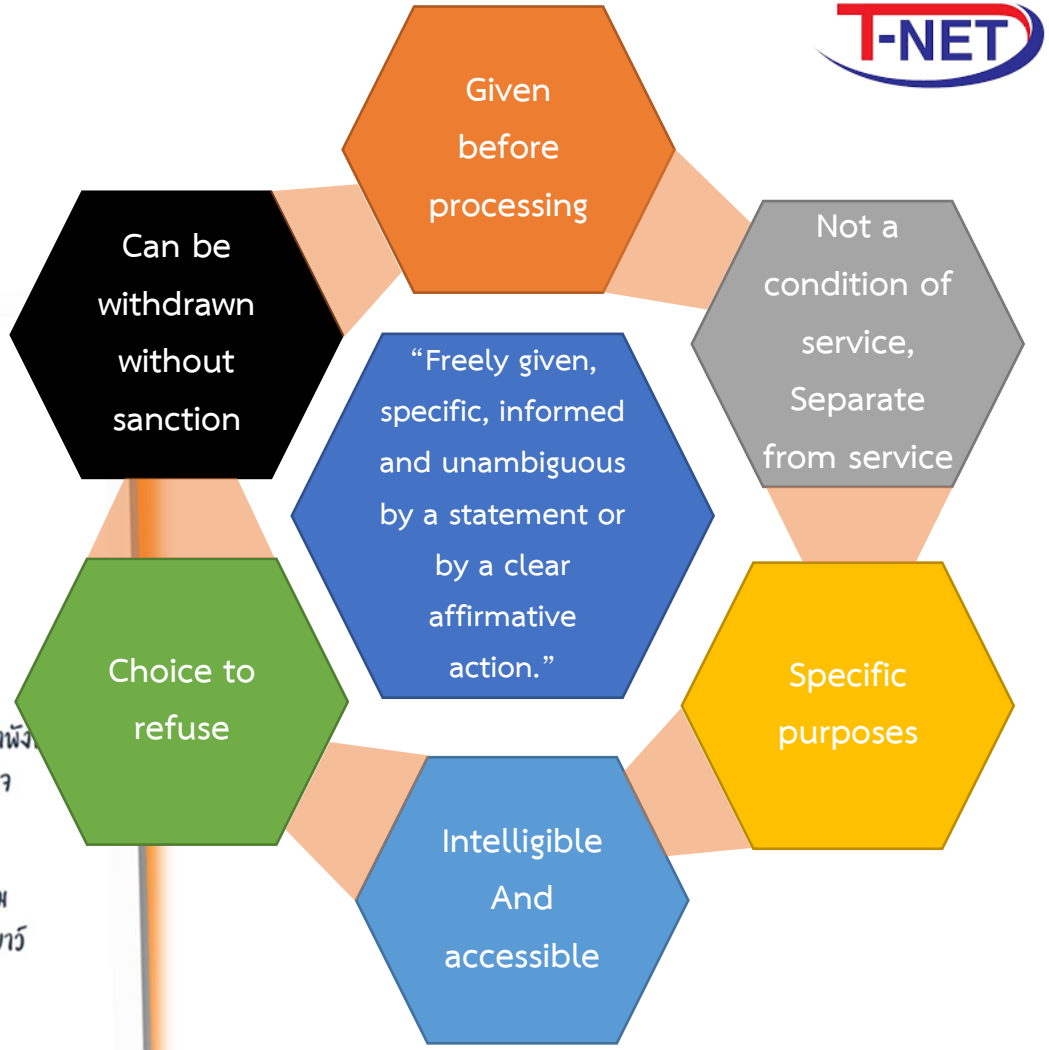
เพื่อป้องกันอันตรายต่อชีวิตของเจ้าของข้อมูล

มูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

เจ้าของข้อมูลยินยอมโดยชัดแจ้งให้เปิดเผยต่อสาธารณะ

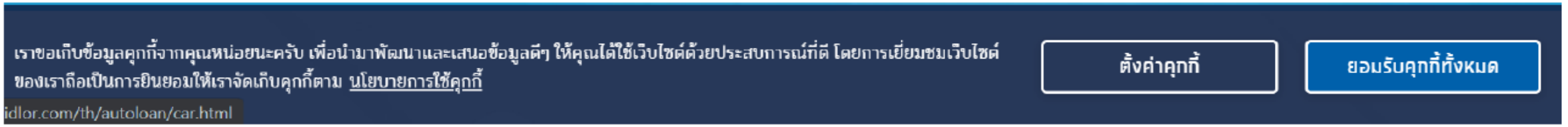
เพื่อสิทธิเรียกร้องตามกฎหมาย

GDPR Conditions for Consent (Art.4)
เงื่อนไขความยินยอม (มาตรา19)

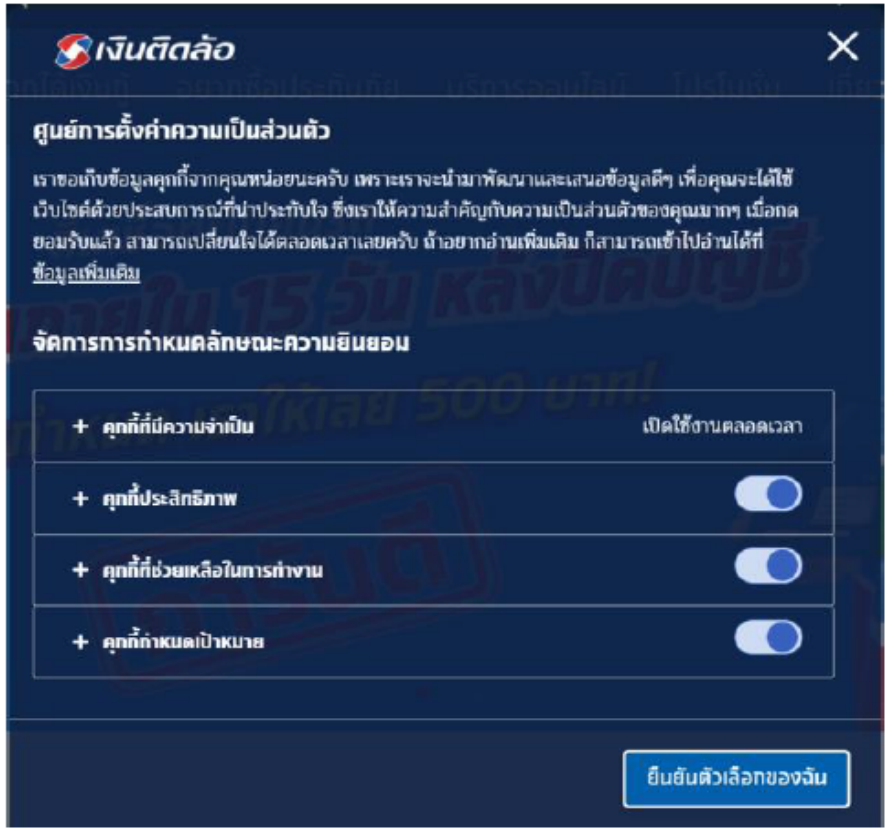


ตัวอย่าง การขอความยินยอมที่ชัดแจ้ง

Cookie Consent



- คุกกี้ที่มีความจำเป็น (Strictly Necessary Cookies)
- คุกกี้เพื่อการวิเคราะห์และประเมินผลการใช้งาน (Performance Cookies)
- คุกกี้เพื่อการใช้งานเว็บไซต์ (Functional Cookies)
- คุกกี้เพื่อการโฆษณาไปยังกลุ่มเป้าหมาย (Targeting Cookies)



Privacy Policy กับ Privacy Notice ต่างกันอย่างไร ?

PART 1

MUST HAVE

PRIVACY NOTICE

ประกาศความเป็นส่วนตัว

เป็นประกาศถึงเจ้าของข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบเกี่ยวกับรายละเอียดวิธีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงวิธีการดำเนินการต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคล โดยกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

PRIVACY POLICY

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

เป็นนโยบายภายในองค์กรที่วางแนวปฏิบัติหรือกำหนดทิศทางเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลภายในองค์กรหรือหน่วยงานนั้น ๆ เพื่อให้สอดคล้องกับหลักการและเงื่อนไขตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

อ้างอิง : Russell Densmore, Privacy Program Management
หน้า 88 "Privacy Notice versus Privacy Policy"

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

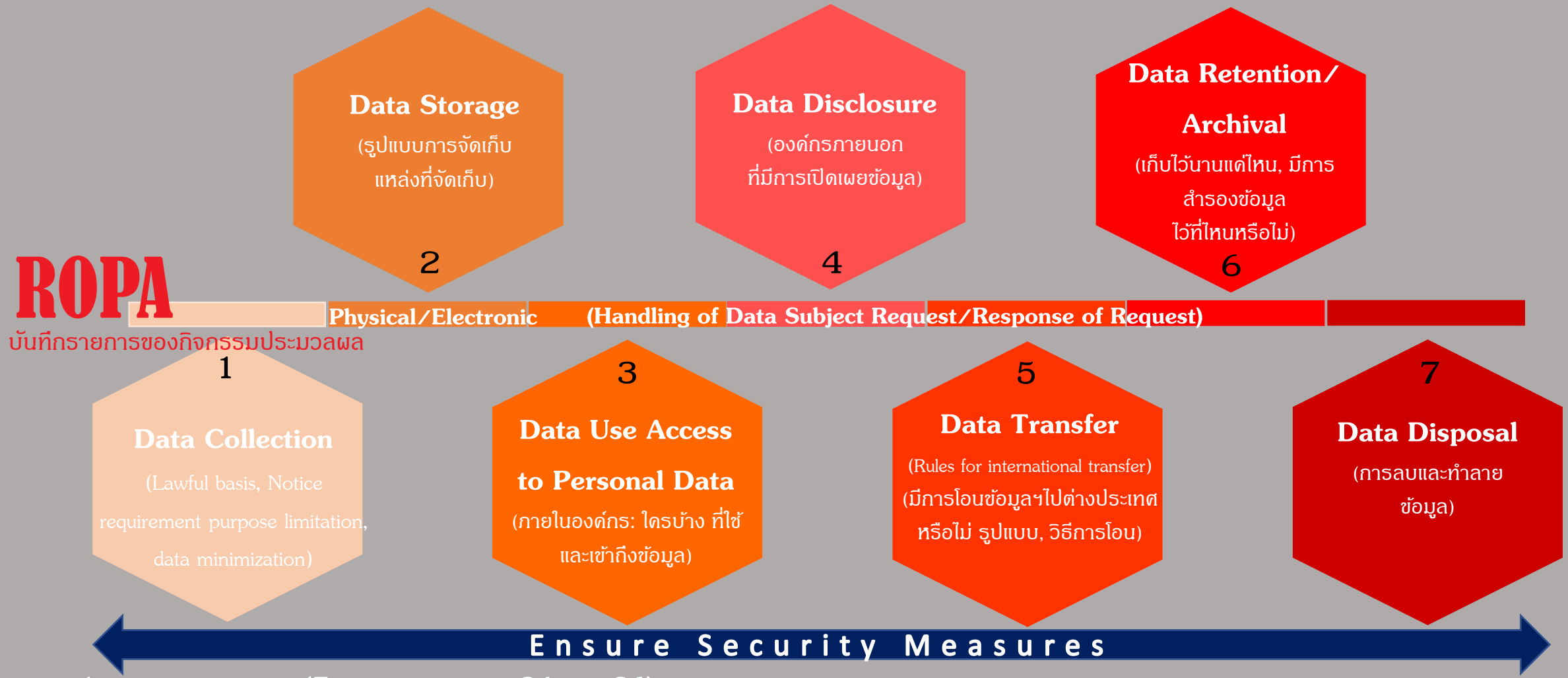
Privacy Policy กับ Privacy Notice ต่างกันอย่างไร?

PART 2

ข้อแตกต่าง	PRIVACY POLICY นโยบายการคุ้มครองข้อมูลส่วนบุคคล	PRIVACY NOTICE ประกาศความเป็นส่วนตัว
สภาพบังคับทางกฎหมาย	กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)	กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้ง ตามมาตรา 23
ขอบเขต	เป็นเอกสารที่สื่อสารถึงบุคคลภายในองค์กร	เป็นประกาศที่มีผลเฉพาะเจ้าของข้อมูลส่วนบุคคลเท่านั้น
เนื้อหา	เป็นนโยบายและแนวปฏิบัติขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล	เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

หมายเหตุ : Privacy policy อาจจะครอบคลุม Privacy notice ได้ โดยพิจารณาเนื้อหาภายใน หากครบถ้วนตามที่กฎหมายกำหนด ก็จะถือว่ามีการแจ้งวัตถุประสงค์ ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

ROPA มาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ทำไมต้องทำ ROPA?

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

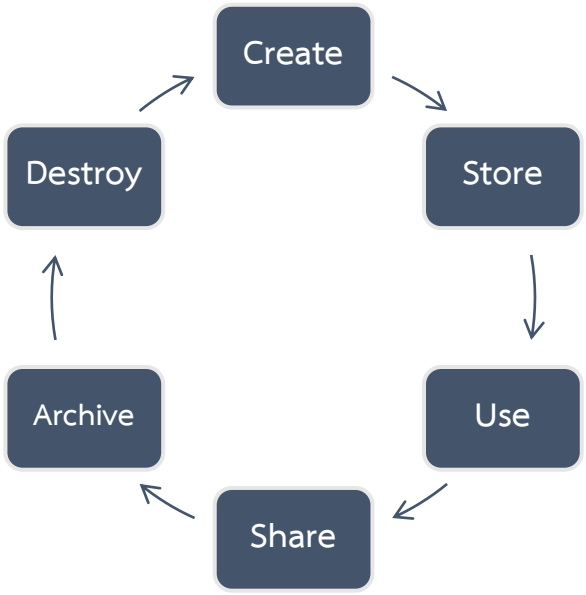
(๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (๑) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (๓) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

ROPA มาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



Descriptions

Collection

Storage

Usage

Transfer

Disposal

Access Control

Encryption

Availability

Backup

Recovery

Data Subjects' Rights

ROPA มาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. Activity_ID
2. Bureau
3. Process Name
4. Process Owner
5. ฐานะขององค์กร
6. ผู้ควบคุมข้อมูลส่วนบุคคล

7 การได้มาซึ่งข้อมูลส่วนบุคคล

- ประเภทของข้อมูล
- ปริมาณของข้อมูล
- แหล่งที่มาของข้อมูล
- วิธีการได้รับข้อมูล
- ข้อมูลทั่วไป
- ข้อมูลส่วนบุคคลอ่อนไหว
- วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- ระยะเวลาในการจัดเก็บข้อมูล

8 สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล

- บุคคลภายนอกที่มีสิทธิเข้าถึงข้อมูล
- ส่วนงานภายในที่มีสิทธิเข้าถึงข้อมูล
- รูปแบบ/ช่องทางการเข้าถึงข้อมูล
- จำนวนครั้ง/ความถี่ในการเรียกใช้ข้อมูล
- สิทธิในการเข้าถึงข้อมูล
- เงื่อนไขของบุคคลที่มีสิทธิ์เข้าถึง และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

9 รูปแบบการเก็บข้อมูลส่วนบุคคล

- ลักษณะการเก็บข้อมูล
- ที่จัดเก็บ/ระบบจัดเก็บ
- สถานที่ตั้ง

10 การโอนข้อมูลส่วนบุคคลไปต่างประเทศ

- Cross-Border
- ประเทศหรือองค์กรที่โอนข้อมูลส่วนบุคคล
- มาตรการคุ้มครองข้อมูลส่วนบุคคลของปลายทาง
- ความถี่ในการโอน

11 ฐานทางกฎหมาย

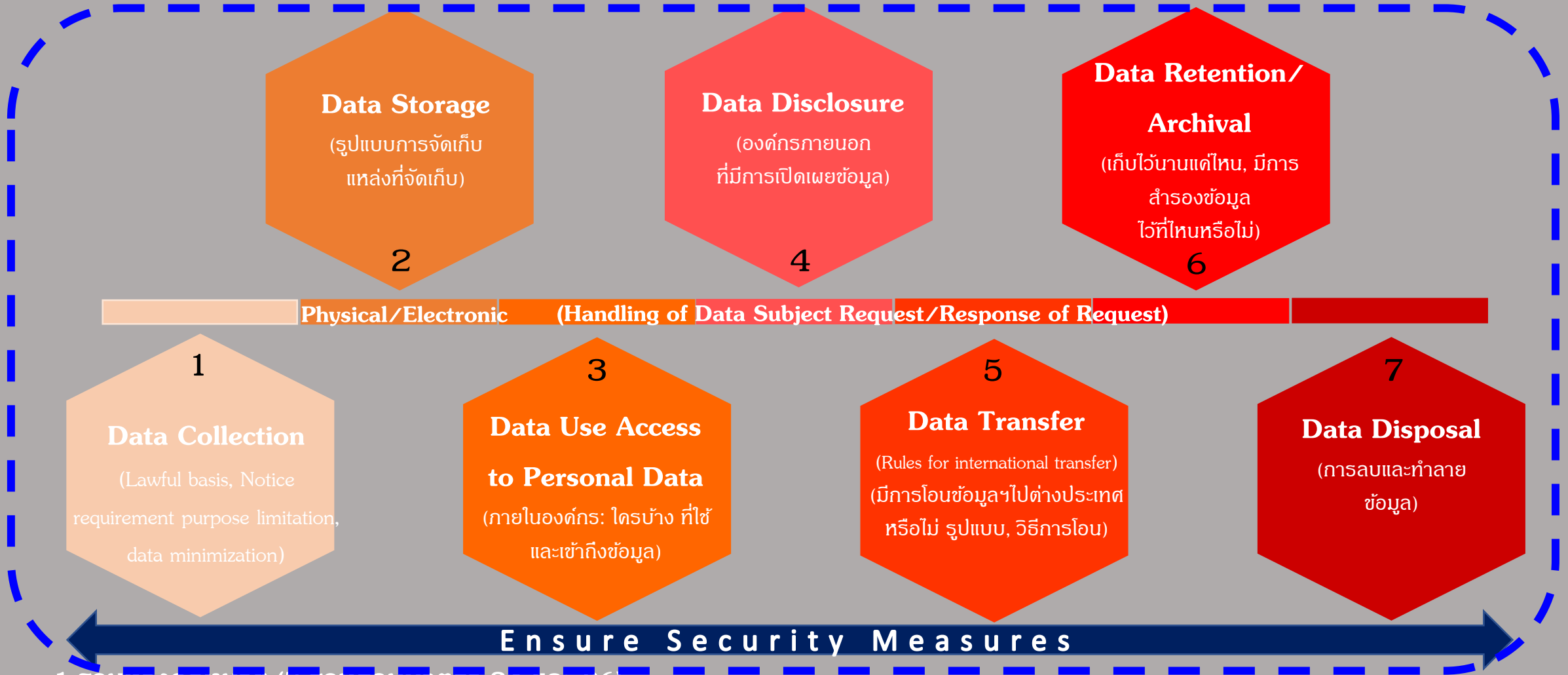
- ฐานประโยชน์สำคัญต่อชีวิต
- ฐานสัญญา
- ฐานภารกิจสาธารณะ/อำนาจรัฐ
- ฐานประโยชน์อันชอบธรรมด้วยกฎหมาย
- ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
- ฐานจดหมายเหตุ/วิจัย/สถิติ
- ฐานความยินยอม

12 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามมาตรา 37 (1)

มาตรการด้านความมั่นคงปลอดภัย

Security Measures (ม.37)

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(๕) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

โดยที่มาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ กำหนดให้ผู้ควบคุมข้อมูลซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกาดังกล่าวต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

อาศัยอำนาจตามความในมาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาจนถึงวันที่ ๓๑ พฤษภาคม ๒๕๖๔

ข้อ ๓ ในประกาศนี้

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical

safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

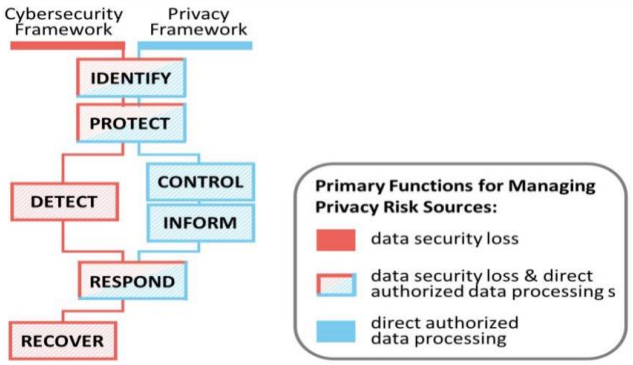
(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๖ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้

ข้อ ๗ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามประกาศนี้ และให้มีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่ ๒๔ มิถุนายน พ.ศ. ๒๕๖๓
พุทธิพงษ์ ปุณณกันต์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



https://www.nist.gov/privacy-framework.

ISO 27001

องค์ประกอบของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

1

การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูล

2

การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

3

การเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว (User access management)

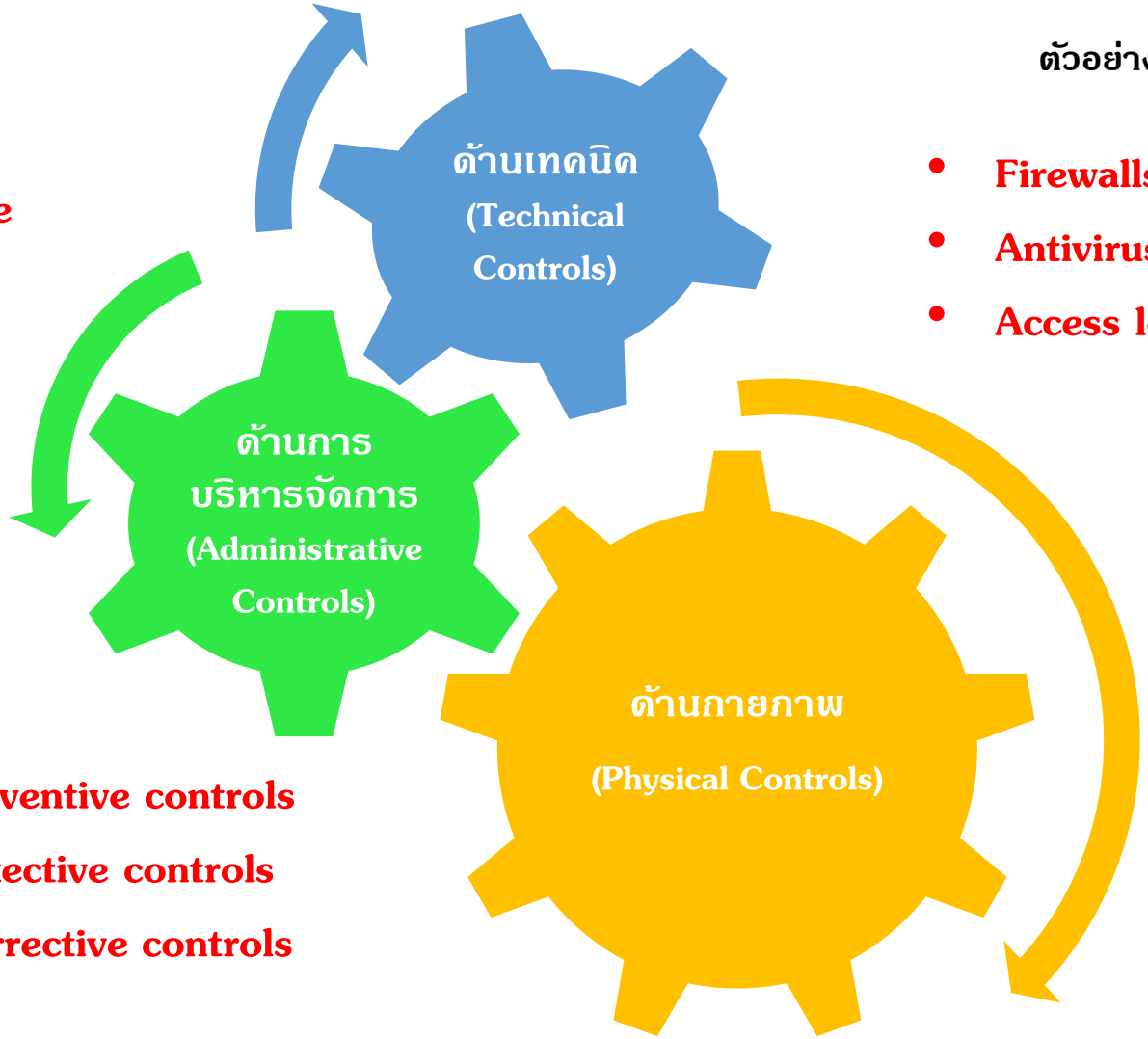
4

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

5

การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง

องค์ประกอบของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล



ตัวอย่าง

Incident response procedures and training

- Preventive controls
- Detective controls
- Corrective controls

ตัวอย่าง

- Firewalls
- Antivirus Software
- Access logs

ตัวอย่าง

- Locks
- CCTV
- Fences

Privacy v$ Security

Privacy

- Collection of Personal Information
- Using and disclosing personal information in authorized manner
- Data quality
- Access to personal information

Protection of personal information

Security

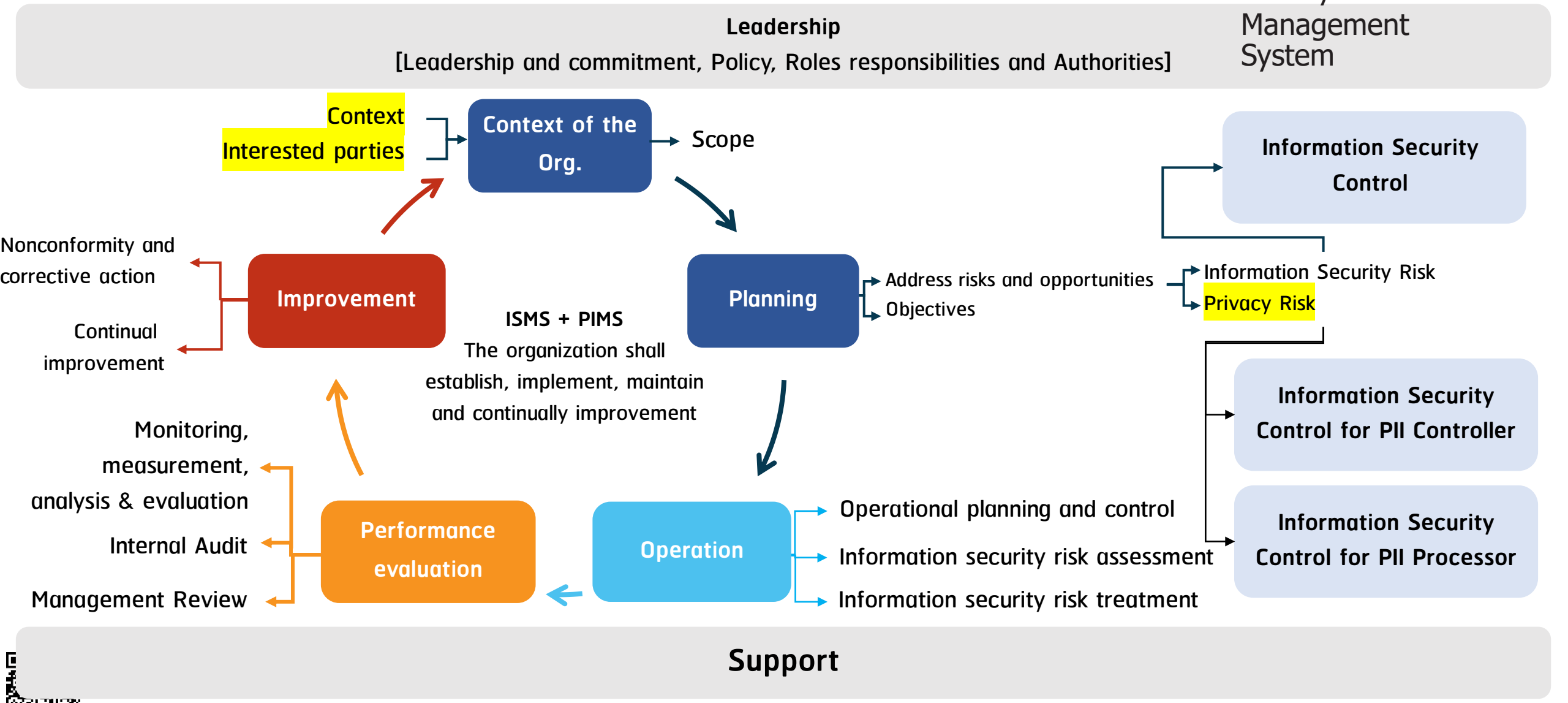
- **Confidentiality**: data being stored is safe from unauthorized access and use
- **Integrity**: data is reliable and accurate
- **Availability**: data is available for use when it is needed

ISO/IEC 27001 Framework

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

ISMS + PIMS

PIMS = Privacy Information Management System



ISMS + PIMS

Requirements	Information Security Control
1. Context of the organization 2. Leadership 3. Planning 4. Support 5. Operation 6. Performance evaluation 7. Physical and environmental security 8. Improvement	1. Information security policies 2. Organization of information security 3. Human resource security 4. Asset management 5. Access control 6. Cryptography 7. Physical and environmental security 8. Operations security 9. Communications security 10. Systems acquisition, development and maintenance 11. Supplier relationships 12. Information security incident management 13. Information security aspects of business continuity management 14. Compliance

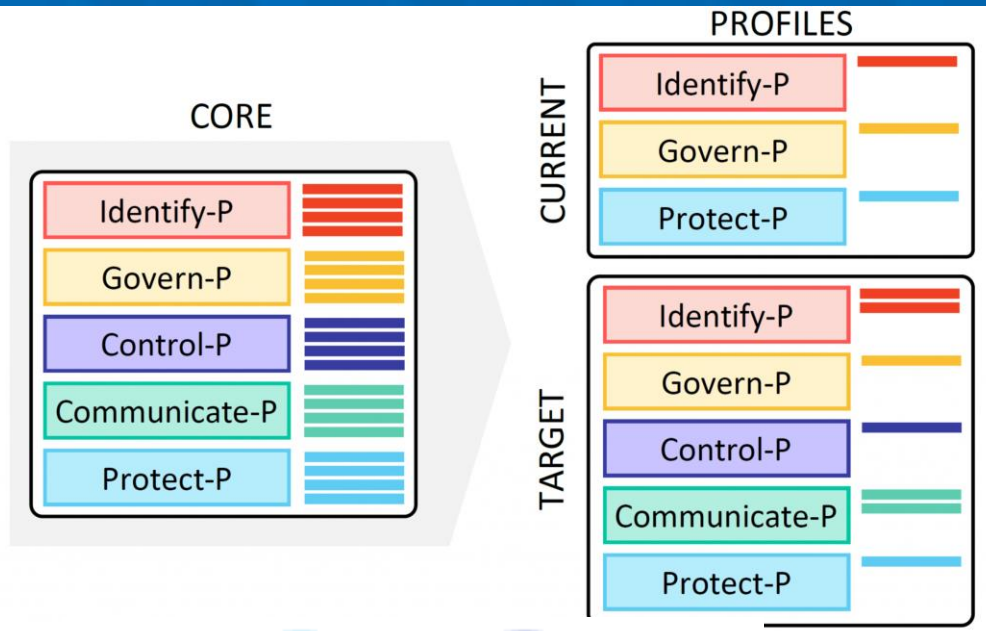
Information Security Control for PII Controller	Information Security Control for PII Processor
1. Conditions for collection and processing 2. Obligations to PII principals 3. Privacy by design and privacy by default 4. PII sharing, transfer, and disclosure	1. Conditions for collection and processing 2. Obligations to PII principals 3. Privacy by design and privacy by default 4. PII sharing, transfer, and disclosure

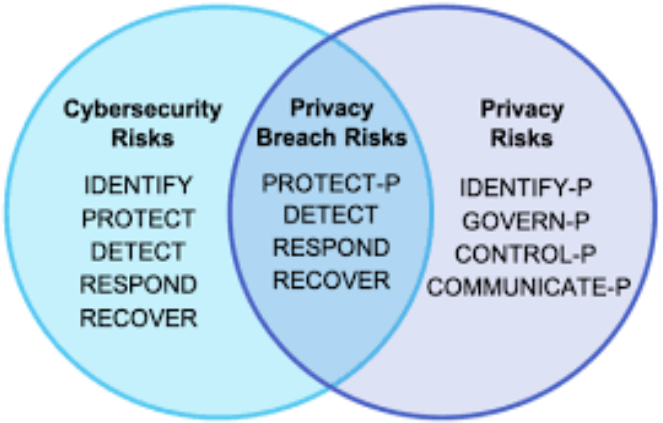
= ขยายข้อกำหนดเพิ่มเติมของ ISO/IEC 27001:2013 เพื่อคำนึงถึงการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูล PII ที่อาจได้รับผลกระทบจากการประมวลผลข้อมูล PII

PII = personally identifiable information

= ข้อแนะนำเพิ่มเติมของ ISO/IEC 27002 สำหรับผู้ควบคุมข้อมูล PII และสำหรับผู้ประมวลผลข้อมูล PII

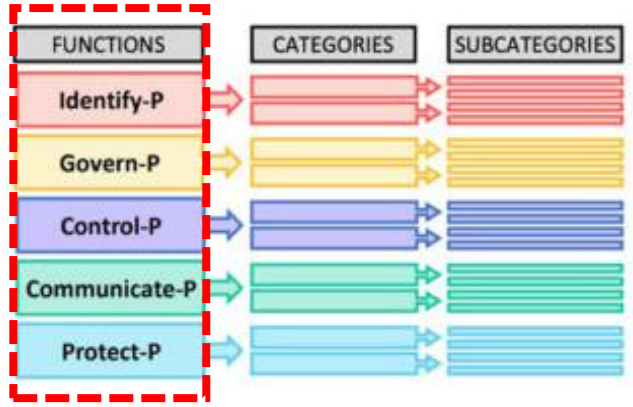
PRIVACY FRAMEWORK





อ้างอิง https://www.nist.gov/system/files/documents/2021/05/05/NIST-Privacy-Framework-V1.0-Core-PDF.pdf

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

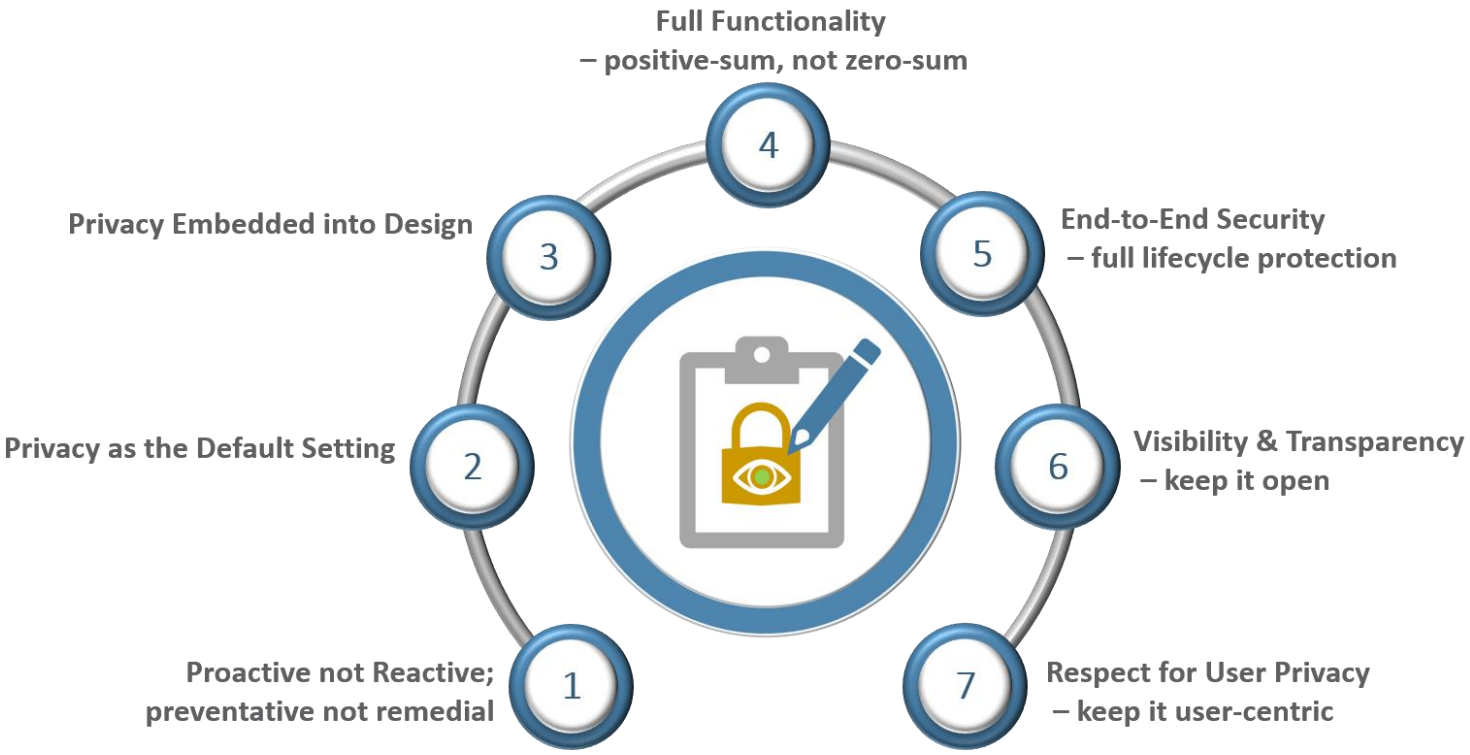


The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

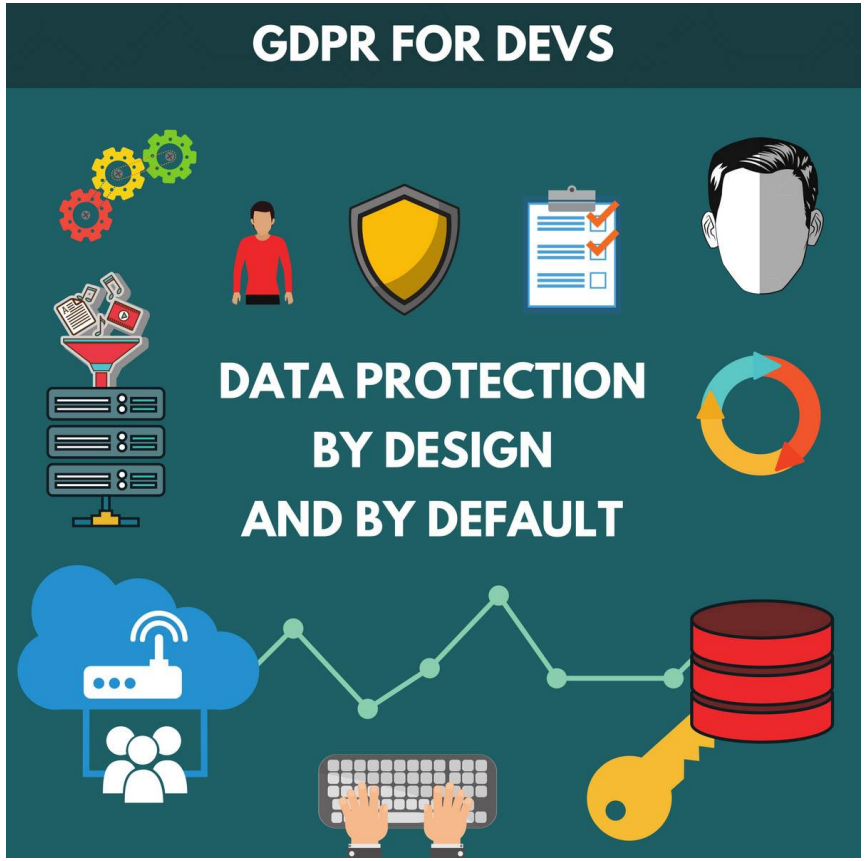
Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

Privacy by design and by default



Ref: https://www.coreio.com/gdpr-makes-a-compelling-case-for-privacy-by-design/

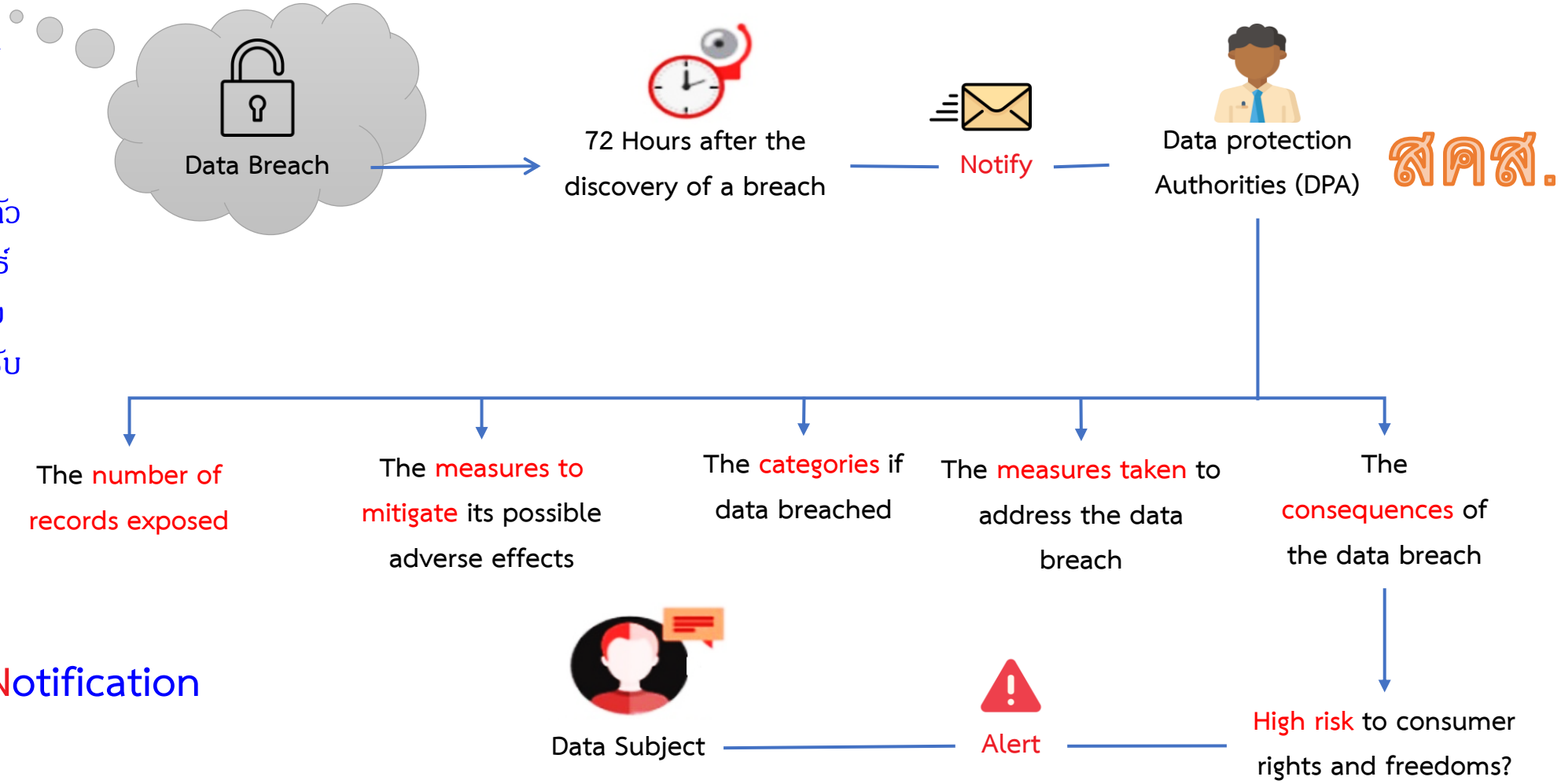


Picture by GDPR for developers

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล) มาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

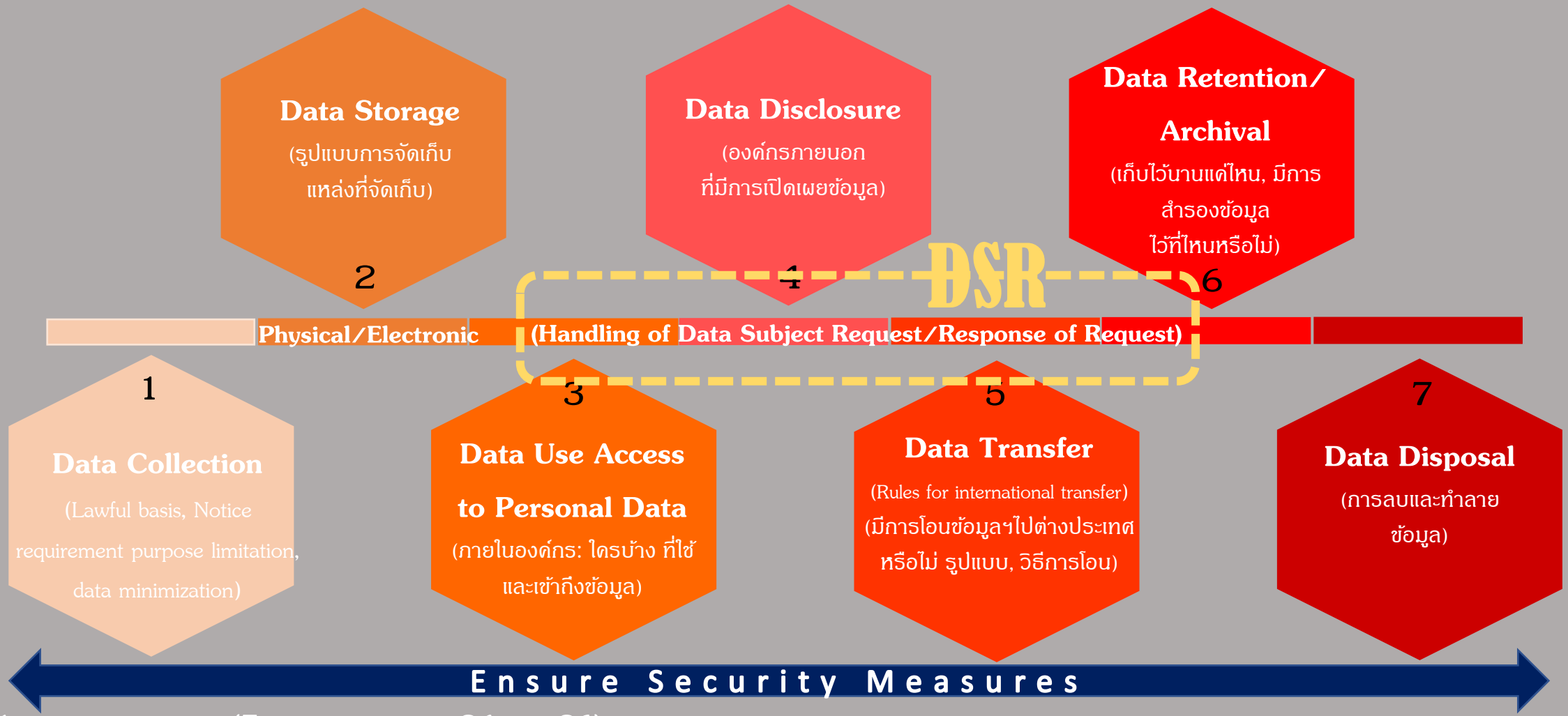
... Data Breach ได้แก่

- การเข้าถึงโดยผู้ไม่ได้รับอนุญาต
- อุบัติเหตุ/ไม่เจตนา
- ส่งไปให้ผู้รับที่ไม่ถูกตัว
- อุปกรณ์คอมพิวเตอร์สูญหายหรือถูกขโมย
- แก้ไขข้อมูลโดยไม่ได้รับอนุญาต
- ไม่มีข้อมูลใช้งาน



Data Breach Notification

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรา 30-36 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Data Subject Right

มาตรา 30 - 36

01 Right to be Informed
สิทธิที่จะได้รับการแจ้งให้ทราบ

02 Right of Access
สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล

03 Right to Data Portability
สิทธิในการได้รับและโอนถ่ายข้อมูล

04 Right to Object
สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

05 Right to Erasure
สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล

06 Right to Withdraw Consent
สิทธิในการเพิกถอนความยินยอม

07 Right to Restrict Processing
สิทธิในการขอระงับการใช้ข้อมูล

08 Right of Rectification
สิทธิขอให้แก้ไขข้อมูล

สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)

- Privacy Notice
- ชื่อและที่ติดต่อของผู้ควบคุมข้อมูล
- ชื่อและที่ติดต่อของ DPO
- วัตถุประสงค์และฐานการประมวลผล
- ผู้ใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย
- ข้อมูลอ่อนไหวที่ใช้
- ผู้รับข้อมูลส่วนบุคคล
- รายละเอียดของประเทศที่ส่งข้อมูลรวมถึงมาตรการที่ใช้
- ระยะเวลาในการจัดเก็บข้อมูล รวมถึงหลักเกณฑ์ที่ใช้
- เงื่อนไขตามกฎหมายหรือสัญญา
- แหล่งข้อมูลต้นทาง
- การประมวลผลอัตโนมัติ

สิทธิเข้าถึงข้อมูล (Right of Access)

- หนังสือรับรองการประมวลผล
- สำเนาข้อมูลส่วนบุคคล
- ข้อมูลเพิ่มเติม
- วัตถุประสงค์และฐานการประมวลผล
- ประเภทข้อมูลที่ใช้
- ผู้รับข้อมูลส่วนบุคคล
- รายละเอียดของประเทศ ที่ส่งข้อมูลรวมถึงมาตรการที่ใช้
- ระยะเวลาในการจัดเก็บข้อมูลรวมถึงหลักเกณฑ์ที่ใช้
- สิทธิของเจ้าของข้อมูล รวมถึง การเข้าถึง, แก้ไข, ลบ, ระงับ, คัดค้าน, โอน และถอน
- สิทธิในการร้องเรียนยังสำนักงาน
- แหล่งข้อมูลต้นทาง
- การประมวลผลอัตโนมัติ

สิทธิในการโอนข้อมูล (Right to Data Portability)

ข้อมูลที่ผู้ควบคุมได้รับ Structured, commonly used and machine-readable Observation (web history, traffic and location, raw data such as smart meters & wearables)

การประมวลผลด้วยฐาน ความยินยอม หรือ สัญญา

การประมวลผลด้วยระบบอัตโนมัติ

Inferred or derived data

Technical feasibility

Without hindrance

สิทธิคัดค้านการประมวลผล (Right to Object)

การตลาดแบบตรง (สิทธิเด็ดขาด)

การประมวลผลตามภารกิจของรัฐ เพื่อประโยชน์สาธารณะ เป็นการดำเนินการต่อเจ้าของข้อมูล

ประโยชน์โดยชอบของเจ้าของข้อมูลหรือบุคคลอื่น

งานวิจัย สถิติ ประวัติศาสตร์ จดหมายเหตุ

สิทธิลบข้อมูล (Right to Erasure)

- ไม่จำเป็นต้องใช้
- ได้ถอนความยินยอม
- ได้คัดค้านการประมวลผล
- ไม่มีฐานการประมวลผล
- ทำตามกฎหมาย
- ข้อมูลผู้เยาว์

- เสรีภาพในการแสดงออก
- ปฏิบัติตามกฎหมายกำหนด
- ภารกิจของรัฐ
- งานวิจัย สถิติ ประวัติศาสตร์ จดหมายเหตุ
- การใช้สิทธิตามกฎหมาย
- จำเป็นเพื่อการแพทย์

สิทธิระงับการประมวลผล (Right to Restriction)

กำลังตรวจสอบความถูกต้องของข้อมูล **สิทธิแก้ไขข้อมูลให้ถูกต้อง**

กำลังตรวจสอบประโยชน์โดยชอบด้วยกฎหมาย **สิทธิคัดค้านการประมวลผล**

ไม่มีฐานประมวลผลแต่ไม่ต้องการให้ลบ

ถูกหลักขอให้เก็บข้อมูลไว้เพื่อใช้สิทธิ์ตามกฎหมาย

ย้ายข้อมูลออกชั่วคราว

ทำให้ข้อมูลใช้งานไม่ได้

ถอนข้อมูลออกจากเว็บไซต์ชั่วคราว

สิทธิเกี่ยวข้องกับการประมวลผลอัตโนมัติ

(Right related to automated decision-making including profiling)

การประมวลผลเพื่อกำหนดวงเงินกู้

ข้อมูล หรือคำอธิบายที่สมเหตุสมผล

ป้องกันไม่ให้มีความผิดพลาด หรืออคติ

การทดสอบประเมินความสามารถด้วยโปรแกรม

ให้สิทธิโต้แย้งและทบทวนกระบวนการ

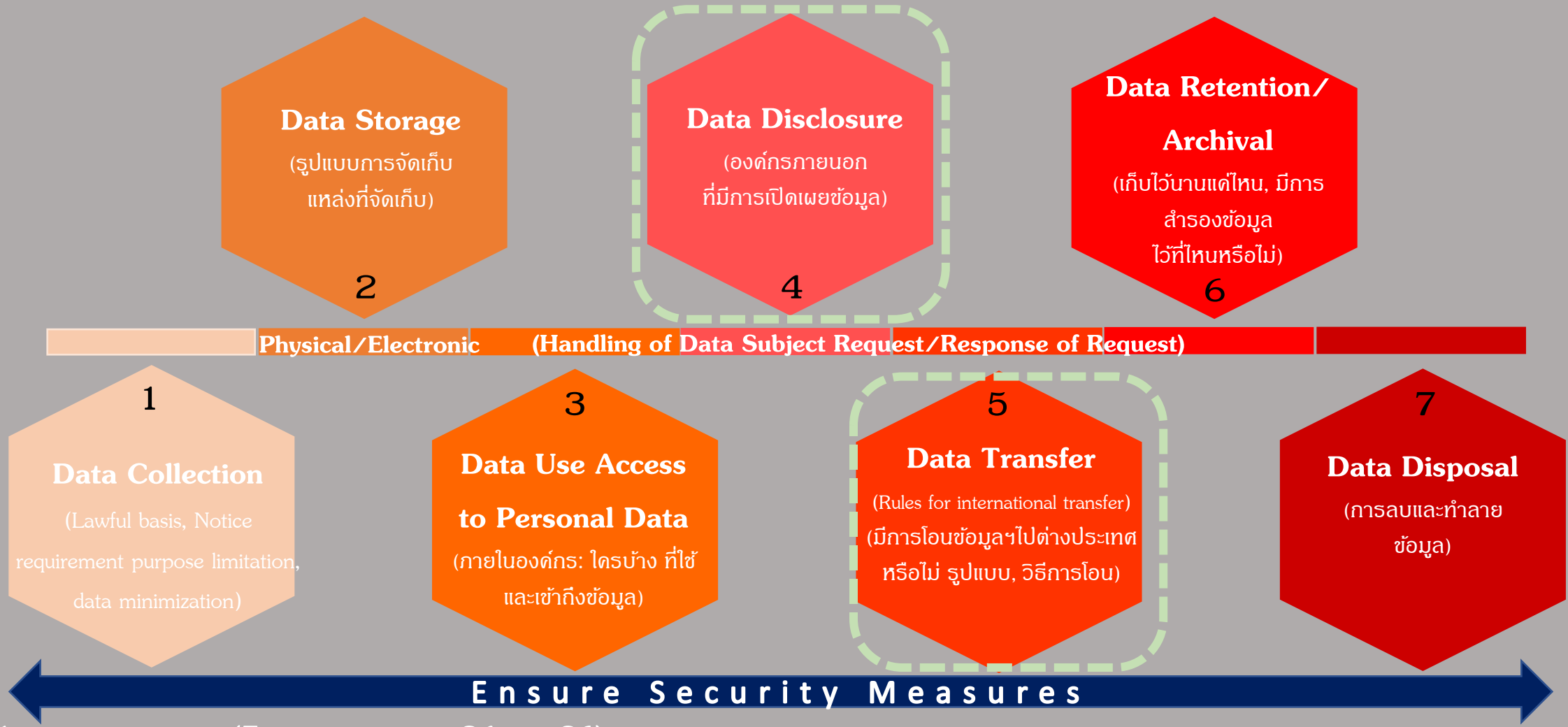
สิทธิแก้ไขข้อมูลให้ถูกต้อง (Right to Rectification)

ข้อมูลวินิจฉัยไม่ถูกต้อง

ข้อมูลความเห็น

ระงับการประมวลผล

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

สัญญาหรือข้อตกลงการประมวลผล มาตรา 40 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นจะขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

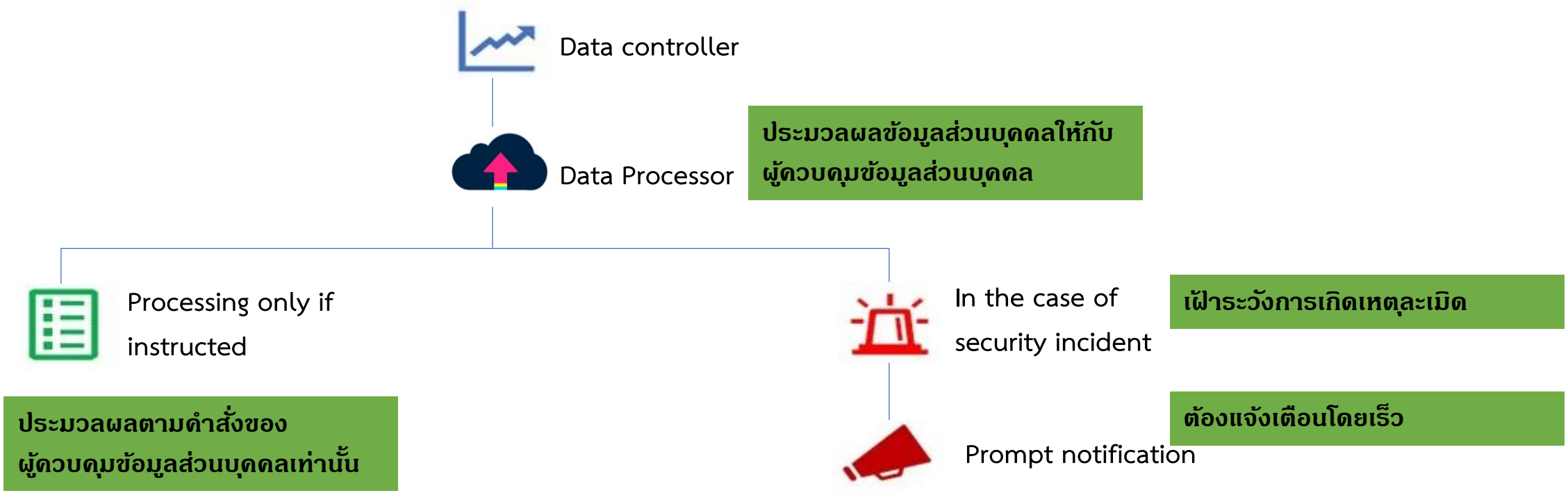
- การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

- ในการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงที่มีเงื่อนไขอย่างน้อย ดังต่อไปนี้

  1. ต้องมีข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ
  2. มีข้อตกลงเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
  3. มีข้อตกลงเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
  4. มีข้อตกลงเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

Data Processing Agreement

To what extent personal data will be processed and what if there is an accident?



ตัวอย่าง

(เพื่ออำนวยความสะดวกแก่หน่วยงาน และองค์กรนำไปพิจารณาใช้เป็นต้นแบบ)

(เวอร์ชั่นกำกับ A.5.1)

DGA

Logo คู่สัญญา

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

โครงการ.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก).....

ระหว่าง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กับ.....(ชื่อคู่สัญญา).....

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ("ข้อตกลง") ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนามในข้อตกลง)..... ณ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

โดยที่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า "สพร." ฝ่ายหนึ่ง ได้ตกลงใน....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า "(บันทึกความร่วมมือ/สัญญา)" กับ ..... (ระบุชื่อคู่สัญญา)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า ".....(ระบุชื่อเรียกคู่สัญญา....." อีกฝ่ายหนึ่ง

ตาม (ระบุชื่อบันทึกความร่วมมือ/สัญญาหลัก) ดังกล่าวกำหนดให้ สพร. มีหน้าที่และความรับผิดชอบในส่วนของการ.....(ระบุขอบเขต สิทธิ หน้าที่ของ สพร. ตามบันทึกตวามร่วมมือ/สัญญาหลัก)..... ซึ่งในการดำเนินการดังกล่าวประกอบด้วยการมอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา).....เป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย ("ประมวลผล") ข้อมูลส่วนบุคคลแทนหรือในนามของ สพร.

สพร. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบและกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ได้.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้..... (ระบุชื่อคู่สัญญา).....ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ..... (ระบุวัตถุประสงค์ที่ สพร. มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เพื่อการรับจ้างทำระบบยืนยันตัวตน เพื่อการรับทำ Survey เพื่อการลงทะเบียนผู้เข้าร่วมงานสัมมนา เพื่อการรับจ้างพิมพ์บัตรพนักงาน เพื่อการรับส่งเอกสาร เป็นต้น).....

๒. .....

โดยข้อมูลส่วนบุคคลที่ สพร. มอบหมาย.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้.... (ระบุชื่อคู่สัญญา).....ประมวลผล ประกอบด้วย

๑. ..... (ระบุรายการข้อมูลส่วนบุคคลที่ สพร. มอบหมาย/เปิดเผยให้คู่สัญญาประมวลผล เช่น ชื่อนามสกุลของเจ้าหน้าที่ เบอร์โทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชั่นทางรัฐ รายชื่อผู้เข้าร่วมงานสัมมนา เป็นต้น).....

๒. .....

ด้วยเหตุนี้ ทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือข้อตกลงฉบับนี้เป็นส่วนหนึ่ง....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่ สพร. มอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา)..... ดำเนินการ อันเนื่องมาจากการดำเนินการตามหน้าที่และความรับผิดชอบตาม.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า "กฎหมายคุ้มครองข้อมูลส่วนบุคคล" ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๓. ..... (ระบุชื่อคู่สัญญา)..... รับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดย..... (ระบุชื่อคู่สัญญา)..... จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

โดยในการดำเนินการตามข้อตกลงนี้ ..... (ระบุชื่อคู่สัญญา).....จะประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก สพร. แล้วเท่านั้น ทั้งนี้ เพื่อให้ปราศจากข้อสงสัย การดำเนินการประมวลผลข้อมูลส่วนบุคคลโดย..... (ระบุชื่อคู่สัญญา).....ตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....ถือเป็นการได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก สพร. แล้ว

ตัวอย่าง

(เพื่ออำนวยความสะดวกแก่หน่วยงาน และองค์กรนำไปพิจารณาใช้เป็นต้นแบบ)

(เวอร์ชั่นกำกับ B.1.1)

DGA Digital Government Development Agency สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Logo คู่สัญญา

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล

(Personal Data Sharing Agreement)

ระหว่าง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กับ...(ชื่อคู่สัญญาอีกฝ่าย)....

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (“**ข้อตกลง**”) ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนาม ในข้อตกลง) ..... ณ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

โดยที่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**สพร.**” ฝ่ายหนึ่ง ได้ตกลงใน.... (ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก) .... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**สัญญาหลัก**” กับ ..... (ระบุชื่อคู่สัญญาอีกฝ่าย) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “..... (ระบุชื่อเรียกคู่สัญญาอีกฝ่าย .....” อีกฝ่ายหนึ่ง รวมเรียกว่า “**คู่สัญญา**”

เพื่อให้บรรลุวัตถุประสงค์ภายใต้ความตกลงของสัญญาหลัก คู่สัญญามีความจำเป็นต้องแบ่งปัน โอน แลกเปลี่ยน หรือเปิดเผย (รวมเรียกว่า “**แบ่งปัน**”) ข้อมูลส่วนบุคคลที่ตนเก็บรักษาแก่อีกฝ่าย ซึ่งข้อมูลส่วนบุคคลที่แต่ละฝ่าย เก็บรวมรวม ใช้หรือเปิดเผย (รวมเรียกว่า “**ประมวลผล**”) นั้น แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือแต่ละฝ่ายต่างเป็นผู้มีอำนาจตัดสินใจกำหนดรูปแบบ และกำหนดวัตถุประสงค์ ในการประมวลผลข้อมูลส่วนบุคคลในข้อมูลที่ตนต้องแบ่งปัน ภายใต้ข้อตกลงนี้

ด้วยเหตุนี้ คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อเป็นหลักฐานการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญาและเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้ และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. คู่สัญญารับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยคู่สัญญาแต่ละฝ่าย จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การ ประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ข้อมูลส่วนบุคคลที่คู่สัญญาแบ่งปันกัน คู่สัญญาแต่ละฝ่ายตกลงแบ่งปันข้อมูลส่วนบุคคลดังรายการต่อไปนี้แก่คู่สัญญาอีกฝ่าย

ข้อมูลส่วนบุคคลที่แบ่งปันโดย สพร.	วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล
1. (ระบุรายการข้อมูลส่วนบุคคลที่ สพร. แบ่งปันให้คู่สัญญาอีกฝ่าย เช่น ชื่อ นามสกุลของเจ้าหน้าที่ หมายเลขโทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชันทางรัฐ)	1. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคล ระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)
2. ...	2. ...
3.	3.
ข้อมูลส่วนบุคคลที่แบ่งปัน~~เปิดเผยหรือโอน~~โดย (ระบุชื่อคู่สัญญาอีกฝ่าย)	**วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล**
1. (ระบุรายการข้อมูลส่วนบุคคลที่คู่สัญญาอีกฝ่ายแบ่งปันแก่ สพร. เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ ข้อมูล Location)	1. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคล ระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)

ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer)

- **Adequacy Decision (มาตรา 28 วรรค 1)**
- **Appropriate Safeguards**

  Legal binding instrument between public authorities (1)

  Binding corporate rules (1)
- **Derogations**

  Legal claim (1)

  Explicit consent (2)

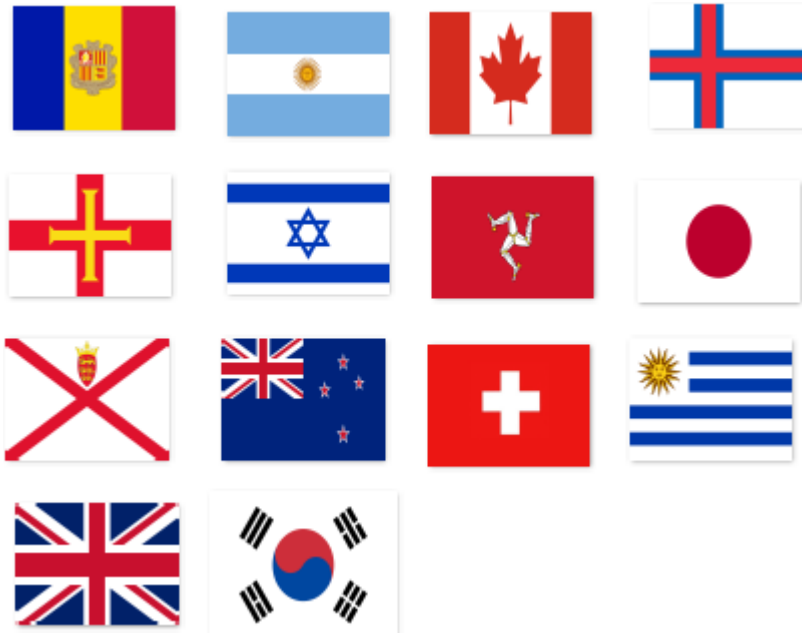
  Necessary for pre-contractual measures (3)

  Necessary for data subject's interest (4)

  Vital interest (5)

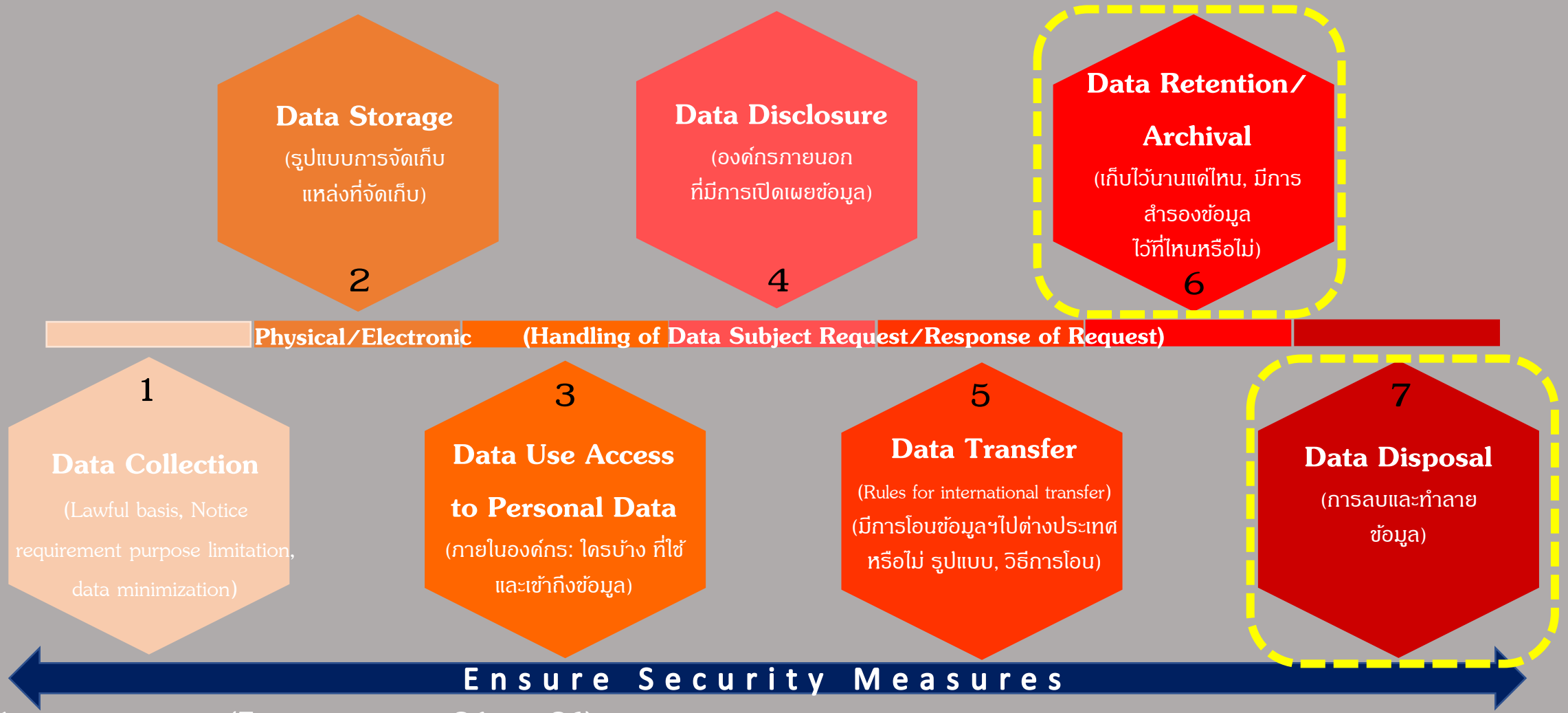
  Important Public Interest (6)

Adequacy Decision (European Commission) [25 February 2022] Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, **Japan**, Jersey, New Zealand, Switzerland, Uruguay, the United Kingdoms, South Korea



Binding Corporate Rules (BCRs) เป็นหลักการที่ให้ธุรกิจในเครือ (Intra-Group Companies) ที่ประกอบธุรกิจ ทั้งในและนอกสหภาพยุโรป สามารถโอนข้อมูลส่วนบุคคลระหว่างกันได้โดยอิสระ และได้รับความคุ้มครองข้อมูล ส่วนบุคคลตามกฎหมายฉบับนี้ถึงแม้บริษัทในเครือบางแห่งจะประกอบธุรกิจในประเทศที่อยู่นอกสหภาพยุโรปก็ตาม

วงจรชีวิตข้อมูลส่วนบุคคล



1.ฐานทางกฎหมาย (7 ฐานตามมาตรา 24 และ 26)

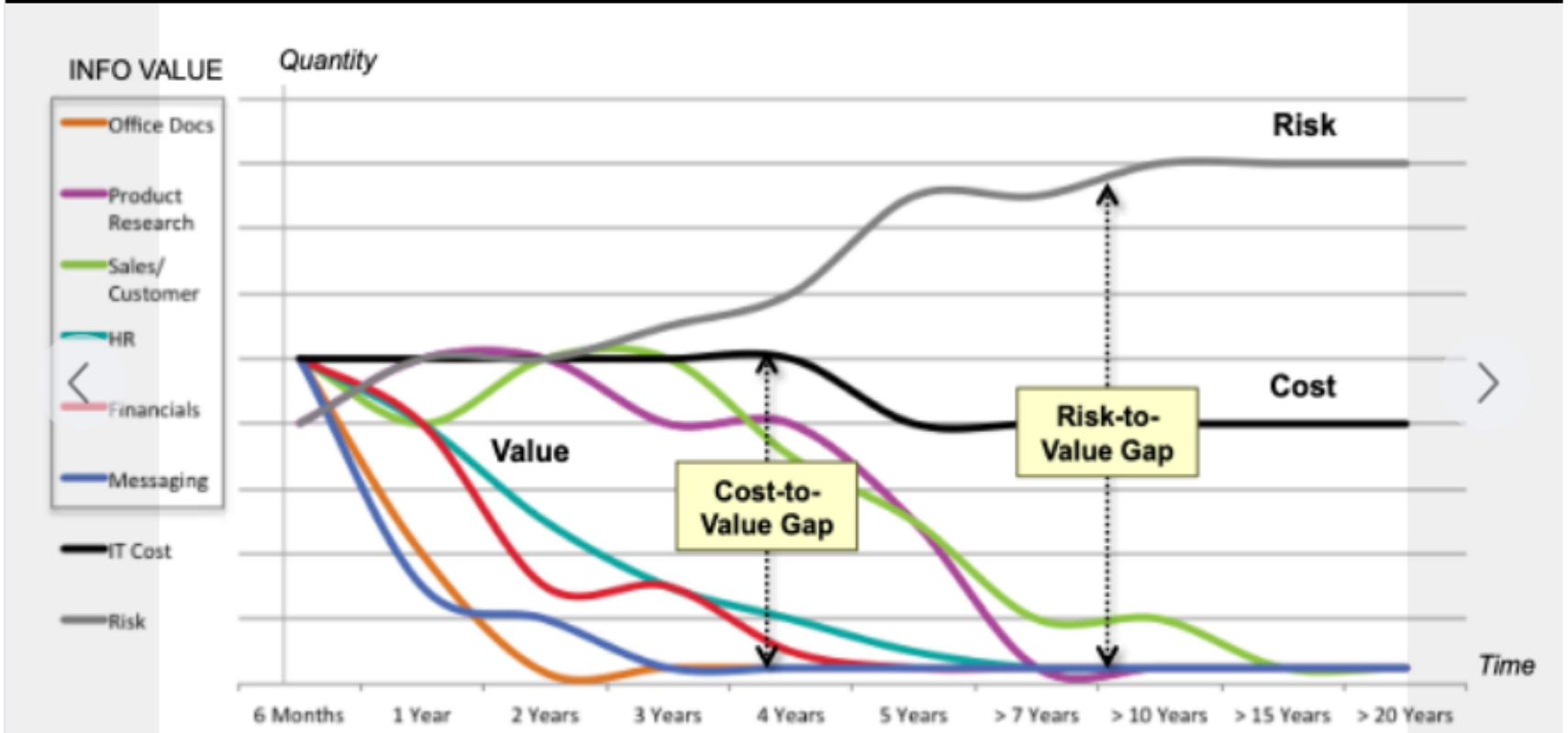
2.การแจ้ง (ม.23 Privacy Notice)

3.วัตถุประสงค์จำกัด (ม.21)

4.ใช้ข้อมูลน้อยที่สุด (ม.22)

“The best way to reduce the amount of data… delete it.”

Gartner



PrivacyNote
17 เมษายน เวลา 06:52 น. ·

"The best way to reduce the amount of data -- delete it."
- Sheila Childs, Research Vice President, Gartner

ข้อมูลทั้งหมดที่เก็บอยู่ในองค์กรนั้น

มีเพียง 1% ที่ต้องเก็บรักษาข้อมูลตามกฎหมาย
5% ต้องเก็บบันทึกเพื่อการกำกับดูแลกิจการ
25% เป็นข้อมูลที่ต้องใช้ในการดำเนินกิจกรรมทางธุรกิจ
ส่วนที่เหลืออีก 69% ไม่มีประโยชน์ใดๆเลย และทำให้เกิดต้นทุนในการเก็บรักษาและความเสี่ยงกับธุรกิจ

Source: Information Lifecycle Governance Leader Reference Guide (https://cedar.princeton.edu/.../information_lifecycle...) **ดูน้อยลง**

6 แชร์ 3 ครั้ง

credit: #PrivacyNote

ตัวอย่าง Data Retention Policy

DATA
PROTECTION
UAS

Guidelines on the retentic

Introduction

Why do we need a data retention policy?

- We need to comply with the requirement of the General Data Protection Regulat personal data is not kept for longer than necessary. If we retain personal data for we need to, we will also breach the requirement that personal data must be relev limited to what is necessary to meet our purposes.
- We need to keep data for as long as it is required to meet operational purposes o organisational archiving relating to scientific, historical research or statistical purp
- We need to make best use of storage space, both physical and digital.

Scope

- This guidance seeks to provide indicative guidance for those responsible for mana student records and student administration. It covers the main corporate system SITS, CMIS, GSR, OXCORT, DWH, and local Access databases, Excel spreadsheets, paper, for example, interview scores held locally in a departmental database.
- Data extracted from master systems and stored in local drives or email should be after use to avoid unnecessary duplication, and to ensure data is not held for any necessary.
- Excluded: Retention guidelines for maintaining transactional records, for example of requests for transcripts.

Retention periods

- The master copy of data should not be deleted before the expiry of the retention Supplementary copies (e.g. Excel downloads, or working files) should be deleted retention period if they no longer serve a purpose. Careful consideration should b to whether supplementary copies of data should be held or could be destroyed.
- When the retention period is reached, the data should be destroyed as soon as p and in a secure manner.

Issued by Student Registry
September 2021

University of Oxford: Guidelines on the retention of student data and records **September 2021**

ID	Sub-category	Purpose	data example	Where processed	Retention Period	Retention Record Owner
A.6.2	Application decisions (departments): unsuccessful candidates; successful candidates who don't enrol	Information on application decisions	departmental decisions, offers (local administration)	Paper copies in departments, local electronic records for distribution and storage (PDF, Excel and Word)	End of the admissions cycle in which applied plus one year for full records. Permanent: anonymised skeleton records without supporting documentation.	Departments
A.7.1	Data in application system: Application for postgraduate courses not submitted	Data saved to enable applicants to continue with their application	previous qualifications, previous education, supporting statements, references, personal data covered under Person (section F).	SITS & eVision, paper copies in central teams	Current admissions cycle + 1 year for full records.	GAR
A.7.2	Data for application for postgraduate courses not submitted (colleges)	Information to enable applicants to complete their application if submitted	previous qualifications, previous education, supporting statements, references, personal data covered under Person (section F).	Paper copies in colleges, local electronic records for distribution and storage (PDF, Excel and Word)	Current admissions cycle + 1 year for full records.	Colleges
A.7.3	Data for applications for postgraduate courses not submitted (departments)	Information to enable applicants to complete their application if submitted	previous qualifications, previous education, supporting statements, references, personal data covered under Person (section F).	Paper copies in departments, local electronic records for distribution and storage (PDF, Excel and Word)	Current admissions cycle + 1 year for full records.	Departments
A.8	Data in applications for postgraduate courses: All records	Information to enable survey invitations to be sent to applicants, information received in survey responses	Name, course applied to, other institutions applied to	Online surveys (formerly BOS), Excel	End of the admissions cycle in which applied plus one year for full records. Permanent: anonymised skeleton records without supporting documentation.	GAR

ตัวอย่างนโยบายระยะเวลาการเก็บรักษาข้อมูลและการทำลายข้อมูล

- เกริ่นนำ
- บทนิยาม
  - ระยะเวลาในการจัดเก็บ หมายถึง
  - การทำลาย หมายถึง
- กำหนดระยะเวลาในการจัดเก็บข้อมูลขององค์กร

ที่	ประเภทข้อมูล	สื่อที่ใช้จัดเก็บ	ระยะเวลาในการจัดเก็บ
1	บันทึกภาพ CCTV	ฐานข้อมูลระบบ CCTV	30 วัน (เขียนทับ)
2	ผู้สมัครงาน	กระดาษ	1 ปี

- กำหนดวิธีการในการทำลายข้อมูล

ประเภทสื่อบันทึกข้อมูล	วิธีการลบ ทำลาย
กระดาษ	ทำลายด้วยเครื่องทำลายเอกสารที่ไม่สามารถนำซากเอกสารที่ทำลายแล้วมาประกอบและอ่านข้อมูลได้อีก และสอดคล้องตามวิธีการที่ระเบียบสารบรรณกำหนด
สื่อบันทึกข้อมูลเคลื่อนที่ได้	ทุบ ทำลายให้สิ้นซาก

Workflow Privacy Guideline

การเก็บรวบรวมข้อมูลส่วนบุคคล

- การจัดทำและปรับปรุงบันทึกกิจกรรม การประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities)
- การกำหนดวัตถุประสงค์ การประมวลผลข้อมูลส่วนบุคคล
- การกำหนดฐาน การประมวลผลข้อมูลส่วนบุคคล
- การบริหารจัดการความยินยอม
- การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล
- การประเมินผลกระทบ ด้านการคุ้มครองข้อมูลส่วนบุคคล

การใช้ข้อมูลส่วนบุคคล

- การใช้ข้อมูลส่วนบุคคล
- มาตรการรักษาความมั่นคง ปลอดภัยสารสนเทศ
- การจัดทำข้อตกลง การประมวลผลข้อมูลส่วนบุคคล
- การบริหารจัดการสิทธิ ของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management)
- การรายงานเหตุละเมิด ข้อมูลส่วนบุคคล

การเผยแพร่ หรือ ส่งต่อข้อมูลส่วนบุคคล

- หลักเกณฑ์การโอนข้อมูลส่วนบุคคล ไปยังต่างประเทศหรือองค์กรระหว่างประเทศ
- การได้รับการยกเว้น ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและ สามารถโอนย้ายข้อมูลไปยังต่างประเทศได้
- ขั้นตอนปฏิบัติสำหรับการจัดส่ง ข้อมูลส่วนบุคคลไปยังต่างประเทศ
- ขั้นตอนปฏิบัติสำหรับการร้องขอ ข้อมูลส่วนบุคคลจากหน่วยงานภายนอก

การเก็บรักษา และ การทำลายข้อมูลส่วนบุคคล

- มาตรการเชิงเทคนิค เพื่อแปลงข้อมูลที่จัดเก็บไว้เป็นข้อมูล อย่างอื่นเพื่อรักษาความปลอดภัยของข้อมูล
- ขั้นตอนปฏิบัติสำหรับการลบ หรือทำลายข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา 41-42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Data Protection Officer

มาตรา 41 - 42

- ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้
  - เป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
  - การดำเนินกิจกรรมที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
  - กิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย
- ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานทราบ
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงาน หรือเป็นผู้รับจ้างให้บริการตามสัญญาก็ได้
- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา 41-42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 41 - 42

Data Protection Officer

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
  - ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้
  - ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
  - ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
  - รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่
- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ไม่ได้
- กรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

หน้าที่ความรับผิดชอบของ DPO

1. **กำหนดขอบเขตงานและจัดทำแผนผังแสดงภาพรวมการไหลของข้อมูล**ในกิจกรรมการประมวลผลขององค์กร
2. **ให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลขอมูลสวนบุคคล** และทบทวนกิจกรรมการประมวลผลขอมูลสวนบุคคล
3. **ติดตามผลการประเมินความเสี่ยงหรือผลการประเมินผลกระทบต่อข้อมูลส่วนบุคคล**จากหน่วยงานต่าง ๆ เพื่อพิจารณาให้ข้อคิดเห็นตามความจำเป็น
4. **กำหนดแนวทางการรับมือต่อเหตุละเมิดข้อมูลส่วนบุคคล** และแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
5. **กำหนดแนวทางการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล**
6. **ให้คำแนะนำและคำปรึกษารวมถึงสร้างความตระหนัก**เกี่ยวกับการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล แก่หน่วยงานต่าง ๆ
7. **ตรวจสอบและทบทวนการดำเนินงานการประมวลผลข้อมูลส่วนบุคคล**ของหน่วยงานต่าง ๆ ให้มีความสอดคล้องตามวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลที่กำหนดไว้ และไม่ละเมิดกฎหมาย ระเบียบข้อบังคับ
8. **ติดตามการเปลี่ยนแปลงด้านกฎหมาย** มาตรการ กฎระเบียบต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูล
9. ประสานงานและให้ความ**ร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**ตามความจำเป็น
10. **รักษาความลับ**ของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่
11. รายงานไปยังคณะกรรมการกำกับดูแลข้อมูลส่วนบุคคลและผู้บริหารขององค์กรในกรณีที่เกิดปัญหาในการปฏิบัติหน้าที่
12. หน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

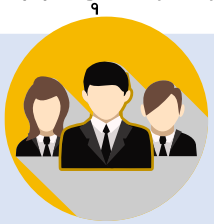
อ้างอิงจากเอกสาร: Thailand Data Protection Guidelines 3.0

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

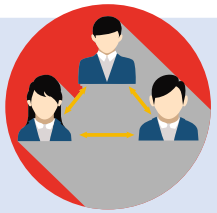
แนวปฏิบัติในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

องค์กรสามารถแต่งตั้ง DPO เป็นตัวบุคคลหรือคณะบุคคลก็ได้ แล้วแต่ความเหมาะสมและบริบทขององค์กร

การแต่งตั้ง DPO เป็น**ตัวบุคคล**จะทำให้**มีอำนาจตัดสินใจอย่างเบ็ดเสร็จเด็ดขาด**แต่ต้องมีทักษะความรู้ความสามารถหลายด้านประกอบกันจึงอาจเป็นการยากลำบากที่จะหาบุคคลที่มีความรู้ครอบคลุมทุกด้านได้ในคนเดียวกัน



การแต่งตั้ง DPO เป็น**คณะบุคคล**จะสามารถแก้ไขปัญหาเรื่องการหาคนที่มีทักษะความรู้พร้อมทุกด้านในคนเดียวกันได้ แต่จะ**เกิดปัญหาเรื่องอำนาจในการตัดสินใจขึ้น** หากแต่ละท่านมีความเห็นไม่ตรงกัน

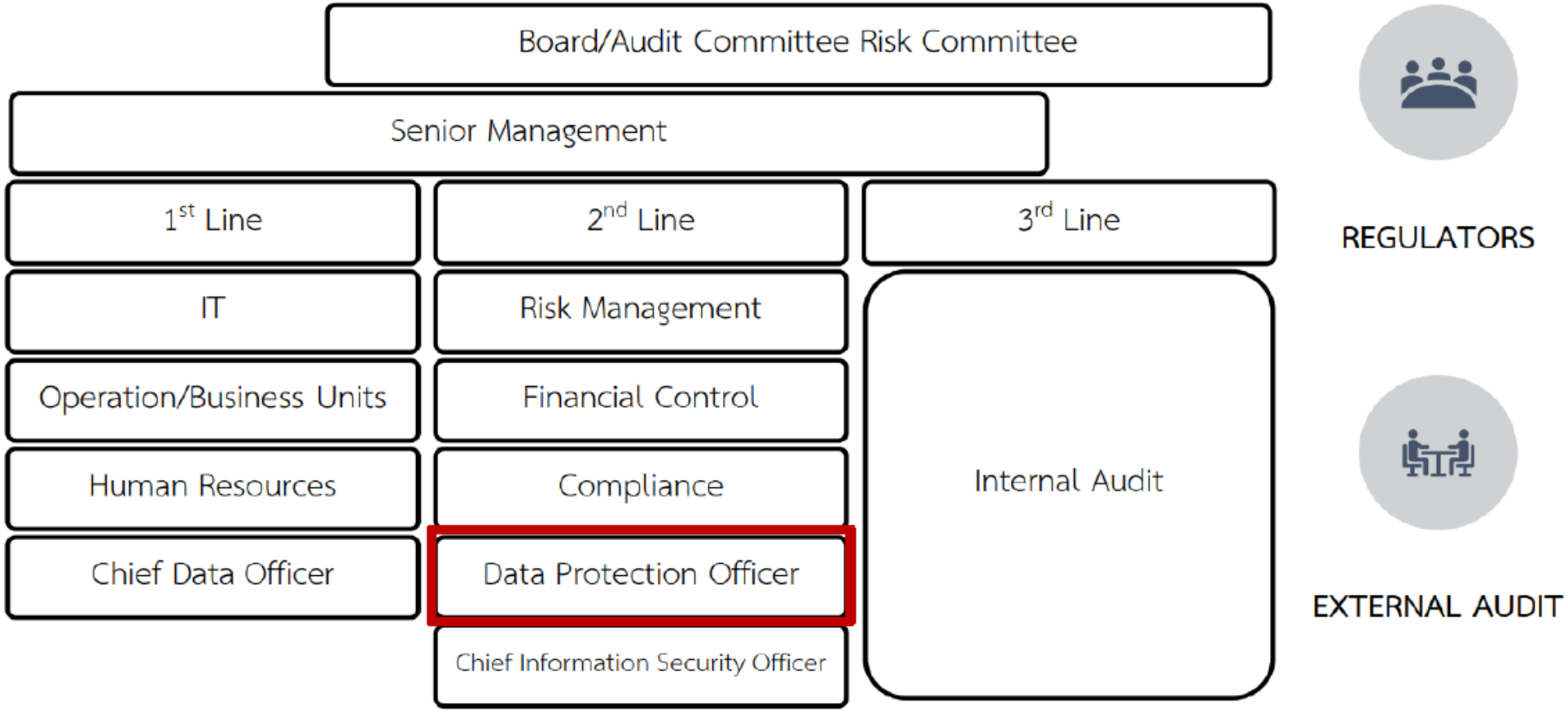


แนวทางการแก้ปัญหาอาจทำได้โดยการแต่งตั้ง DPO ขึ้นมาเพียงคนเดียวและ**มีทีมที่ประกอบไปด้วยบุคคลที่มีความรู้ความสามารถหลากหลายด้าน**ที่สำคัญต่อการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้คำแนะนำปรึกษาและช่วยคิดก่อนการตัดสินใจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

Note: เพื่อหลีกเลี่ยง COI จนท.DPO ไม่ควรมีส่วนในการตัดสินใจต่อวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

อ้างอิงจากเอกสาร: Thailand Data Protection Guidelines 3.0

DPO in Three line of defense



Thailand Data Protection Guidelines 3.0

Penalty

โทษอาญา จำคุกไม่เกิน 1 ปี
ปรับไม่เกิน 1,000,000 บาท

โทษทางปกครอง
ปรับไม่เกิน 5,000,000 บาท

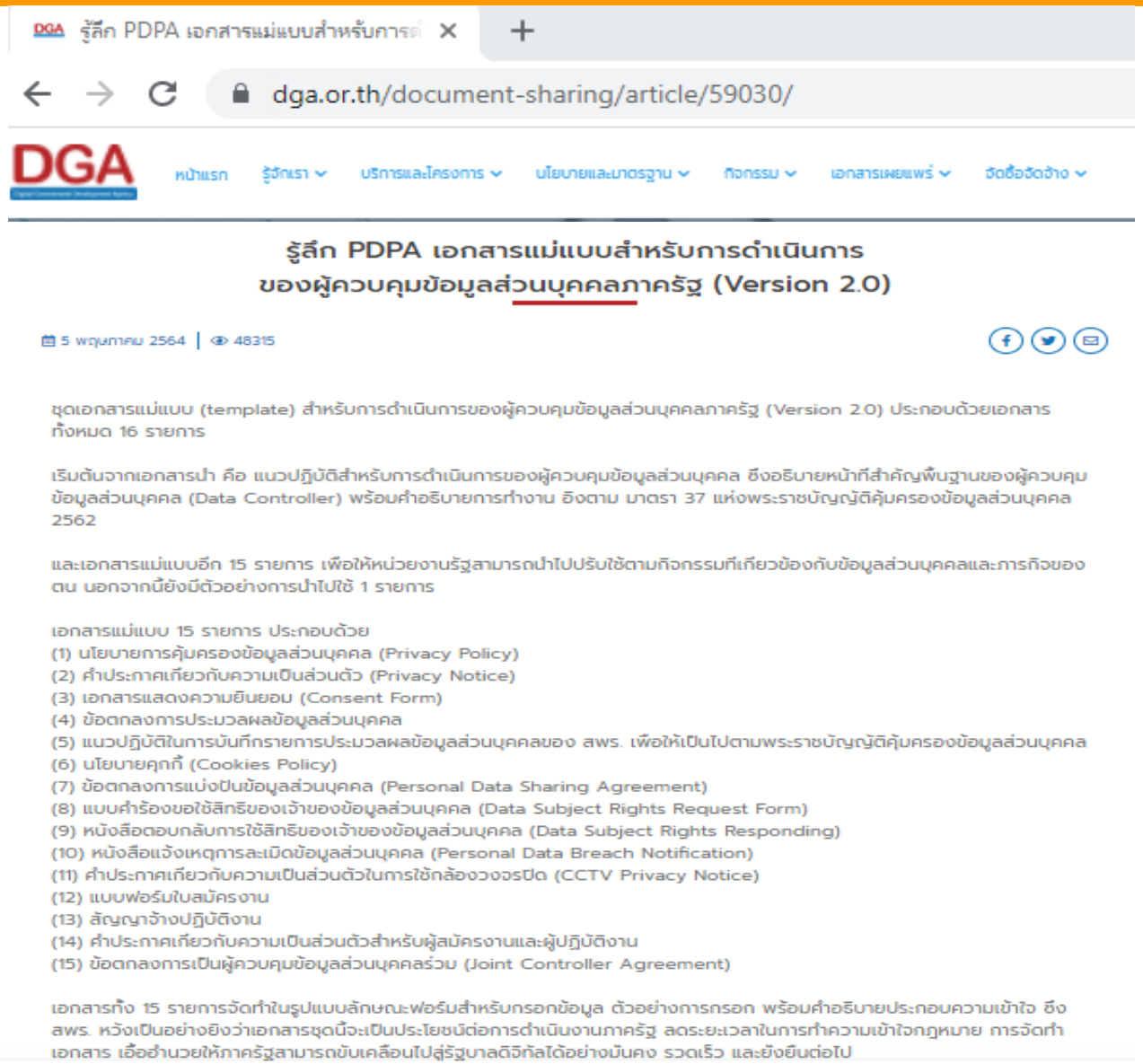
ความรับผิดทางแพ่ง 2x
ค่าสินไหมทดแทน

สิ่งที่ควรเตรียมพร้อม
ก่อน PDPA ใช้บังคับ

Source: RSAConference 2018

ตัวอย่าง Template เอกสารเพื่อปฏิบัติให้สอดคล้องตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

https://www.dga.or.th/document-sharing/article/59030/



แหล่งอ้างอิงสำหรับการดำเนินการเพื่อให้สอดคล้องกับพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

TDPG 3.0 Thailand Data Protection Guidelines 3.0 – Business Functions แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 3.0

เปิดรับสมัคร/Upcoming โครงการอบรม

22 ธันวาคม 2563

ดาวน์โหลดเอกสาร

- **TDPG 3.0 Thailand Data Protection Guidelines 3.0**

แหล่งอ้างอิงสำหรับการดำเนินการเพื่อให้สอดคล้องกับพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

เผยแพร่ ณ วันที่ 28 เมษายน 2564

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

https://www.tba.or.th/wp-content/uploads/2021/04/Guideline-on-Personal-Data-Protection-for-Thai-Banks-final-Version-MS-TH-28042021-%E0%B8%AA%E0%B8%B5%E0%B8%99%E0%B9%89%E0%B8%B3%E0%B9%80%E0%B8%87%E0%B8%B4%E0%B8%99.pdf

แหล่งอ้างอิงสำหรับการดำเนินการเพื่อให้สอดคล้องกับพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

บริษัท ที-เน็ต จำกัด
121 หมู่ 9 อาคาร Garden of Innovation ห้องเลขที่ 1-11 อุทยานวิทยาศาสตร์ประเทศไทย
ถนนพหลโยธิน คลองหนึ่ง คลองหลวง ปทุมธานี 12120
โทรศัพท์: 02-564-7886 โทรสาร: 02-564-7854
e-mail: doungkamol@tnetsecurity.com