



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ETDA
สพด
www.etda.or.th

Personal Data Protection for Service Providers in e-Commerce ecosystem

Soontaree Songserm, Ph.D.
Ministry of Digital Economy and Society

16 December 2020



การคุ้มครองข้อมูลส่วนบุคคลในโลกยุคใหม่



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



การเตรียมความพร้อมเพื่อปฏิบัติตามกฎหมาย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

“มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงพอเพื่อประโยชน์สาธารณะ”

GDPR – General Data Protection Regulation

กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป บังคับใช้เมื่อ 25 พฤษภาคม 2561 มีการบังคับใช้แบบขยายหลักดินแดน (Extraterritorial Scope) คือ ใช้บังคับกับผู้ประกอบการที่ประมวลผลข้อมูลส่วนบุคคลของคนยุโรป แม้ว่าจะไม่มีสถานประกอบการตั้งอยู่ในสหภาพยุโรป

International Ranking

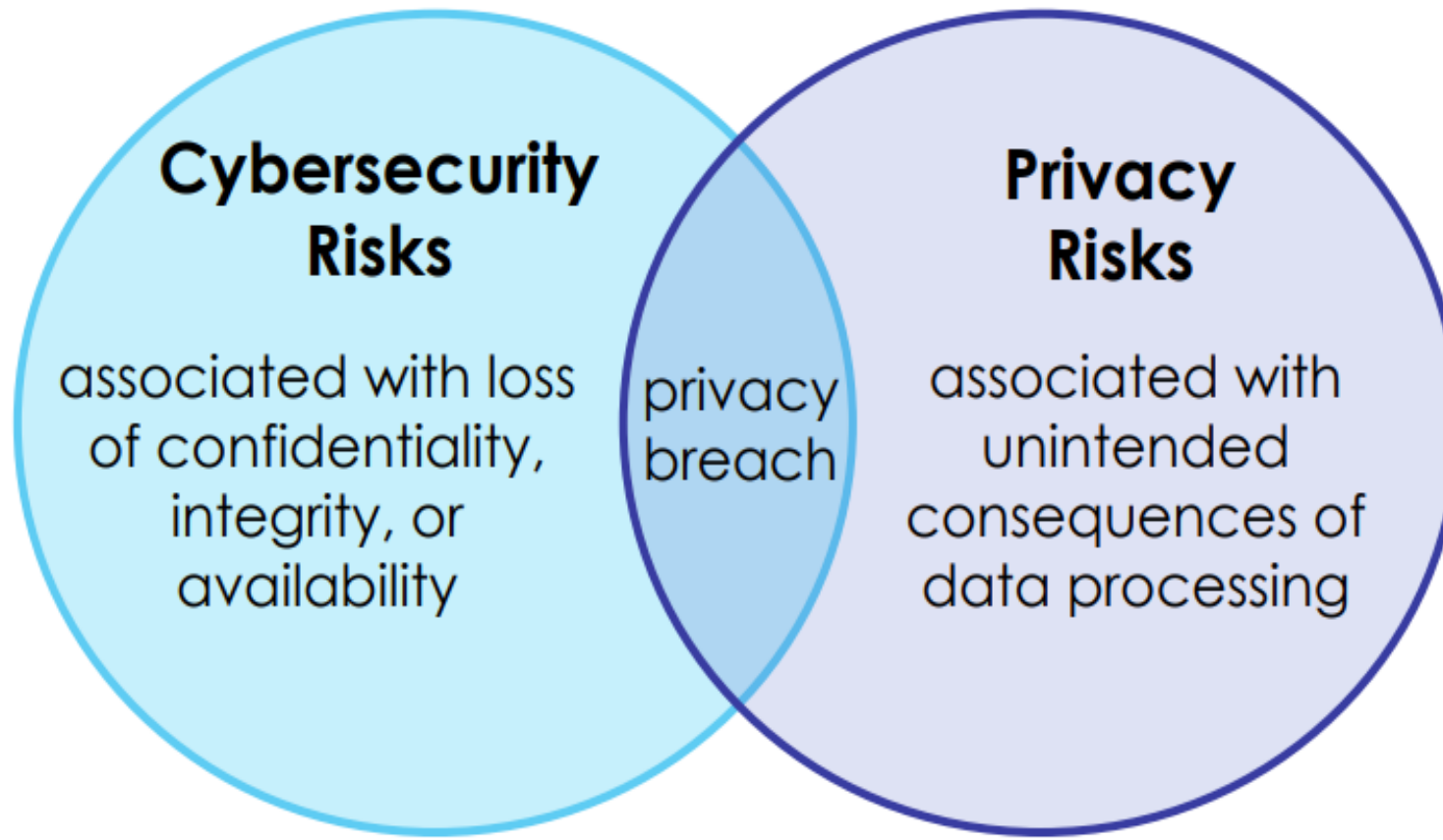
- ITU Global Cybersecurity Index

ไทยได้รับการจัดอันดับความน่าเชื่อถือด้านความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติ ตั้งแต่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- WEF Digital Competitiveness Ranking

ไทยได้รับการจัดอันดับความสามารถในการแข่งขันด้านดิจิทัล ของ World Economic Forum ในด้าน Cyber Security ดีขึ้นตั้งแต่ปี 2018

Relationship Between Cybersecurity and Privacy Risk



Data: A representation of information, including digital and non-digital formats

Data Action: A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

“ข้อมูลส่วนบุคคล” มีความเสี่ยงอะไรบ้าง?

Cloud
IoT
AI

Machine Learning
Cyber Attack
Big Data & Data Analytic



Identity theft

“ถูกขโมยตัวตน”

เพื่อใช้ก่ออาชญากรรม และ
โจรกรรมข้อมูลทางการเงิน



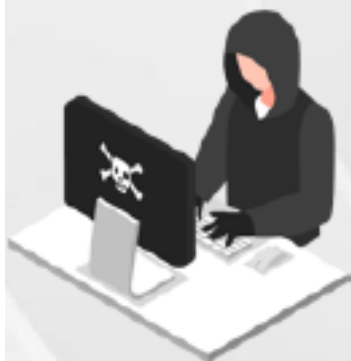
SPAM

เช่น เบอร์โทรศัพท์,
email เป็นต้น



Tracking
Stalking

“ติดตาม
สะกดรอย
สอดแนม”



Profiling

“ประมวลข้อมูล
เพื่อกำหนด Profile”

เพื่อเจาะโฆษณาหาประโยชน์
ทางการเมือง / การตลาด



Misuse

“ข้อมูลถูกขาย
ให้กับคนที่ 3”

เพื่อใช้ประโยชน์ทางการตลาด
เช่น กรณีของ Facebook
และ Cambridge Analytica

ประเภทของ Data Breach

หรือการละเมิดข้อมูลส่วนบุคคล

การละเมิด**ความพร้อมใช้**ของข้อมูล (Availability Breach)

ทำให้ หรือ ทำลายระบบ ให้ข้อมูลไม่อยู่ในสถานะที่พร้อมใช้งาน

การละเมิด**ความครบถ้วนสมบูรณ์**ของข้อมูล (Integrity Breach)

การเปลี่ยนแปลงข้อมูลส่วนบุคคล

การละเมิด**ความลับ**ของข้อมูล (Confidentiality Breach)

การเปิดเผยหรือเข้าถึงโดยไม่มีสิทธิของข้อมูลส่วนบุคคล



TOTAL NUMBER OF GDPR FINES

465

LARGEST FINE

€50,000,000

Google Inc.

SMALLEST FINE

€28

Google Ireland Ltd.

From May 2018 – January 2020

TOP 5 BIGGEST GDPR FINES



1	Google Inc.		€50 000 000
2	H&M Hennes & Mauritz		€35 200 000
3	TIM - Telecom Provider		€27 800 000
4	British Airways		€21 900 000
5	Marriott International		€20 450 000



● Countries with personal data protection law

- **Malaysia *** : Personal data protection act 2010
- **Singapore **** : Personal data protection act 2012
- **The Philippines *** : Data privacy act 2012
- **Thailand** : Personal data protection act 2019
- Indonesia : draft personal data protection act

* ongoing amendment

** amended 2020

การบังคับใช้พระราชบัญญัติฯ

พ.ร.บ. ^๒คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประกาศในราชกิจจานุ 27 พ.ค. 62

บังคับใช้ระยะที่ 1

28 พ.ค. 62 (หมวด 1 คณะกรรมการฯ และ หมวด 4 สำนักงานฯ) และบทเฉพาะกาลที่เกี่ยวข้อง

บังคับใช้ระยะที่ 2

27 พ.ค. 63 บังคับใช้ครบทุกหมวด ได้แก่

▶ หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล

▶ หมวด 5 การร้องเรียน

▶ หมวด 7 บทกำหนดโทษ (โทษอาญา-ปกครอง)

▶ หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล

▶ หมวด 6 ความรับผิดชอบทางแพ่ง

พ.ร.ฎ. กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคล
ไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.
2562 พ.ศ. 2563 ใช้บังคับตั้งแต่ 27 พ.ค. 63 ถึง 31 พ.ค. 64

บทเฉพาะกาล มาตรา 96

การออกระเบียบและประกาศตาม พ.ร.บ. นี้

ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปี
นับแต่วันที่ พ.ร.บ. นี้ใช้บังคับ (27 พ.ค. 64)

เพื่อให้การคุ้มครองข้อมูล
ส่วนบุคคลมีประสิทธิภาพ
โดยกำหนดหน้าที่และ
ความรับผิดชอบที่เหมาะสม



เพื่อให้มีมาตรการเยียวยา
จากการถูกละเมิดสิทธิ
ในข้อมูลส่วนบุคคลที่มี
ประสิทธิภาพ



หลักการคุ้มครอง
ข้อมูลส่วนบุคคล

เพื่อส่งเสริมการใช้ข้อมูล
ในการพัฒนานวัตกรรม
อย่างมั่นคงปลอดภัย



เพื่อสร้างความโปร่งใส
และเป็นธรรม ในการใช้
ข้อมูลส่วนบุคคล



PDPA มาเสริมหลักเกณฑ์ Data Protection ใน กฎหมายอื่น ที่มีอยู่เดิม

PAYMENT

พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต

ปกป้องข้อมูลเครดิตที่ครอบคลุม
ข้อมูลส่วนบุคคล
(เป็นข้อมูลเว้นของ PDPA)

ประกาศ สปท. เรื่อง หลักเกณฑ์ทั่วไป
ในการกำกับดูแลการประกอบธุรกิจ
ระบบการชำระเงินภายใต้การกำกับ
กำหนดมาตรการดูแลการเก็บข้อมูลส่วนบุคคล

TELECOM

พ.ร.บ. กสทช.

กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล
ของผู้ใช้บริการโทรคมนาคม

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการ
โทรคมนาคม เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว
และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล สิทธิเจ้าของข้อมูล
และหน้าที่ผู้ให้บริการ

INSURANCE

ประกาศ คปท. เรื่อง หลักเกณฑ์ วิธีการ
ออก และการเสนอขายกรมธรรม์
กำหนดมาตรการดูแลข้อมูลส่วนบุคคล

รัฐธรรมนูญ 2560

สิทธิในความเป็นส่วนตัว
และข้อมูลส่วนบุคคล

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

GOVERNMENT

พ.ร.บ. ข้อมูลข่าวสารราชการ

กำหนดมาตรการดูแลข้อมูลส่วนบุคคลที่รัฐดูแล

พ.ร.บ. การบริหารงานและ การให้บริการภาครัฐผ่านระบบดิจิทัล

กำหนดธรรมาภิบาลข้อมูลภาครัฐ
ที่ครอบคลุมการดูแลข้อมูลส่วนบุคคล

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

ดูแลธุรกรรมออนไลน์ภาครัฐ เน้นสร้างความปลอดภัย
ลดความเสี่ยงต่อข้อมูลส่วนบุคคล & ระบบ

ประกาศ ครอ. เรื่อง แนวนโยบายและ แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ของหน่วยงานรัฐ

แนวปฏิบัติดูแลข้อมูลส่วนบุคคลในการทำ
ธุรกรรมออนไลน์ภาครัฐ

HEALTHCARE

พ.ร.บ. สุขภาพแห่งชาติ

ปกป้องข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครอง และจัดการข้อมูลด้านสุขภาพของบุคคล

กำหนดเงื่อนไขการเปิดเผยข้อมูลสุขภาพ
พร้อมมาตรการดูแล

2 ข้อมูลส่วนบุคคล คืออะไร ?

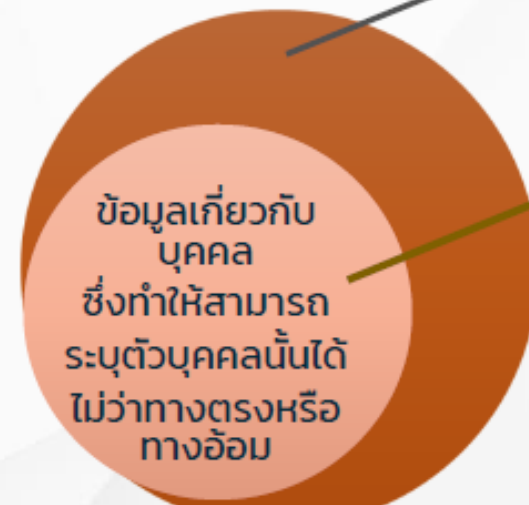
ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ
ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม
แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลที่จะต้องดูแล เป็นพิเศษ ตามมาตรา 26 (Sensitive Data)

ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความ
คิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือ
ปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม
ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน
ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ฯลฯ

ความสัมพันธ์ ระหว่าง

ความเป็นส่วนตัว
และ ข้อมูลส่วนบุคคล



ความเป็นส่วนตัว

เช่น สิทธิที่จะอยู่โดยลำพัง
(The right to be let alone)

ข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

มาตรา 6

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
เช่น สำนักงานปลัดกระทรวงฯ สพธอ. ธนาคารกรุงเทพ
บริษัท เซ็นทรัล เจริญ คอมเมอร์เชียล จำกัด ฮาชั้นอาหารทะเลตากแห้ง

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

มาตรา 6

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนาม
ของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
(และไม่ใช้เจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล)
เช่น บริษัท รปภ. จำกัด (รับดูแลระบบการรักษาความปลอดภัยของหน่วยงาน)
บริษัท ไอบีเอ็ม จำกัด (รับดูแลระบบไอทีของหน่วยงาน)

การคุ้มครอง ข้อมูลส่วนบุคคล ภายใต้ PDPA



ใคร

ที่มีสิทธิ
& หน้าที่
ทำอะไร
เก็บรวบรวม,
ใช้, เปิดเผย

เจ้าของ ข้อมูลส่วนบุคคล (Data Subject)

- ให้ความยินยอม
เท่าที่เหมาะสม
- รับทราบและใช้สิทธิที่มี

ผู้ควบคุม ข้อมูลส่วนบุคคล (Controller)

- มีมาตรการดูแล Security
ที่เหมาะสม และทบทวนสม่ำเสมอ
- ลบ ทำลายข้อมูล เมื่อ
พ้นระยะเวลาเก็บรักษา
- แจ้งเหตุละเมิด ภายใน 72 ชั่วโมง
นับแต่ทราบเหตุ
- ถ้าเป็น บจก. ตปท.
ต้องแต่งตั้งตัวแทน และตั้ง DPO
- จัดทำ + เก็บรักษาบันทึกการงาน

ผู้ประมวลผล ข้อมูลส่วนบุคคล (Processor)

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

คณะกรรมการ ที่ดูแล Law Compliance ตาม PDPA

คณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล

- จัดทำแผนแม่บท และแผนระดับชาติ
- กำหนดมาตรการและแนวทาง
การดำเนินงานเกี่ยวกับ DP
- ออกประกาศหลักเกณฑ์/มาตรการ
- วินิจฉัยชี้ขาด
- ส่งเสริมและสนับสนุนด้าน DP

คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียน
- ตรวจสอบการดำเนินการของ
ผู้ที่เกี่ยวข้อง
- โกล่เกลี่ยข้อพิพาท



Law Compliance ตามกฎหมายอื่น

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

เก็บเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และ **จะต้องแจ้งวัตถุประสงค์** ให้เจ้าของข้อมูลส่วนบุคคลทราบ

- 1 ได้รับคามยินยอมจากเจ้าของข้อมูล (Consent)
- 2 เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
- 3 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)
- 4 มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
- 5 มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล หรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public Task)
- 6 มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
- 7 เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด **โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล**

เว้นแต่

- 1 ป้องกันหรือระงับอันตรายต่อชีวิต
- 2 ชอบด้วยกฎหมายของมูลนิธิ สมาคม องค์กร
- 3 เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
- 4 การก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- 5 จำเป็นในการปฏิบัติตามกฎหมาย

ก) เวชศาสตร์ป้องกัน การวินิจฉัยโรคและการรักษาทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคมหรือด้านสังคมสงเคราะห์

ข) ประโยชน์สาธารณะด้านการสาธารณสุข

ค) คัมครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ

ง) วิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

จ) ประโยชน์สาธารณะที่สำคัญ โดยมีมาตรการเพื่อคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคล
จากแหล่งอื่นที่ไม่ใช่จากเจ้าของ
ข้อมูลส่วนบุคคลโดยตรง

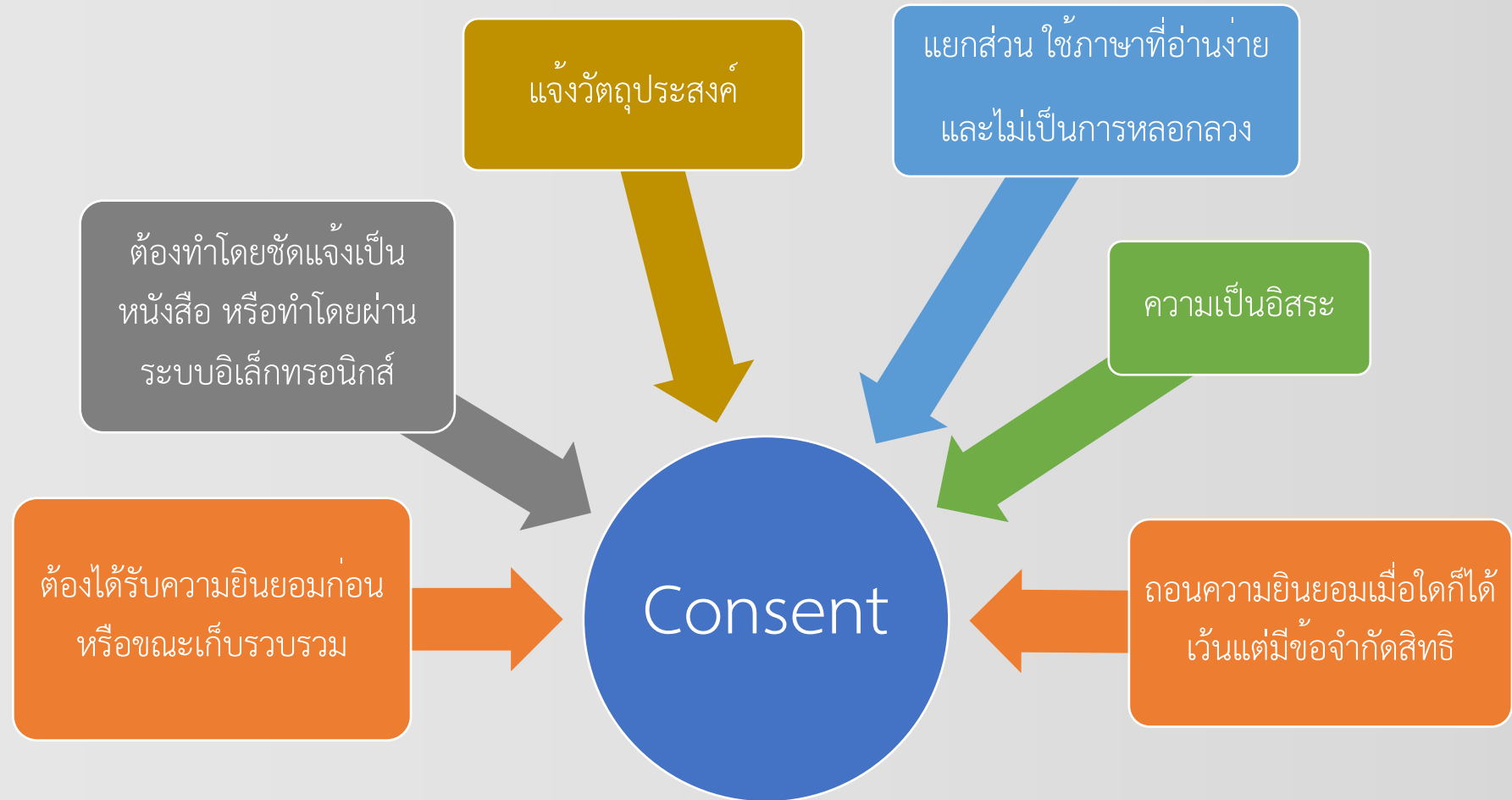
ข้อยกเว้น

- (1) แจ้งเจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า
แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม
และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคล
ที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล สำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศที่รับข้อมูลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

เว้นแต่

- 1 การปฏิบัติตามกฎหมาย
- 2 ได้รับความยินยอมจากเจ้าของข้อมูล
- 3 การปฏิบัติตามสัญญา
- 4 การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น
- 5 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
- 6 เพื่อประโยชน์สาธารณะที่สำคัญ



สิทธิของเจ้าของข้อมูลส่วนบุคคล



สิทธิได้รับการแจ้งให้ทราบ
(Right to be informed)



สิทธิขอเข้าถึงข้อมูลส่วนบุคคล
(Right of access)



สิทธิในการขอให้โอนข้อมูลส่วนบุคคล
(Right to data portability)



สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
(Right to object)



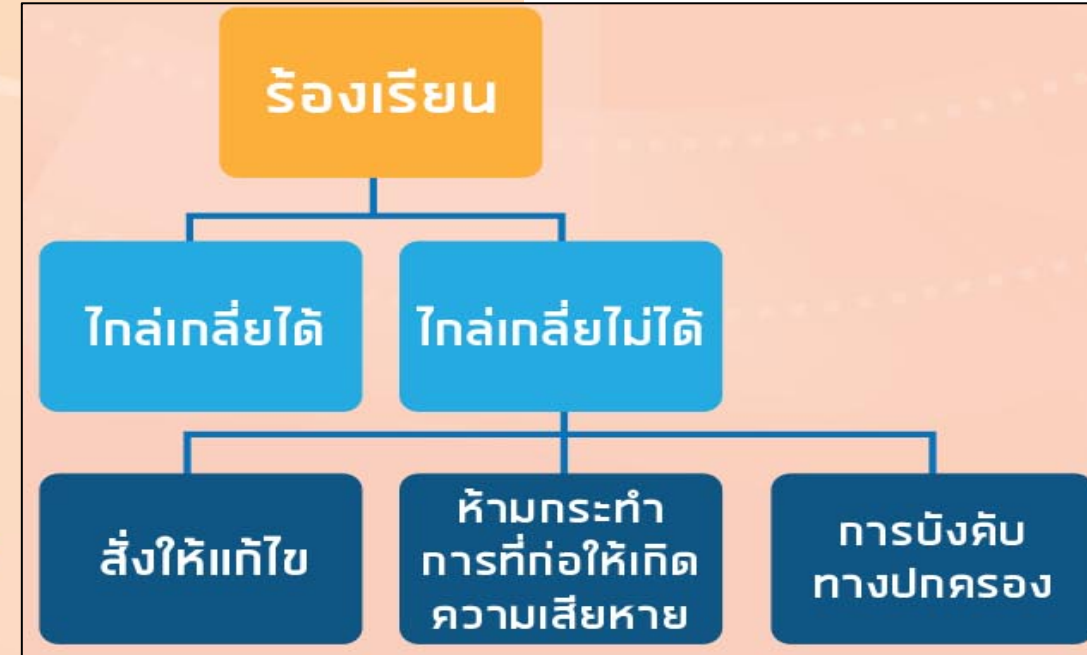
สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
(Right to erasure (also known as right to be forgotten))



สิทธิขอให้ระงับการใช้ข้อมูล
(Right to restrict processing)



สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล
(Right of rectification)



ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี DPO

มาตรา 41

- 1 หน่วยงานของรัฐ ตามที่ประกาศกำหนด
- 2 การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด
- 3 กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผย Sensitive Personal Data



หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

มาตรา 42

- 1 ให้คำแนะนำ
- 2 ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
- 3 ประสานงานและให้ความร่วมมือกับสำนักงานฯ
- 4 รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

- 1 ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม
ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูล
- 2 ส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถ
แจ้งยกเลิกความยินยอมได้โดยง่าย
- 3 การเปิดเผยและการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตาม
พระราชบัญญัตินี้



พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ใช้บังคับตั้งแต่ 27 พฤษภาคม 2563 ถึง 31 พฤษภาคม 2564 ยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคล 22 หน่วยงานหรือกิจการ ยังไม่ต้องปฏิบัติตามบางหมวดในกฎหมาย
ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล การร้องเรียน ความรับผิดชอบทางแพ่ง และบทกำหนดโทษ

- | | |
|--|--|
| 1 หน่วยงานของรัฐ | 12 กิจการด้านการท่องเที่ยว |
| 2 หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ | 13 กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล |
| 3 มูลนิธิ สมาคม องค์การศาสนา และองค์กรไม่แสวงหาผลกำไร | 14 กิจการด้านการเงิน การธนาคาร และการประกันภัย |
| 4 กิจการด้านเกษตรกรรม | 15 กิจการด้านอสังหาริมทรัพย์ |
| 5 กิจการด้านอุตสาหกรรม | 16 กิจการด้านการประกอบวิชาชีพ |
| 6 กิจการด้านพาณิชยกรรม | 17 กิจการด้านการบริหารและบริการสนับสนุน |
| 7 กิจการด้านการแพทย์และสาธารณสุข | 18 กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ |
| 8 กิจการด้านพลังงาน ใต้น้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง | 19 กิจการด้านการศึกษา |
| 9 กิจการด้านการก่อสร้าง | 20 กิจการด้านความบันเทิงและนันทนาการ |
| 10 กิจการด้านการซ่อมและการบำรุงรักษา | 21 กิจการด้านการรักษาความปลอดภัย |
| 11 กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า | 22 กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน |

พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตาม มาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

- ◆ ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
- ◆ แจ้างมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ เพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด
- ◆ จัดให้มีมาตรการเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วย
 - ① การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผล
 - ② การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
 - ③ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
 - ④ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
 - ⑤ การจัดให้มีวิธีการตรวจสอบย้อนหลังการเข้าถึงข้อมูลส่วนบุคคลได้
- ◆ สามารถใช้มาตรฐานความมั่นคงปลอดภัยที่สูงกว่าประกาศฉบับนี้ได้
- ◆ ใช้บังคับจนถึง 31 พฤษภาคม 2564



จัดทำ DP policy กำหนดเป้าหมาย การเก็บรวบรวม การใช้ การเปิดเผย สร้างความโปร่งใส

เมื่อ :

- Controller, Processor เป็นหน่วยงานของรัฐ
- มีการเก็บ ใช้เปิดเผยข้อมูลจำนวนมาก
- มีกิจกรรมหลักเป็นการเก็บ ใช้เปิดเผย Sensitive Data

DPO มีหน้าที่

- ให้คำแนะนำ
- ตรวจสอบการดำเนินการที่เกี่ยวข้องกับการเก็บ ใช้เปิดเผย
- ประสานงานกับ สบง.เมื่อมีปัญหา
- รักษาความลับ

ขอความยินยอมที่ชัดเจน เข้าใจง่าย มีหลักฐานเป็น doc หรือ e-document

แจ้งวัตถุประสงค์ เช่น

- การใช้
- การเปิดเผย
- ระยะเวลาการเก็บ
- แจ้งสิทธิต่าง ๆ แก่เจ้าของข้อมูล

การเก็บรวบรวมต้องทำเท่าที่จำเป็นเหมาะสม

ใช้เปิดเผยตามวัตถุประสงค์

ทำสัญญากับ Third Party กำหนดหน้าที่ดูแล หากมีการประมวลผลข้อมูล

โอนข้อมูลไปต่างประเทศได้ เมื่อหน่วยงาน / องค์กร มาตรฐานที่เพียงพอ

โอนข้อมูลไปต่างประเทศ ในเครือเดียวกันได้ หาก DP Policy ได้รับการรับรองจาก สบง..

ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน

ต้องปฏิบัติตามคำขอเจ้าของข้อมูล

ปฏิเสธคำขอได้ ถ้ามีกฎหมาย คำสั่งศาล กำหนดไว้ หรือกระทบต่อสิทธิ เสรีภาพ ของผู้อื่น และต้องบันทึกเหตุผลด้วย

ลบ ทำลายข้อมูลเมื่อพ้นระยะเวลาเก็บ

หากได้รับคำขอให้ลบ ทำลาย หรือ Anonymous ต้องรับผิดชอบทั้งทางเทคโนโลยีและค่าใช้จ่ายตามคำขอนี้

กรณีให้ข้อมูลแก่คนอื่น ต้องป้องกันไม่ให้ผู้อื่นใช้ /เปิดเผย ข้อมูลโดยไม่ชอบ

จัดทำบันทึกเกี่ยวกับข้อมูล เพื่อให้ตรวจสอบได้.

จัดให้มีมาตรการ Incident response

แจ้งเหตุแก่ สบง. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

แจ้งเหตุแก่เจ้าของข้อมูล + แนวทางเยียวยาโดยไม่ชักช้า

จัดทำช่องทางการถอนที่ง่ายเหมือนตอนขอความยินยอม

แจ้งผลกระทบจากการขอยกเลิก

จัดให้มีมาตรการ Security

ทบทวนมาตรการ Security เมื่อจำเป็นหรือเทคโนโลยีเปลี่ยนแปลงไป

- Data Controller
- Data Processor

สำรวจตนเอง

แต่งตั้ง DPO

การเก็บรวบรวม

การใช้ การเปิดเผยข้อมูล

สิทธิและหน้าที่

Data Breach

ถอนความยินยอม

Security

ศึกษาข้อมูล DP policy ให้มั่นใจในกระบวนการคุ้มครองข้อมูลส่วนบุคคล

มี Contract point ที่เป็น DPO กรณีมีปัญหาเกิดขึ้น

รู้วัตถุประสงค์ ข้อมูลส่วนบุคคลที่จัดเก็บ และสิทธิของตนเอง

ให้ความยินยอมตามความจำเป็นเหมาะสม

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.ผู้พิทักษ์ฯ หากผู้ควบคุมไม่ดำเนินการตามที่ร้อง

ได้รู้ถึงสาเหตุ + แนวทางการเยียวยา

รับทราบผลกระทบของการยกเลิก

มั่นใจในความมั่นคงปลอดภัย



Data subject

การเตรียมความพร้อมระดับองค์กร

1. การตั้งคณะทำงาน (Working Group) ภายในองค์กร

การตั้งคณะทำงานภายในองค์กรควรประกอบไปด้วยกลุ่มคนต่อไปนี้

ฝ่ายกำหนดนโยบายและยุทธศาสตร์ขององค์กร

ฝ่ายกฎหมาย

ฝ่ายเทคโนโลยีสารสนเทศ

ฝ่ายบุคคล หรือฝ่ายที่เกี่ยวข้องกับขบวนการทางธุรกิจขององค์กร



เพื่อศึกษาและทำความเข้าใจบริบทของกฎหมาย และเตรียมความพร้อมในการตรวจสอบ และปรับปรุง การดำเนินขององค์กรให้สอดคล้องตามข้อกำหนดของกฎหมาย



2. การสำรวจข้อมูล (Data Inventory)

รวบรวมกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลทุกประเภทขององค์กร

- สำรวจข้อมูลที่มีอยู่ในองค์กรตามกระบวนการไหลของข้อมูล (Data flows)
- จำแนกข้อมูลให้เป็นหมวดหมู่ ข้อมูลธุรกิจ ข้อมูลความลับ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลอ่อนไหว

จัดทำรายการข้อมูลส่วนบุคคลที่มีใช้ในปัจจุบัน โดยระบุแหล่งที่มา การจัดเก็บ และการใช้งานข้อมูล

- ระบุแหล่งที่มาของข้อมูลส่วนบุคคล วิธีการจัดเก็บ จัดเก็บไว้ด้วยเหตุผลใด และใครมีสิทธิเข้าถึงข้อมูลเหล่านั้นบ้าง
- พิจารณาฐานการประมวลผลที่ชอบด้วยกฎหมาย (Lawfulness of processing) ทั้งในส่วน of ข้อมูลส่วนบุคคลแบบทั่วไป (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 24 และมาตรา 26 โดยลำดับ

3. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

- อธิบายขอบเขตและวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล (จัดเก็บ ใช้ เปิดเผย)
- ประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล
- จัดระดับความเสี่ยงที่จะมีผลกระทบต่อเสรีภาพของบุคคล การดำเนินธุรกิจ ชื่อเสียงและความเสียหายด้านการเงิน
- กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้เหมาะสมกับความเสี่ยงและผลกระทบที่จะเกิดขึ้น



4. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ



หน่วยงานต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ถูกจัดเก็บ ใช้ และเปิดเผย โดยต้องกำหนดให้มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่สอดคล้องกับมาตรฐานสากล เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย

5. จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน

หน่วยงานควรพิจารณาจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่มีเนื้อหาครอบคลุมอย่างน้อย ดังนี้

- 1 หลักการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น (Collection, Use, Disclose Limitation)
- 2 หลักการขอความยินยอม การแจ้งวัตถุประสงค์ที่ชัดเจน (Purpose Specification)
- 3 หลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามฐานการประมวลผล (Lawful Basis)
- 4 หลักการควบคุมคุณภาพของข้อมูลส่วนบุคคล (Integrity)
- 5 หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguard)
- 6 หลักการใช้สิทธิของเจ้าของข้อมูล (Data Subject Rights)
- 7 หลักการแสดงนโยบายคุ้มครองข้อมูลส่วนบุคคลอย่างโปร่งใส (Transparency)
- 8 หลักการรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคล (Accountability)

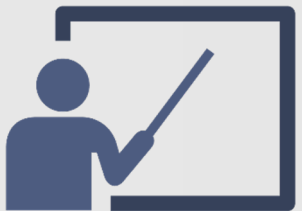


6. จัดทำบันทึกการกิจกรรมที่เกี่ยวข้อง (Record of Processing)

ตามมาตรา 39 และ 40 หน่วยงานต้องจัดทำบันทึกการกิจกรรม เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานตรวจสอบได้ ซึ่งประกอบด้วย

- 1) ข้อมูลที่มีการจัดเก็บ
- 2) วัตถุประสงค์ของการจัดเก็บ
- 3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- 4) ระยะเวลาการเก็บ
- 5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล
- 6) การใช้หรือเปิดเผยข้อมูลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม
- 7) เหตุผลในการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- 8) คำอธิบายเกี่ยวกับมาตรการการรักษาความมั่นคงปลอดภัย

7. สร้างความตระหนักรู้ และฝึกอบรม



หน่วยงานต้องสร้างความตระหนักรู้ สำคัญรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล และหน้าที่ความรับผิดชอบของหน่วยงาน รวมถึงการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และผลกระทบที่เกิดขึ้นจากการละเมิดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ให้แก่บุคลากรของหน่วยงาน โดยการเผยแพร่ข้อมูลข่าวสาร และการฝึกอบรมให้ความรู้ที่เกี่ยวข้องเป็นประจำสม่ำเสมอ

8. กำกับดูแลและตรวจสอบอย่างสม่ำเสมอ



หน่วยงานจะต้องมีการกำกับดูแล และตรวจสอบการดำเนินงานบุคคลากร และผู้เกี่ยวข้องเพื่อให้เกิดการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่หน่วยงานทำการรวบรวม จัดเก็บ และเผยแพร่ถูกควบคุมภายใต้มาตรการที่กำหนดไว้

9. ทบทวนหรือปรับปรุงกระบวนการงานและมาตรการที่เกี่ยวข้อง

หน่วยงานต้องทบทวนหรือปรับปรุงกระบวนการงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เมื่อพบว่ามีความเสี่ยง หรือพบว่ามีการดำเนินงานที่ไม่สอดคล้องกับข้อกำหนดของกฎหมาย โดยทบทวนตามวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้ เผยแพร่ ลบหรือทำลายข้อมูล





Thank you