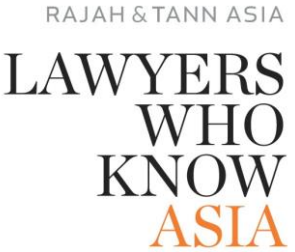
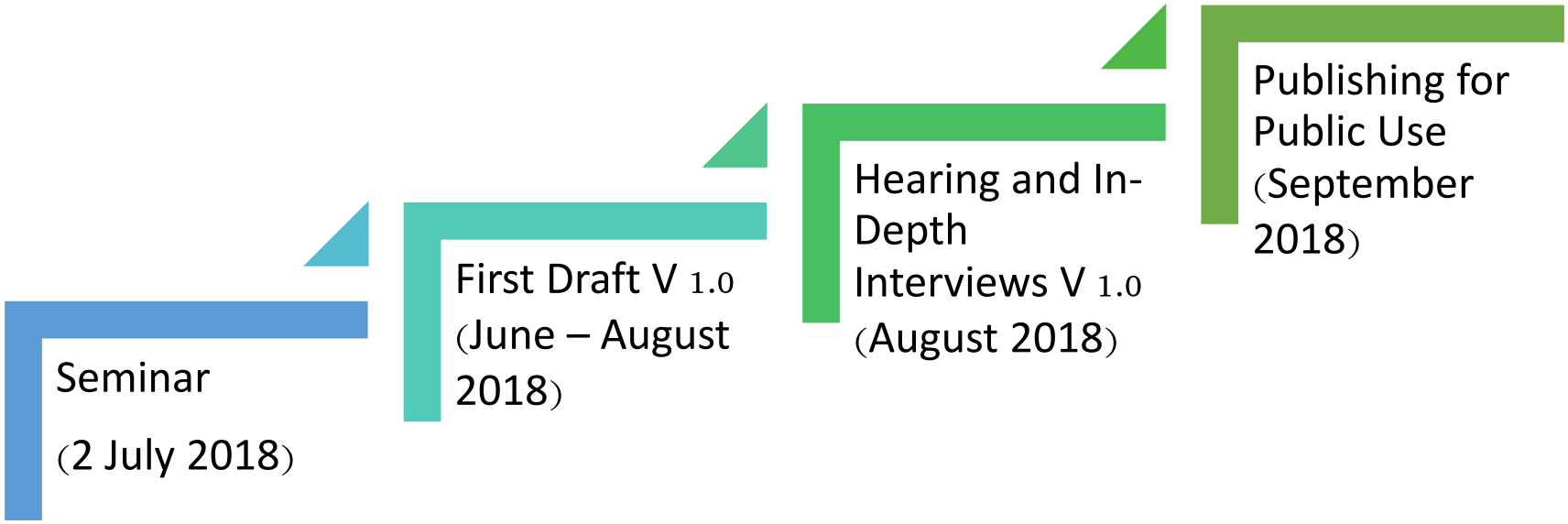
Thailand Data Protection Guideline 1.0



Steps to Thailand Data Protection Guideline V 1.0



Thailand Data Protection Guideline V 1.0

Data Classification

- Scope
- Data and Risk Assessment

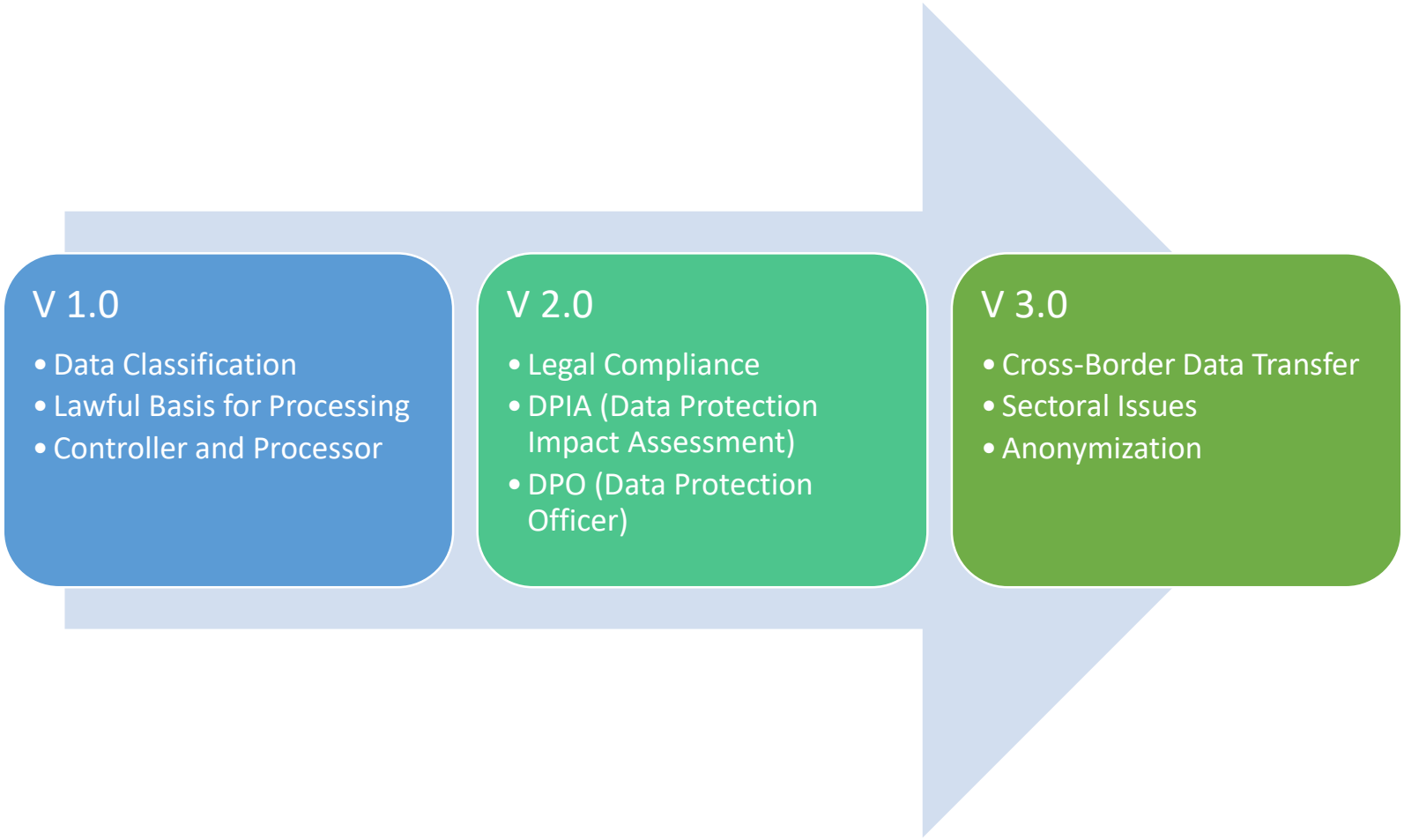
Lawful Basis for Processing

- Contract
- Consent

Controller and Processor

- Duties and Responsibilities
- Agreement between Controller and Processor
- Data Subject Requests
- Government Requests

Future Plan


V 1.0
• Data Classification
• Lawful Basis for Processing
• Controller and Processor
V 2.0
• Legal Compliance
• DPIA (Data Protection Impact Assessment)
• DPO (Data Protection Officer)
V 3.0
• Cross-Border Data Transfer
• Sectoral Issues
• Anonymization

Team

- รศ.ธิติพันธุ์ เชื้อบุญชัย (ที่ปรึกษา)
- ผศ.ดร.ปารีณา ศรีวนิชย์ (ที่ปรึกษา)
- ผศ.ดร.ปิยะบุตร บุญอร่ามเรือง
- อ.ดร.ชวิน อุ่นภัทร
- อ.ดร.ปิติ เอี่ยมจำรูญลาภ
- อ.ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล

Guideline for Personal Data Classification

Data Policy

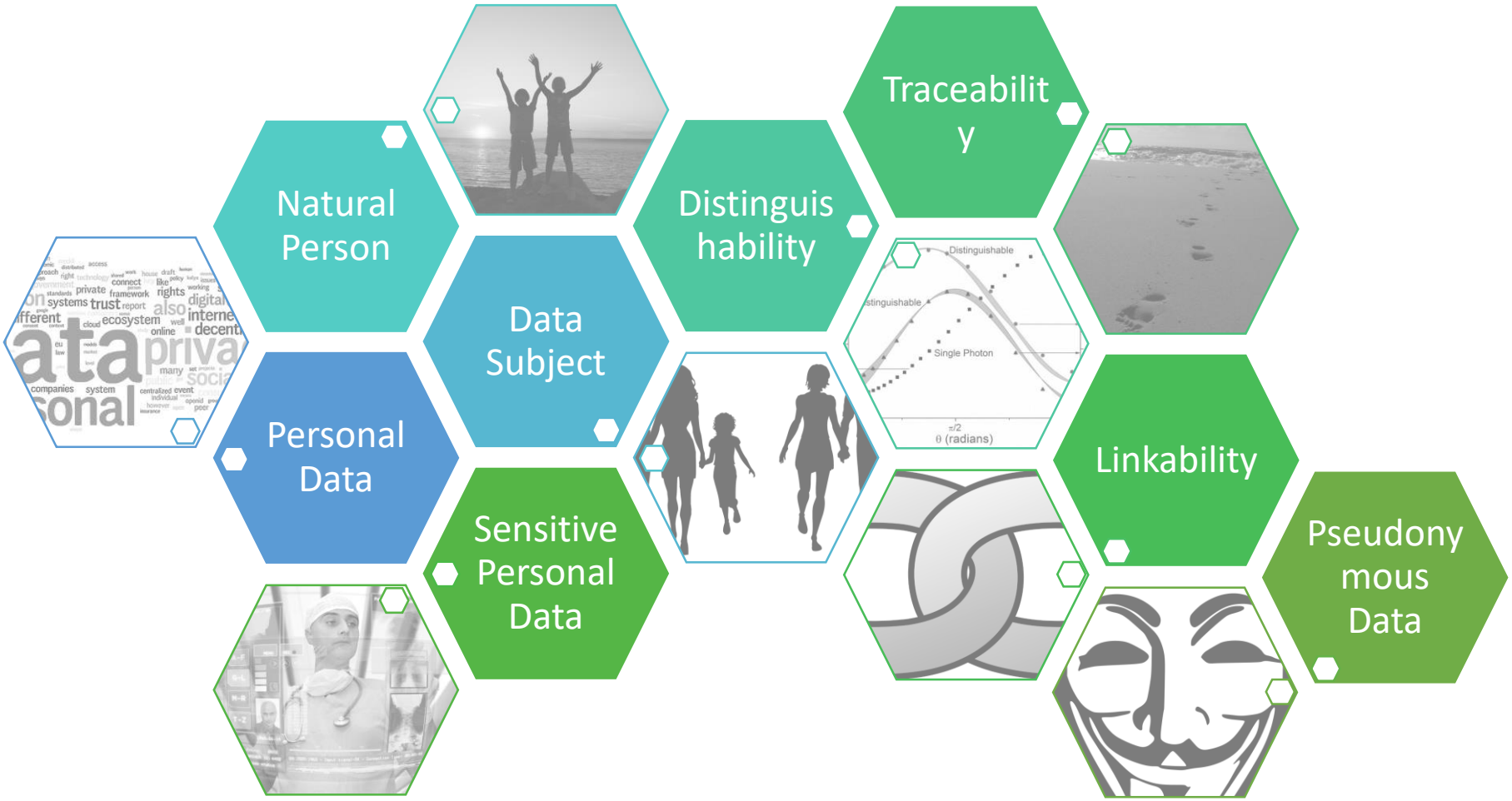
Data Discovery

Data Proliferation

Data Risk Level

Data Protection

Scope of Personal Data



Data Classification

Data Policy

Data Discovery

Data Proliferation

Data Risk Level

Data Protection

Actors, Roles and Interactions

	Data Subject	Controller	Processor	Third Parties
A.	Provider	Recipient		
B.		Provider	Recipient	
C.	Provider		Recipient	
D.	Recipient	Provider		
E.	Recipient		Provider	
F.		Recipient	Provider	
G.		Provider		Recipient
H.			Provider	Recipient

Data Risk Level

Low	• Limited adverse effect
Moderate	• Serious adverse effect
High	• Severe or catastrophic adverse effect

Data Risk Level

Identifiability

Volume

Access & Activity

Adverse Effects to Data Subjects

Adverse Effects to Organization

Legal Basis of Processing

Contract

Consent

Vital Interest

- To protect health and life of data subjects and third persons

Legal Obligations

Public Task

- Usually cases of public authorities

Legitimate Interest

- Must be *balanced* between controller's interest and data subject fundamental rights

Contract or Consent ?

Necessary for contract	Choice of data subject
Home address information for delivery of goods and email address for sending receipt	Email address for newsletter (with easy option to unsubscribe)
Credit card information for hotel reservation	Credit card information remembered on site for next reservation

Legal obligation and public task

Data controller's **legal obligation**	***(Authorities')*** **public task**
A company declares employees' salary to the revenue department	The revenue department processes employees' salary to examine the declared income of a company.
A financial institution reports suspicious transaction to the Anti Money Laundering Office (AMLO).	The Anti Money Laundering Office (AMLO) collects information about suspicious transaction.

What is *valid* consent?

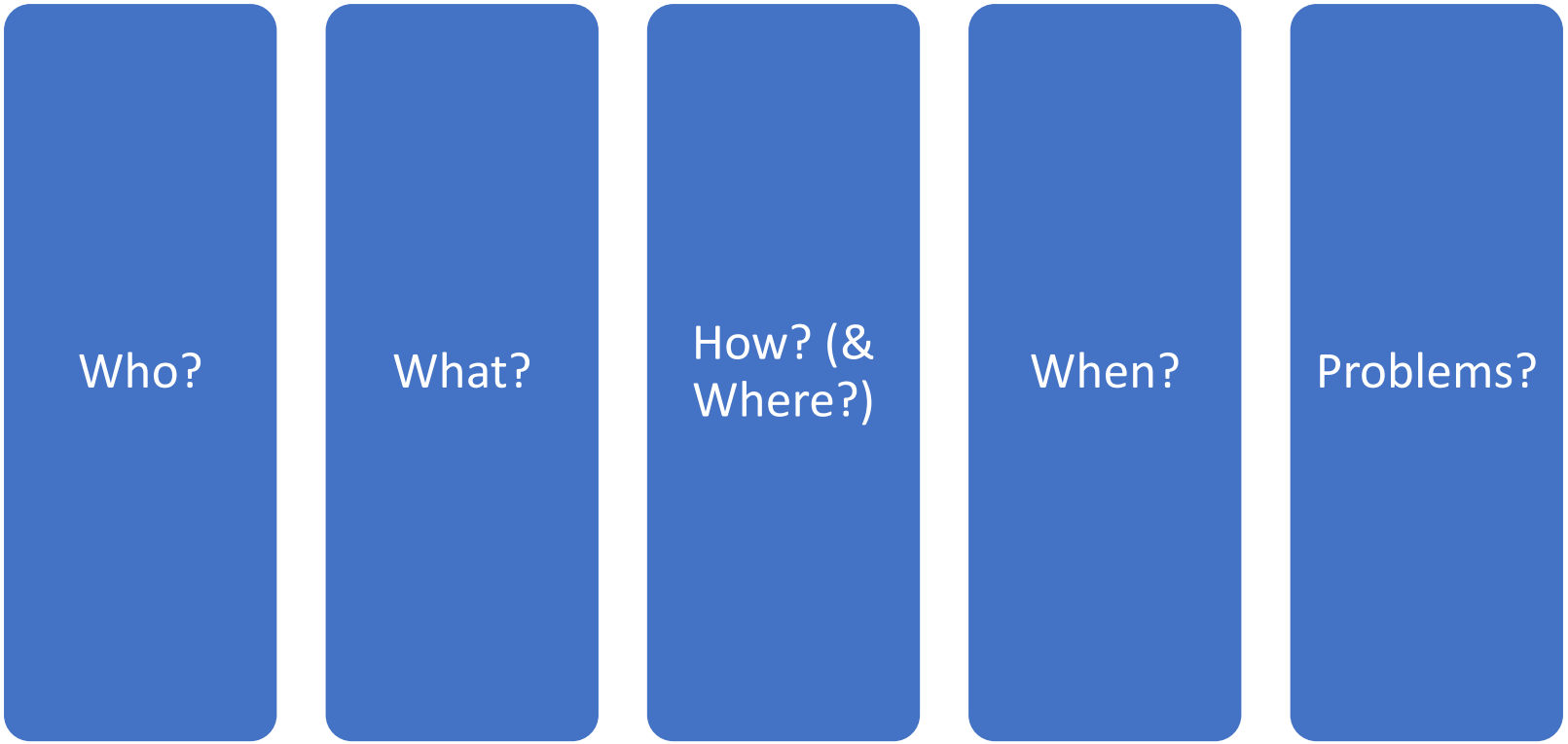
"***Freely given, specific, informed and unambiguous*** by a statement or ***by a clear affirmative action.***"

- Given before processing
- Not a condition of service
- Separate from service
- Specific purposes
- Intelligible and accessible
- Choice to refuse
- Can be withdrawn without sanction

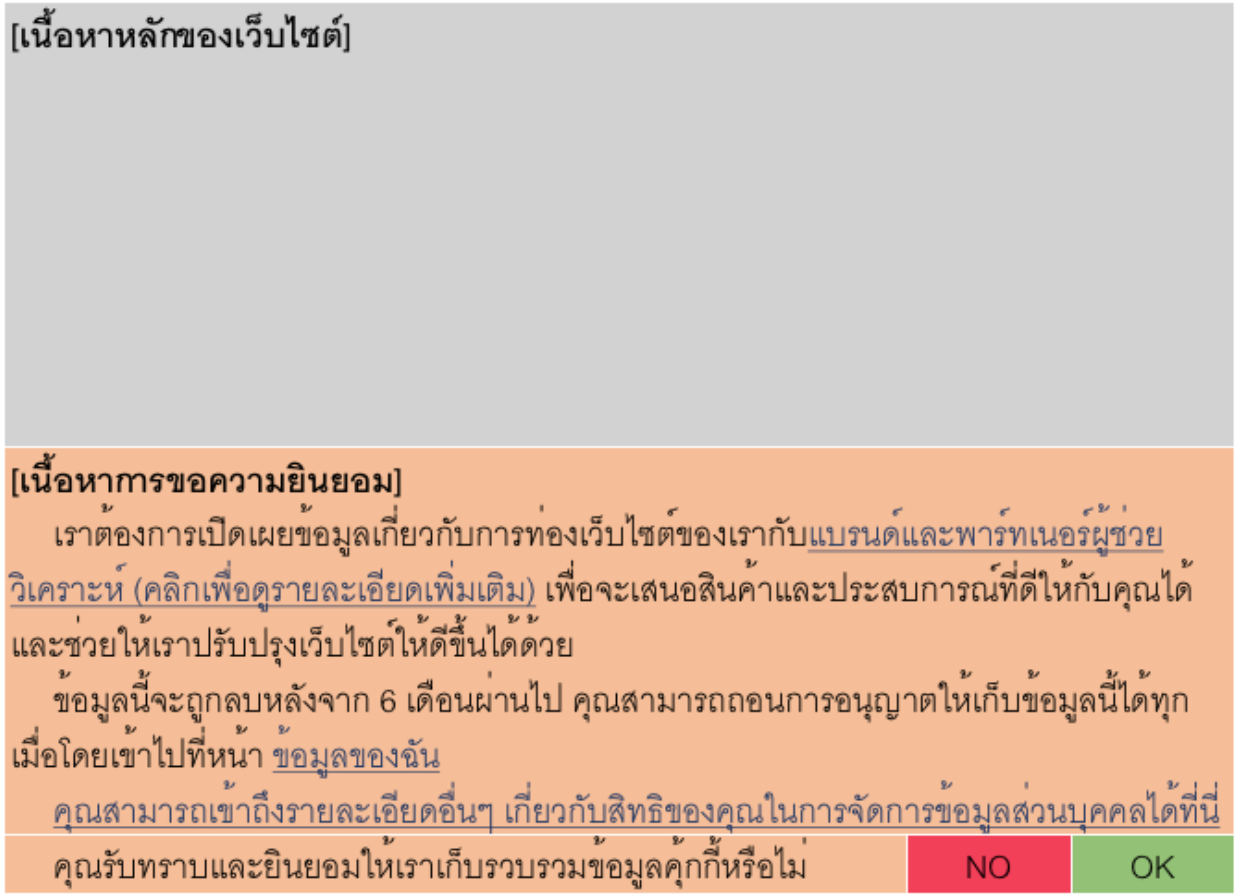
Intelligible and accessible

นโยบายความเป็นส่วนตัว	
• เราเก็บข้อมูลส่วนบุคคลอะไรของคุณบ้าง?	+
• เราใช้ข้อมูลส่วนบุคคลของคุณอย่างไร?	+
• เราเปิดเผยข้อมูลส่วนบุคคลของคุณให้กับใครบ้าง?	+
• เราเก็บข้อมูลส่วนบุคคลของคุณไว้ที่ไหน? มีความปลอดภัยหรือไม่	-
[เนื้อหารายละเอียด] เราได้ใช้มาตรการทางกายภาพและทางเทคนิคเพื่อปกป้องข้อมูลส่วนบุคคลของคุณ แต่อย่างไรก็ตาม.....	
• เราโอนข้อมูลไปต่างประเทศหรือไม่?	+

Informed consent



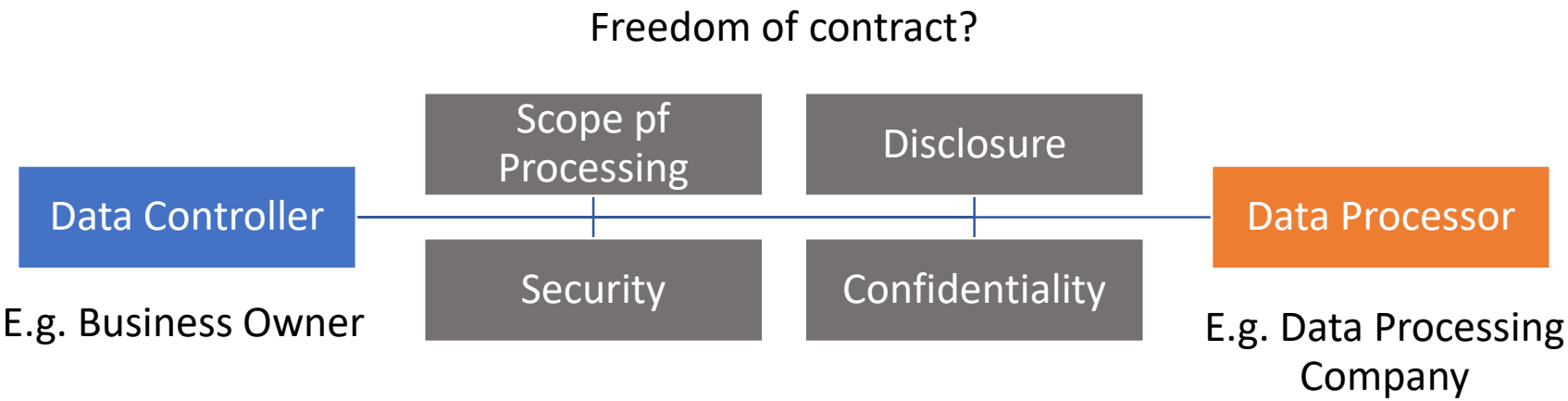
Informed consent



Cautions!!

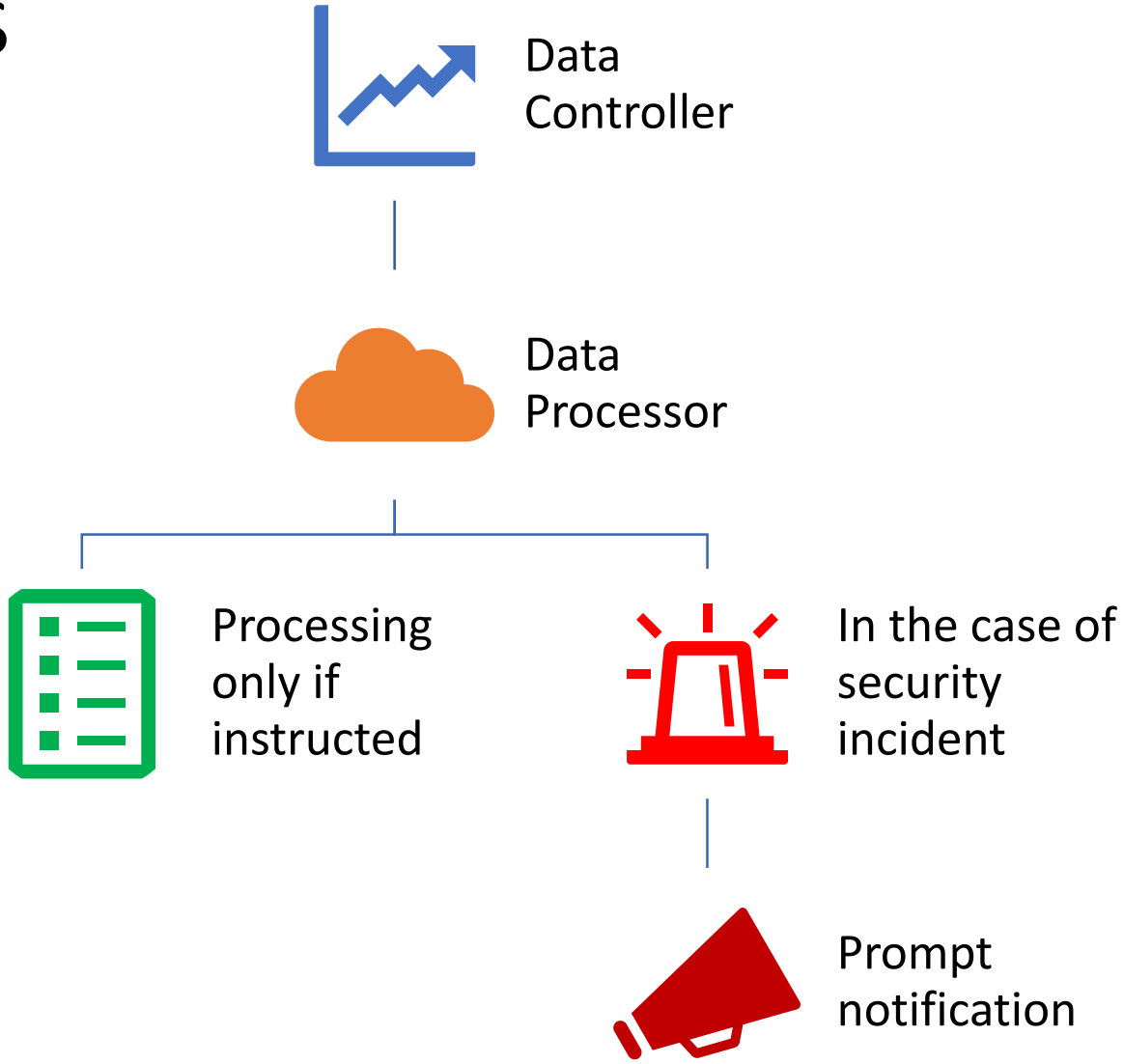
- Necessity
- Transparency
- Records of consent
- Consent management
  - categorisation
  - review
- Easy withdrawal without sanctions
- Ready to response to data subject

Data Processing Agreement: DPA

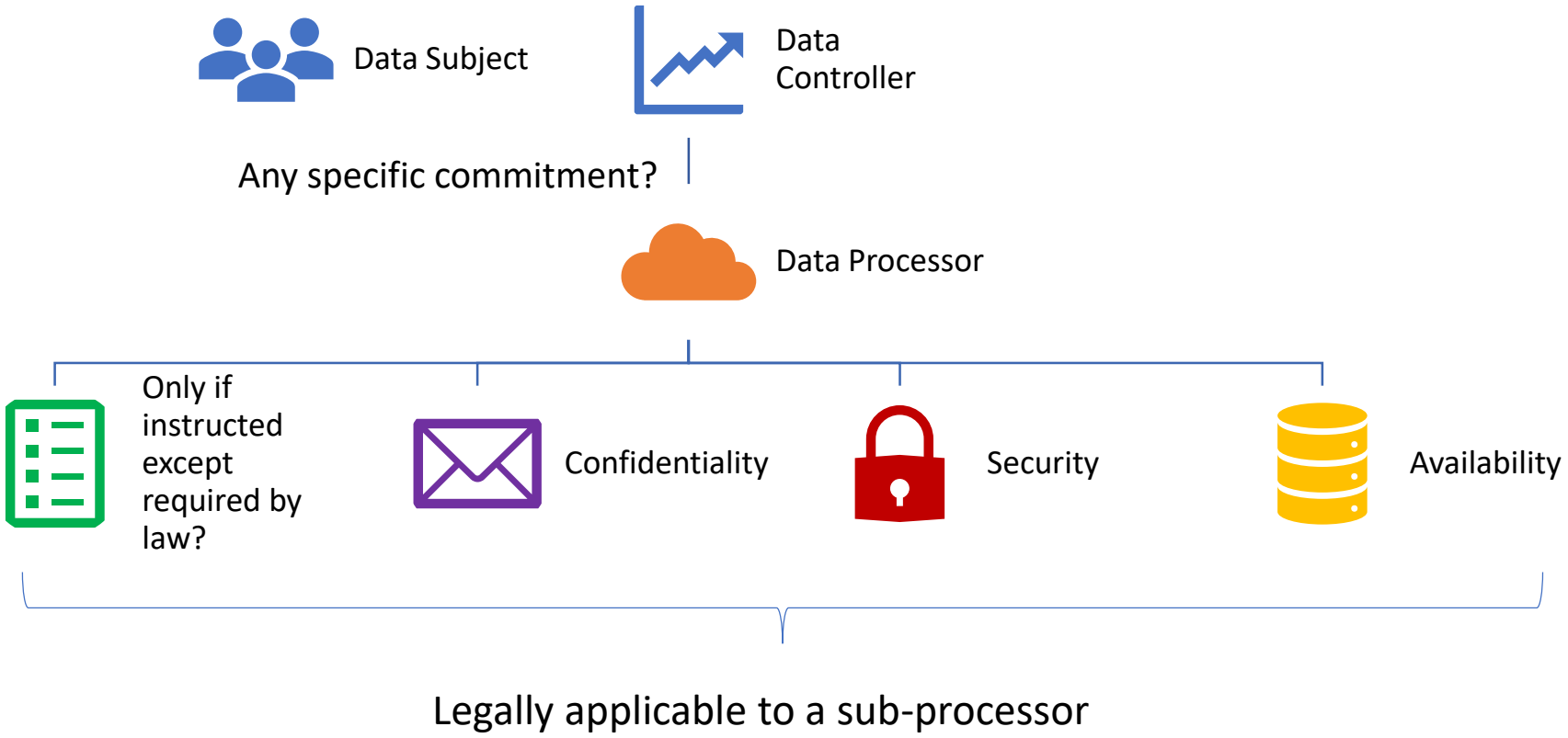


Key Clauses

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



Key Clauses


Data Subject
Data Controller
Any specific commitment?
Data Processor
Only if instructed except required by law?
Confidentiality
Security
Availability
Legally applicable to a sub-processor

Duties & Responsibility of Data Controllers and Data Processors

Data Controller

Data Processor

Duties & Responsibility of Data Controllers and Data Processors

หน้าที่โดยทั่วไป

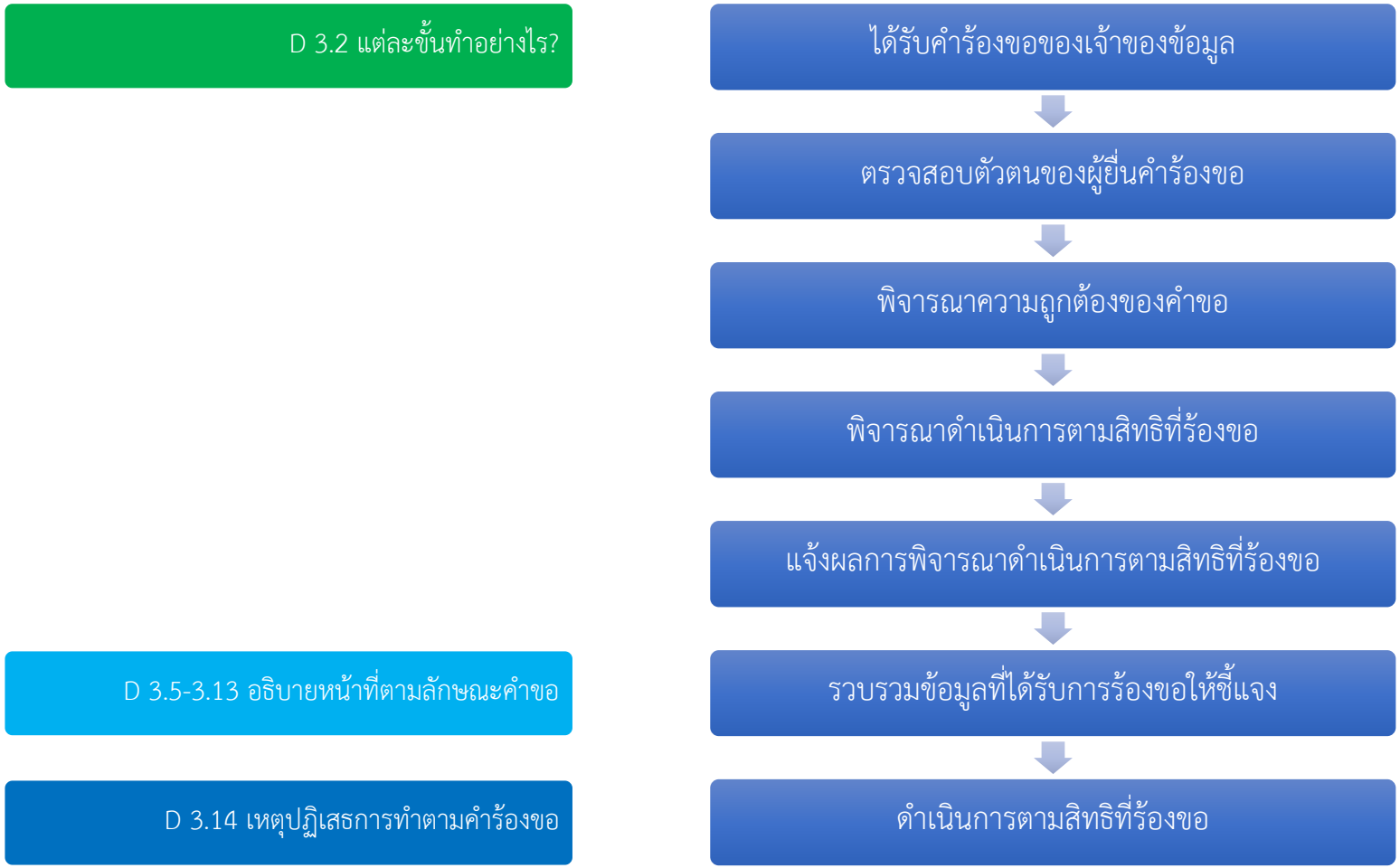
D1

หน้าที่เมื่อมีคำร้องของเจ้าของข้อมูล

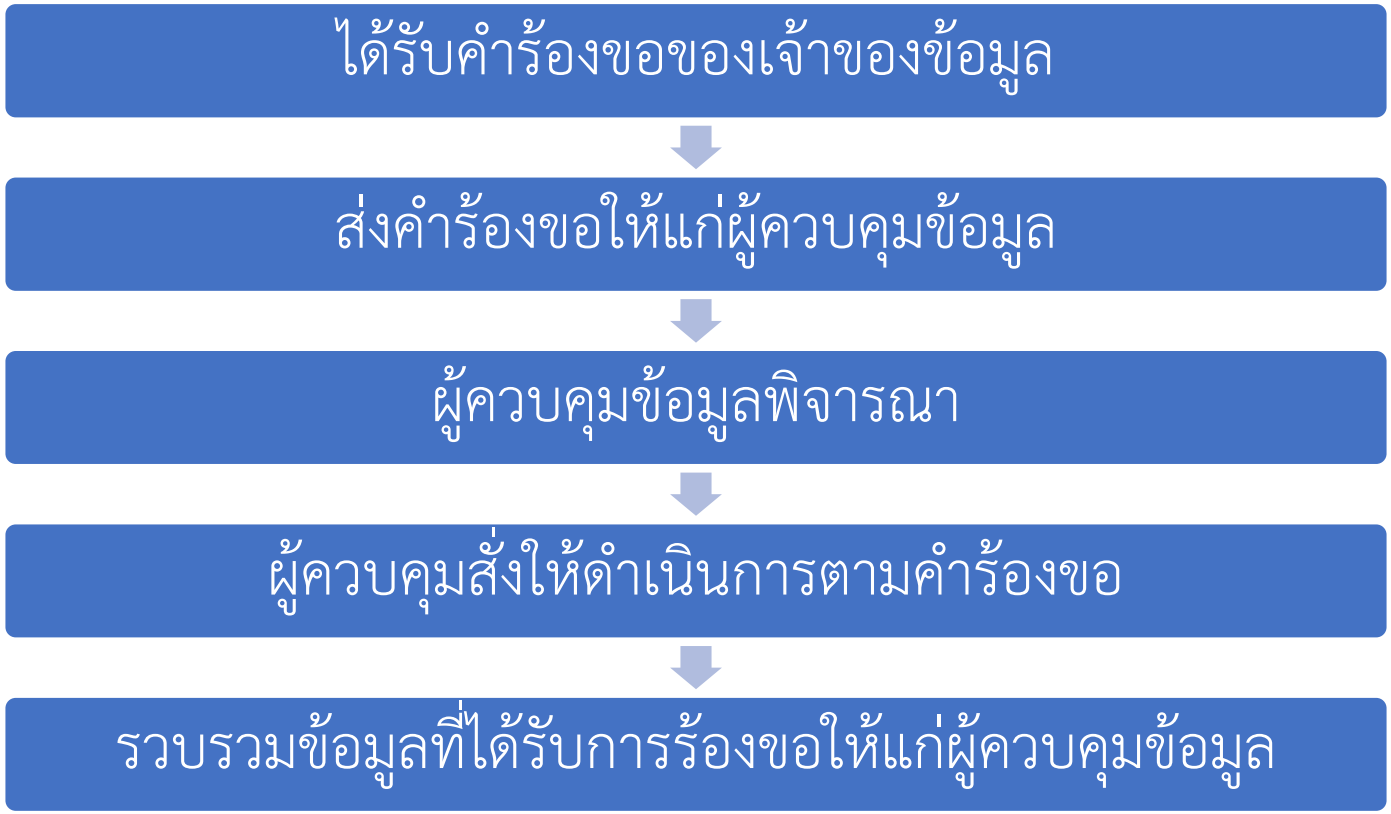
D3

ท่านเป็นผู้ควบคุมข้อมูล (Controller)	ท่านเป็นผู้ประมวลผลข้อมูล (Processor)
หน้าที่ของผู้ควบคุมข้อมูล ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย ○ แจ้งเจ้าของข้อมูล ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง ○ แจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) ○ เก็บบันทึกรายการประมวลผลข้อมูล ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ○ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ○ เลือกผู้ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย	หน้าที่ของผู้ประมวลผลข้อมูล ○ ประมวลผลข้อมูลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล ○ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง ○ แจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) ○ เก็บบันทึกรายการประมวลผลข้อมูล ○ ตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ○ แจ้งผู้ควบคุมข้อมูลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลที่มีความมั่นคงปลอดภัยสูงกว่า

หน้าที่ของผู้ควบคุมข้อมูลเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล



หน้าที่ของผู้ประมวลผลข้อมูลเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล



แนวปฏิบัติกรณีมีคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากรัฐ

ผู้ควบคุมข้อมูล	ผู้ประมวลผลข้อมูล
D4.1 ผู้ควบคุมข้อมูลมีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย	D4.2 ผู้ประมวลผลข้อมูลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมายและความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลหากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย

ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

❑พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ

- ❑ เจ้าหน้าที่และต้นสังกัด
- ❑ วันที่ได้รับคำร้องขอ
- ❑ ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย

❑ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร

- ❑ เจ้าหน้าที่ไม่มีเอกสารมาแสดง
- ❑ เจ้าหน้าที่มีเอกสารมาแสดง
  - ❑ หมายศาล/คำสั่งศาล
  - ❑ อื่นๆ .....

❑พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)

- ❑ กรณีหมายศาล/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ
- ❑ กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไป (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจราจรคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่ามีหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอ
- ❑ กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร ให้ไม่ดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

❑ดำเนินการ ❒ ไม่ดำเนินการตามคำร้องขอ

❑เก็บบันทึกเกี่ยวกับการร้องขอและกระบวนการดำเนินการ/ไม่ดำเนินการตามคำร้องขอทั้งหมด

Key Data Protection Frameworks

GDPR (EU General Data Protection Regulation)

APEC Privacy Framework and CBPR (Cross-Border Privacy Rules System)

Data Protection Certification is Coming!

Guidelines 1/2018 on certification, adopted on 25 May 2018

- uniform and verifiable,
- auditable;
- relevant with respect to the targeted audience
- take into account and inter-operable with other standards
- flexible and scalable for application to different types and sizes of organisations

APEC Privacy Framework and CBPR (Cross-Border Privacy Rules System)

- BCR (Binding Corporate Rules)
- Accountability Agents
- Members: US, Mexico, Japan, Canada, Korea and Singapore

Let’s Prepare and Develop our Standards!

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ.2549

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553

ร่าง พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ... ได้รับความเห็นชอบในหลักการจากคณะรัฐมนตรีเมื่อวันที่ 22 พค. 2561