Thailand PDPA Compliance for Auditor

in legal perspective

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

Key Definition

PDPA: Personal Data Protection Act (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

GDPR: General Data Protection Regulation

Personal Data (ข้อมูลส่วนบุคคล): ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

Data Controller (ผู้ควบคุมข้อมูลส่วนบุคคล): บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

Data Processor (ผู้ประมวลผลข้อมูลส่วนบุคคล): บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

DPA: Data Processing Agreement (ข้อตกลงการประมวลผลข้อมูล)

Consent: ความยินยอมให้ประมวลผลข้อมูล

Privacy Notice: แบบแจ้งการประมวลผลข้อมูล

Thailand PDPA Framework

Lawfulness, fairness and transparency

Personal data shall be processed under *lawful basis*, and data subject shall be *aware of such processing*

Specific purpose

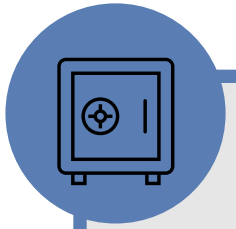
Personal data shall be processed only for *specific purposes* consented by or informed to data subject

Data Minimization

Personal data processed shall be *limited to what is necessary* for the purposes

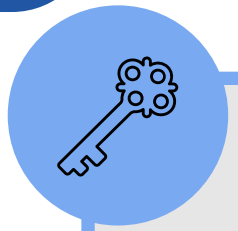
Spirit of

GDPR



Limited Storage

Personal data shall be kept for *no longer than is necessary* for its processing purposes



Integrity and Confidentiality

Personal data shall be processed in a manner that ensures *appropriate security* of such data

มุ่งมั่นพัฒนา รักษาจรรยาบรรณ สรรค์สร้างมาตรฐาน สืบสานวิชาชีพบัญชี

ONE LAW OFFICE

Lawful Basis

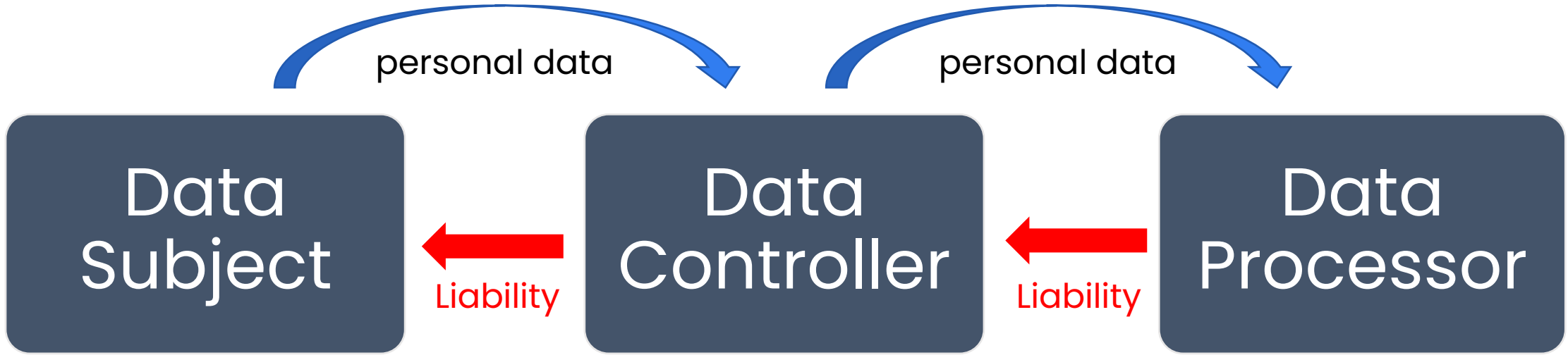
For Normal Personal Data

- Consent
- Contract
- Legal Obligation
- Legitimate Interest
- Vital Interest
- Public Task
- History Record/Statistic/Research

For Sensitive Personal Data

- Express Consent
- Legal Obligations in relation to
  public health, labor protection, social security, research and study
- Medical Service
- Establish and exercise of legal claims
- Self-expression
- Non-profit Organization
- Vital Interest

PDPA Key Players



A natural person identified or could be identified by the personal data

A person having power and duty to make decision regarding processing of the personal data

A person processing the personal data under the order or on behalf of Data Controller

Privacy Notice & Consent

Data Processing Agreement

ONE LAW OFFICE

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.0)

Example: Law firms

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing.

The law firm acts with a ***significant degree of independence***, for example in deciding ***what information to use and how to use it***, and there are ***no instructions from the client company regarding the personal data processing***.

The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as ***controller*** for this processing.

(page 12)

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.0)

Example: Accountants

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A.

Accounting firm C ***decides itself, in accordance with legal provisions regulating the tasks of the auditing activities*** carried out by C, that the ***data it collects will only be processed for the purpose of auditing A*** and it determines ***what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use***.

Under these circumstances, Accounting firm C is to be regarded as a ***controller*** of its own when performing its auditing services for A.

However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.

(pages 15-16)

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.0)

Example: Payroll administration

Employer A hires another company to administer the payment of salaries to its employees.

Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out ***for Company A's purpose to pay salaries to its employees*** and the payroll administrator may not use the data for any purpose of its own.

The way in which the payroll administrator should carry out the ***processing is in essence clearly and tightly defined***.

Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter ***its role as processor*** as long as the administrator does not go against or beyond the instructions given by Company A.

(pages 15-16)

Compliance Requirement

Requirement	Data Controller	Data processor
Obtain consent from data subject	✓	X
Notify data subject of the processing	✓	X
Respond to data subject's exercising of rights	✓	X(1)
Deploy appropriate security	✓	✓
Prevent unauthorized use and disclosure	✓	✓
Monitor and erase unnecessary data	✓	X
Report data breach to PDPC Office	✓	X(2)
Record processing activities(3)	✓	✓
Appoint DPO(4)	✓	✓
Process personal data as instructed by Controller	X	✓
Execute Data Processing Agreement	✓	✓

Compliance Requirement

Remark:

(1) Data processor shall have the duty to inform data controller if it encounters data subject's exercising of rights

(2) Data processor shall have the duty to inform data controller if it encounters any data breach

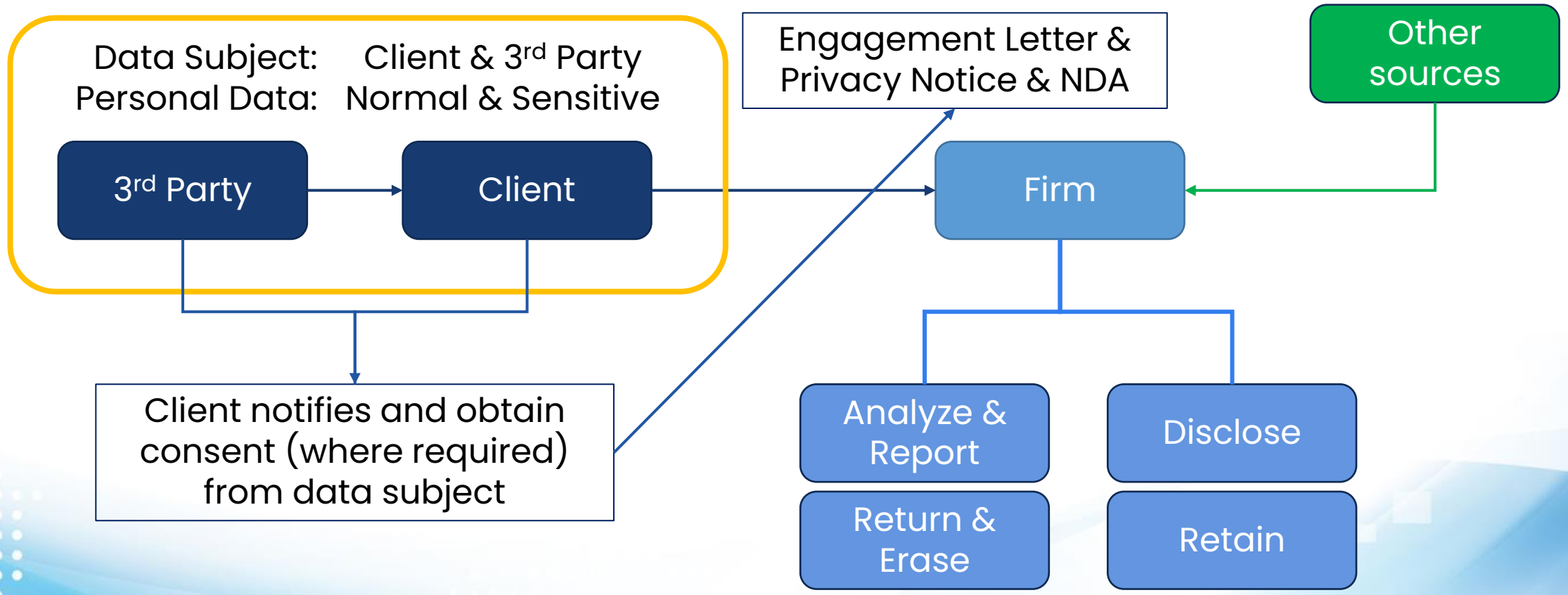
(3) Possible exemption from the duty to record processing activities

"อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด ***เว้นแต่*** มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือ***มิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว*** หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖"

(4) Possible exemption from the duty to appoint DPO

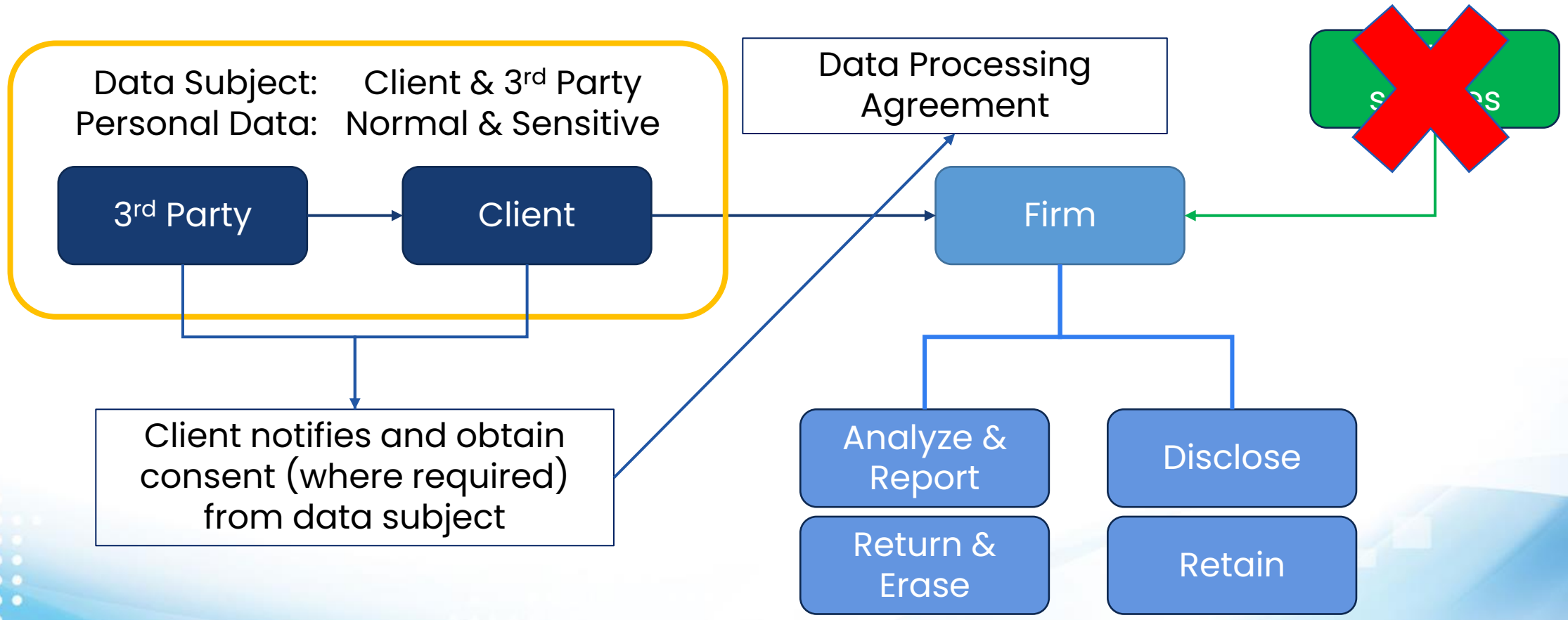
"มีข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอยู่ภายใต้ความดูแลภายในรอบระยะเวลาสิบสองเดือนมากกว่า 50,000 ราย หรือมากกว่า 5,000 รายในกรณีที่ข้อมูลส่วนบุคคล ดังกล่าวเป็นข้อมูลส่วนบุคคลตามมาตรา 26"

Working as a Data Controller



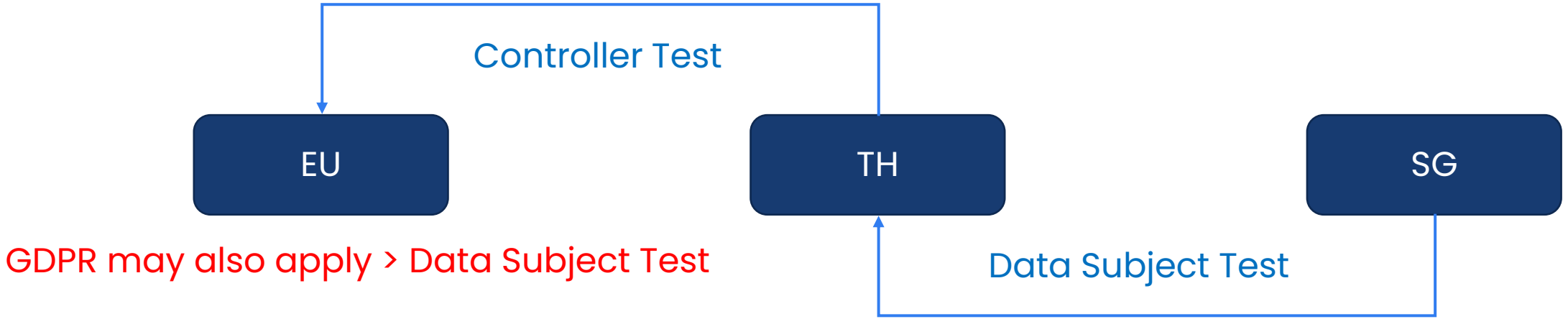
ONE LAW OFFICE

Working as a Data Processor



Cross-border Data Processing

Thai Co. transfers data to or receives data from EU > Thai PDPA applies



SG Co. receives data from TH > Thai PDPA applies

Outward Transmission from TH

- Adequate security
- Legal exception
- Binding Corporate Rule (BCR)
- Appropriate Safeguard

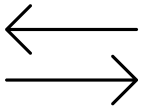
What should be done?

Know your data subject

Who is your *Data Subject* and what are their *Personal Data* you are processing ?

Understand your purposes

Why are you processing such personal data ?



Keep tracking changes

Do you still process the same personal data for the same purposes ?

Ensure appropriate security

Can you foresee any risk when using, disclosing or keeping personal data ?

Report if required

Do you know who you should be in contact with if anything goes wrong with the personal data ?

THANK YOU

https://www.tfac.or.th

@TFAC.FAMILY

tfac@tfac.or.th

https://www.facebook.com/TFAC.FAMILY

https:// www.youtube.com/TFACFamily

02 685 2500