LAW CHULA · SET · RAJAH & TANN ASIA LAWYERS WHO KNOW ASIA · Linklaters · Therakupt INTERNATIONAL LAW OFFICE LTD. · CHANDLER MHM

TDPG 2.0 :
Building Trust with Data Protection

22 ตุลาคม 2562

Go to
pigeonhole.at

Enter passcode

TDPG2

อัญชลี กลิ่นเกษร

Lawful Basis for Processing

Dherakupt
INTERNATIONAL LAW OFFICE LTD.

ศุภวัฒก์ ศรีรุ่งเรือง

Legitimate Interest + Anonymisation

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

พิชิตพล
เอี่ยมมงคลชัย

Data Protection Impact Assessment (DPIA)

Linklaters

อัครพล
พิเชษฐวณิชยโชค

Cross-border Data Transfer

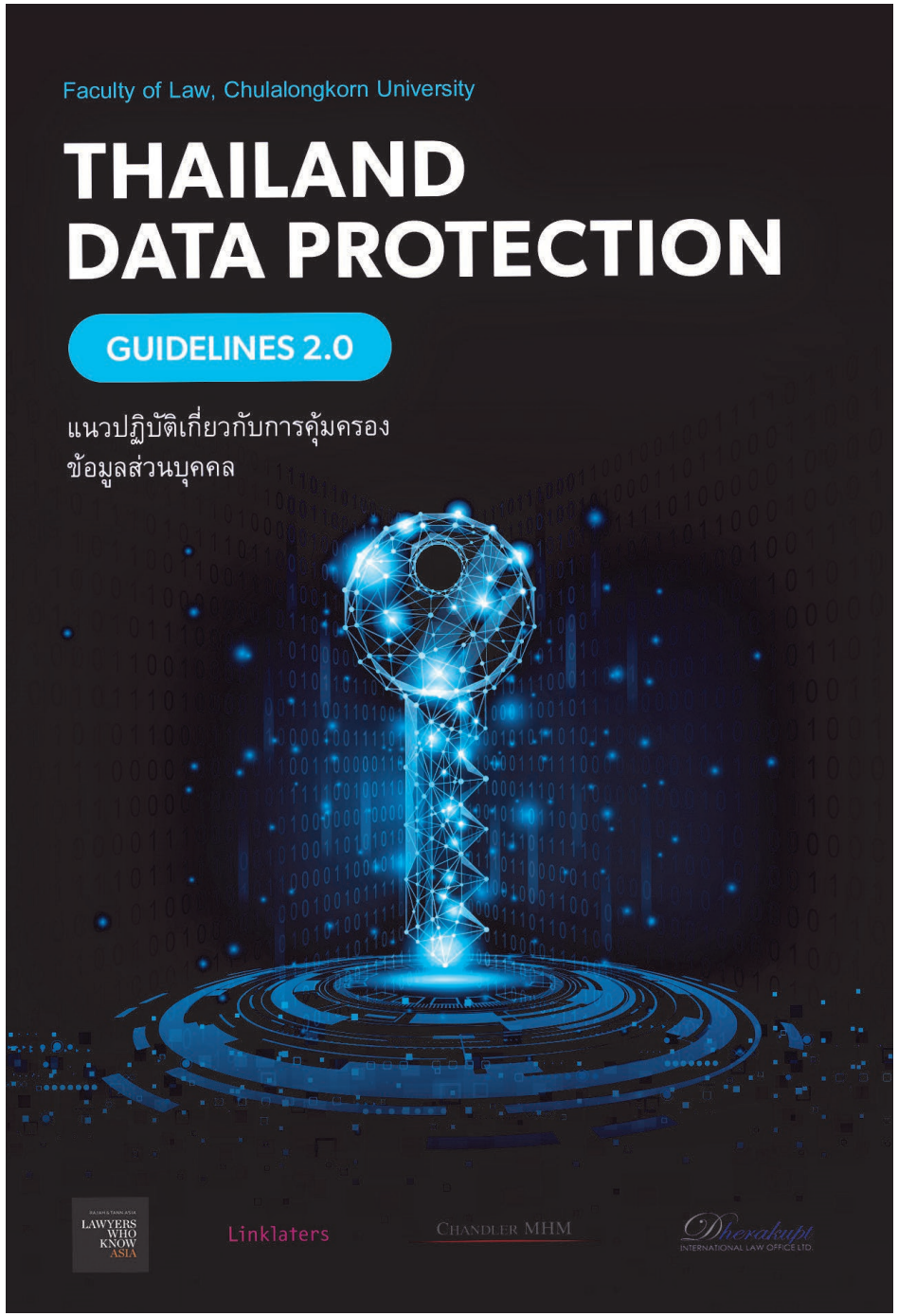
CHANDLER MHM

Go to
pigeonhole.at

Enter passcode

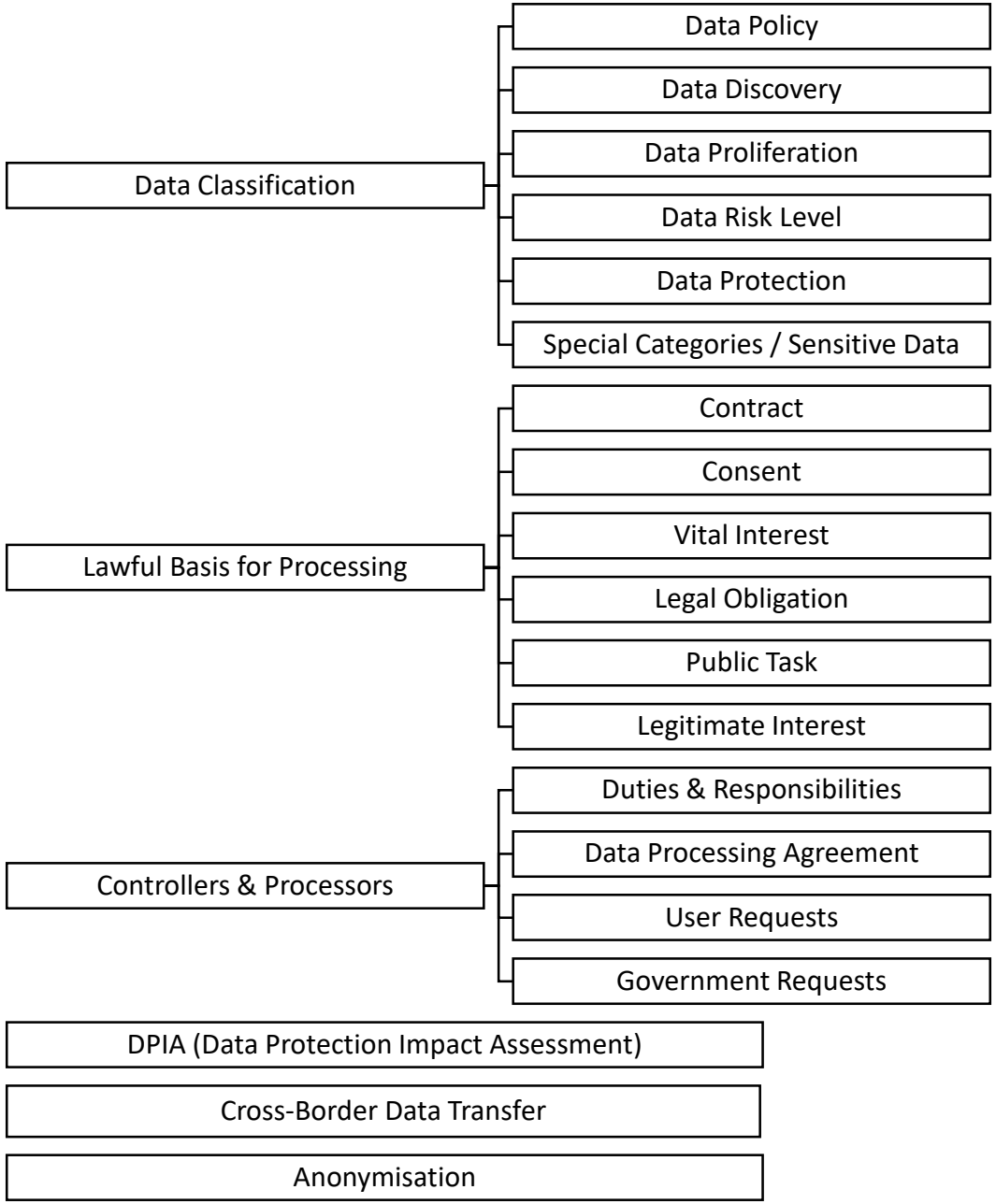
TDPG2

Q/A



http://www.law.chula.ac.th/event/6662/

ISBN 978-616-407-458-3


Data Classification
Data Policy
Data Discovery
Data Proliferation
Data Risk Level
Data Protection
Special Categories / Sensitive Data
Lawful Basis for Processing
Contract
Consent
Vital Interest
Legal Obligation
Public Task
Legitimate Interest
Controllers & Processors
Duties & Responsibilities
Data Processing Agreement
User Requests
Government Requests
DPIA (Data Protection Impact Assessment)
Cross-Border Data Transfer
Anonymisation

Lawful Basis for Processing

Thitirat Thipsamritkul

ฐานในการประมวลผล (Lawful Basis)

GDPR (Art.6)	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (มาตรา 24)
Consent	ความยินยอม
-	จดหมายเหตุ/วิจัย*
Vital Interest	ระงับอันตรายต่อชีวิต/ร่างกาย/สุขภาพ
Contract	สัญญา
Public Task / Official Authority	ภารกิจสาธารณะ/อำนาจรัฐ
Legitimate Interest	ประโยชน์โดยชอบด้วยกฎหมาย
Legal Obligation**	ปฏิบัติตามกฎหมาย**

*ต้องดำเนินมาตรการปกป้องตามที่คณะกรรมการประกาศกำหนด

**ประโยชน์ดังกล่าวต้องไม่มีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

ฐานสัญญา (Contract) หรือ ฐานความยินยอม (Consent)

จำเป็น สำหรับสัญญา	ทางเลือก ของเจ้าของข้อมูล
ที่อยู่สำหรับจัดส่งสินค้า อีเมล์สำหรับส่งใบเสร็จ	อีเมล์สำหรับการส่งจดหมายข่าว
ข้อมูลบัตรเครดิตสำหรับจองโรงแรม	ข้อมูลบัตรเครดิตที่เลือกให้เว็บไซต์จำไว้เพื่อความสะดวกในการจ่ายเงินครั้งต่อไป

“จำเป็น” ในการปฏิบัติตามสัญญา

- “จำเป็น” — ตามปกติของการดำเนินงานให้เป็นไปตามสัญญา
- **ไม่รวมถึงกรณีปัญญาข้อพิพาทที่เกิดขึ้นจากสัญญา**
  - ✗ เปิดเผยข้อมูลให้หน่วยงานภายนอกเพื่อติดตามทวงหนี้
  - ✗ รวบรวมข้อมูลเพื่อฟ้องร้องต่อการไม่ปฏิบัติตามสัญญา
  - ✗ เปิดเผยข้อมูลในการเปิดประมูลสินทรัพย์เพื่อชดใช้หนี้
  - → ฐานอื่น เช่น ผลประโยชน์อันชอบธรรม ความยินยอม

ค่ามาตรฐาน (default) ของความยินยอม

GDPR Art. 7, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ม. 19

- **“ให้โดยอิสระ เฉพาะเจาะจง โดยทราบข้อมูลที่เกี่ยวข้อง และชัดแจ้ง”** (GDPR - *Freely given, specific, informed and unambiguous* by a statement or *by a clear affirmative action.*
- ☑ ดังนั้นควรเป็น **Opt-in เสมอ !**
- ✕ **Pre-ticked ใช้ไม่ได้ !**
- ❗ **Opt-out อาจใช้ได้เฉพาะบางบริบท** (เช่น ลูกค้าเก่า
- *ให้**ก่อน**ที่จะเก็บรวบรวมข้อมูล*
- ***ไม่เป็นเงื่อนไข**ของการให้บริการ / แยกส่วนออกจากการให้บริการ*
- *วัตถุประสงค์**เฉพาะเจาะจง** โดยเข้าถึงได้ เข้าใจได้ อ่านง่าย*
- *มีทางเลือกให้**ปฏิเสธได้** หรือถอนได้โดยไม่เสียประโยชน์*

WHOM

WHAT

HOW

WHEN

CONTACT

ความยินยอมที่ได้มาก่อนที่กฎหมายจะมีผลบังคับใช้

- ✕ ใช้ไม่ได้กับ GDPR
- ! ควรใช้เฉพาะกรณีของลูกค้าเก่าที่ติดต่อยาก + จำเป็นจริงๆ
- ✕ ความยินยอมแบบเหมารวม (Blanket Consent ใช้ไม่ได้ !!
- แยกแยะ

- **ควรแจ้งรายละเอียด**เพื่อปรับปรุงให้ความยินยอมสอดคล้องกับกฎหมายปัจจุบัน
  - แจ้งเป็นการทั่วไป + ช่องทางสำหรับ opt-out
  - แจ้งเมื่อมีการติดต่อธุรกรรมกับลูกค้า

ความยินยอมที่ได้มาก่อนที่กฎหมายจะมีผลบังคับใช้

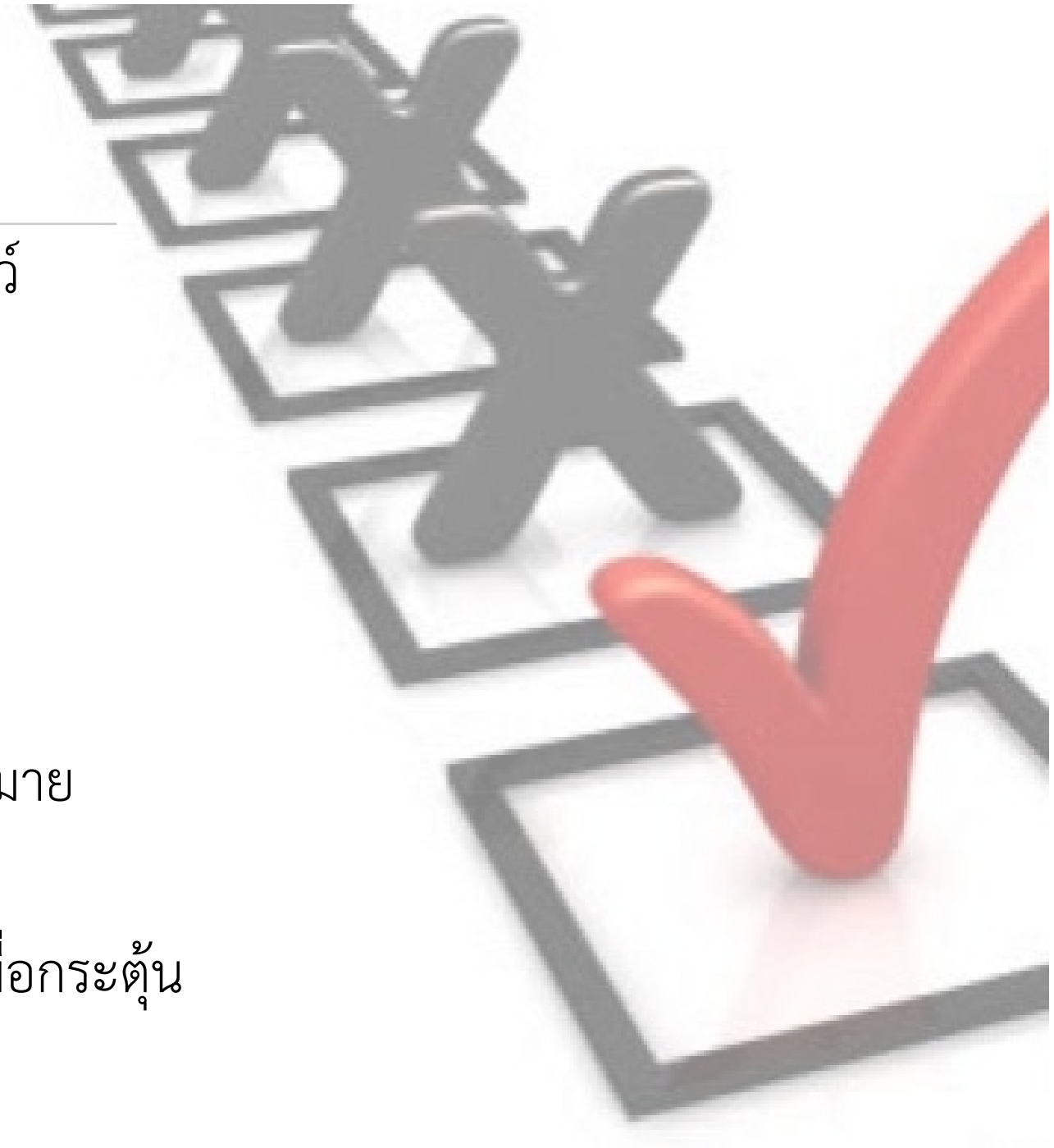
- ตัวอย่าง : “ผู้ใช้บริการยินยอมให้บริษัท X เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อใช้ในการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการได้เท่าที่จำเป็นเพื่อประโยชน์ในการดำเนินการปรับปรุงการให้บริการ โดยรวมถึงการวิเคราะห์และวางแผนทางการตลาด กิจกรรมทางการตลาด และกิจกรรมอื่นๆ อีกทั้งยินยอมให้ผู้ให้บริการแจ้งข้อมูลข่าวสาร รายการส่งเสริมการขาย และข้อเสนอต่างๆเกี่ยวกับการสมัครและการซื้อขาย สินค้า หรือบริการต่างๆของผู้ให้บริการ ตลอดจนการให้บริการใดๆ ร่วมกับบุคคลอื่น ซึ่งรวมถึงยินยอมให้ผู้ให้บริการสามารถเปิดเผย ส่ง และโอนข้อมูลส่วนบุคคลของผู้ใช้บริการให้แก่บุคคลภายนอกได้”

ความยินยอมที่ได้มาก่อนที่กฎหมายจะมีผลบังคับใช้

- ตัวอย่าง : “ผู้ใช้บริการยินยอมให้บริษัท X เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการ**เพื่อใช้ในการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการได้เท่าที่จำเป็นเพื่อประโยชน์ในการดำเนินการปรับปรุงการให้บริการ โดยรวมถึงการวิเคราะห์และวางแผนทางการตลาด กิจกรรมทางการตลาด และกิจกรรมอื่นๆ** อีกทั้งยินยอมให้ผู้ให้บริการ**แจ้งข้อมูล ข่าวสาร รายการส่งเสริมการขาย และข้อเสนอต่างๆเกี่ยวกับการสมัคร และการซื้อขายสินค้า หรือบริการต่างๆ ของผู้ให้บริการ** ตลอดจนการให้บริการใดๆ ร่วมกับบุคคลอื่น ซึ่งรวมถึงยินยอมให้ผู้ให้บริการสามารถเปิดเผย ส่ง และโอนข้อมูลส่วนบุคคลของผู้ใช้บริการให้แก่บุคคลภายนอกได้”

กรณีควรระวัง

- การขอความยินยอมจากผู้เยาว์
- การทำการตลาดแบบตรง (Direct Marketing
- ระบบสมาชิกสะสมแต้ม (Loyalty Program
- การโฆษณาแบบเจาะจงเป้าหมาย (Targeted Advertisement
- การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุ้นยอดขาย



ฐานปฏิบัติตามกฎหมาย (Legal Obligation) หรือ ฐานภารกิจสาธารณะ (Public Task) ?

(ผู้ควบคุมข้อมูล) ปฏิบัติตามกฎหมายที่ต้องทำอยู่แล้ว	(เจ้าหน้าที่) ปฏิบัติหน้าที่เพื่อบรรลุภารกิจสาธารณะ
บริษัทแจ้งข้อมูลการจ่ายเงินเดือนพนักงานต่อสรรพากร	สรรพากรประมวลผลข้อมูลเงินเดือน
องค์กรทางการเงินส่งข้อมูลการทำธุรกรรมที่น่าสงสัยให้หน่วยงานปราบปรามการฟอกเงิน	หน่วยงานปราบปรามการฟอกเงินประมวลผลข้อมูลธุรกรรมที่น่าสงสัยเพื่อนำไปตรวจสอบต่อ

ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)

- ❗ความเสี่ยงสูง ควรใช้ในกรณีที่ใช้ฐานอื่นไม่ได้ (ไม่เหมาะสม
- ✅ ใช้เท่าที่จำเป็น (ใช้ให้น้อยที่สุด

  - LIA — Legitimate Interest Assessments
    - A. Expectation
    - B. Risk
    - C. Safeguard

- ตัวอย่าง : การยืนยันตัวตนลูกค้า, ข้อมูลการทำงานของลูกจ้าง, ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย, industry watch-list, ข้อมูลเพื่อการปรับปรุงการให้บริการ ฯลฯ

ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

- ✅ ใช้ได้เฉพาะข้อมูลที่ไม่ใช่ sensitive data
  - เช่น ข้อมูลสิทธิการรักษาพยาบาล ข้อมูลการเดินทางไปประเทศที่มีโรคติดต่อ
- ✅ ใช้เมื่ออยู่ในสถานการณ์ที่ขอความยินยอมไม่ได้เท่านั้น หากขอความยินยอมได้ให้ใช้ความยินยอม

ฐานจดหมายเหตุ/วิจัย/สถิติ

- ❌ ไม่มีใน GDPR
- ✅ ควรเป็นไปตามมาตรฐานการวิจัย หรือมาตรฐานวิชาชีพ
- ✅ ต้องมี Safeguard (รอประกาศของกระทรวง

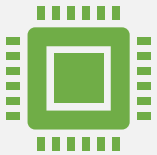
Data Protection Officer (DPO)

Chawin Ounpat

Who must designate DPO?

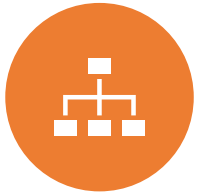
public authority & body (as designated by the Committee)

data controller & processor where the core activities consist of regular and systematic monitoring of data subjects on a large scale (as designated by the Committee)



data controller & processor where the core activities involve the processing of sensitive data

Who is qualified to be a DPO?



business model & organization

IT and data management

data protection law

Controller/Processor and DPO

Employment contract

Service contract

Tasks of DPO

Ensuring	Ensuring the compliance with PDPA
Performing	Performing tasks in an independent manner
Cooperating	Cooperating with the regulator

Safeguards to ensure DPO can act in an independent manner

No instruction by the controller/processor regarding the exercise of the DPOs tasks

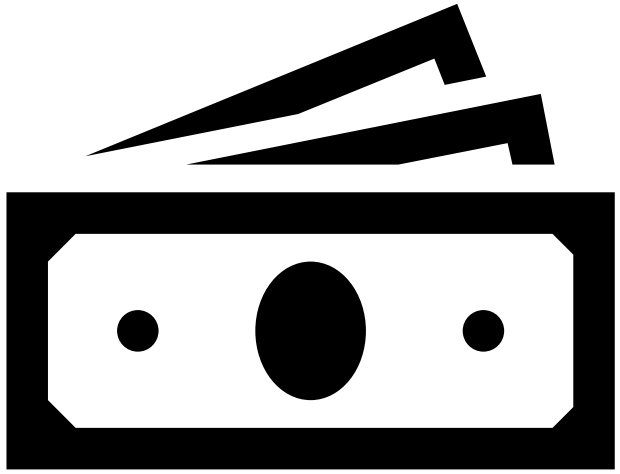
No dismissal or penalty by the controller for the performance of the DPO’s tasks

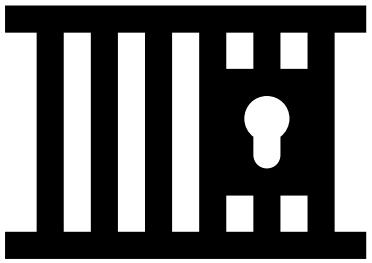
No conflict of interest with possible tasks and duties

DPO must be supported by the controller/processor

necessary resources must be provided to perform DPO's tasks

failure to provide sufficient resources for DPO leads to controller/processor's liability





Is DPO liable for the failure to comply with PDPA?

Data Protection Impact Assessment

When it is likely to result in a high risk to the rights and freedoms of natural persons

Piyabutr Bunaramrueang

Data Protection Impact Assessment

systematic description

assessment of the necessity and proportionality

assessment of the risks to the rights and freedoms

measures envisaged to address the risks

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- มาตรา 30 กำหนดให้ผู้ควบคุมข้อมูลต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลให้เจ้าของข้อมูลทราบถึง**ผลกระทบที่อาจก่อนให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น**
- มาตรา 37(4 กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม**ความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล**
- มาตรา 39 วรรคสาม และมาตรา 40 วรรคสี่ กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกรายการโดยคำนึงถึง**ความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล**
- มาตรา 37(1 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป
- มาตรา 39(8 และมาตรา 40(2 กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกรายการโดยคำอธิบาย และจัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม**
- มาตรา 4 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มี**การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน**ด้วย

Risk to the rights and freedoms

Likelihood

Severity

Severity \ Likelihood	โอกาสต่ำ	โอกาสพอสมควร	โอกาสสูง
ร้ายแรงมาก	ระดับต่ำ	ระดับสูง	ระดับสูง
ร้ายแรงพอสมควร	ระดับต่ำ	ระดับกลาง	ระดับสูง
ร้ายแรงน้อย	ระดับต่ำ	ระดับต่ำ	ระดับต่ำ

Factors of high risk to the rights and freedoms

Systematic and extensive profiling with significant effects

Processing of sensitive data on a large scale

Public monitoring on a large scale

Scoring

Automated-decision with legal effect

Systematic monitoring

Sensitive data

Large scale

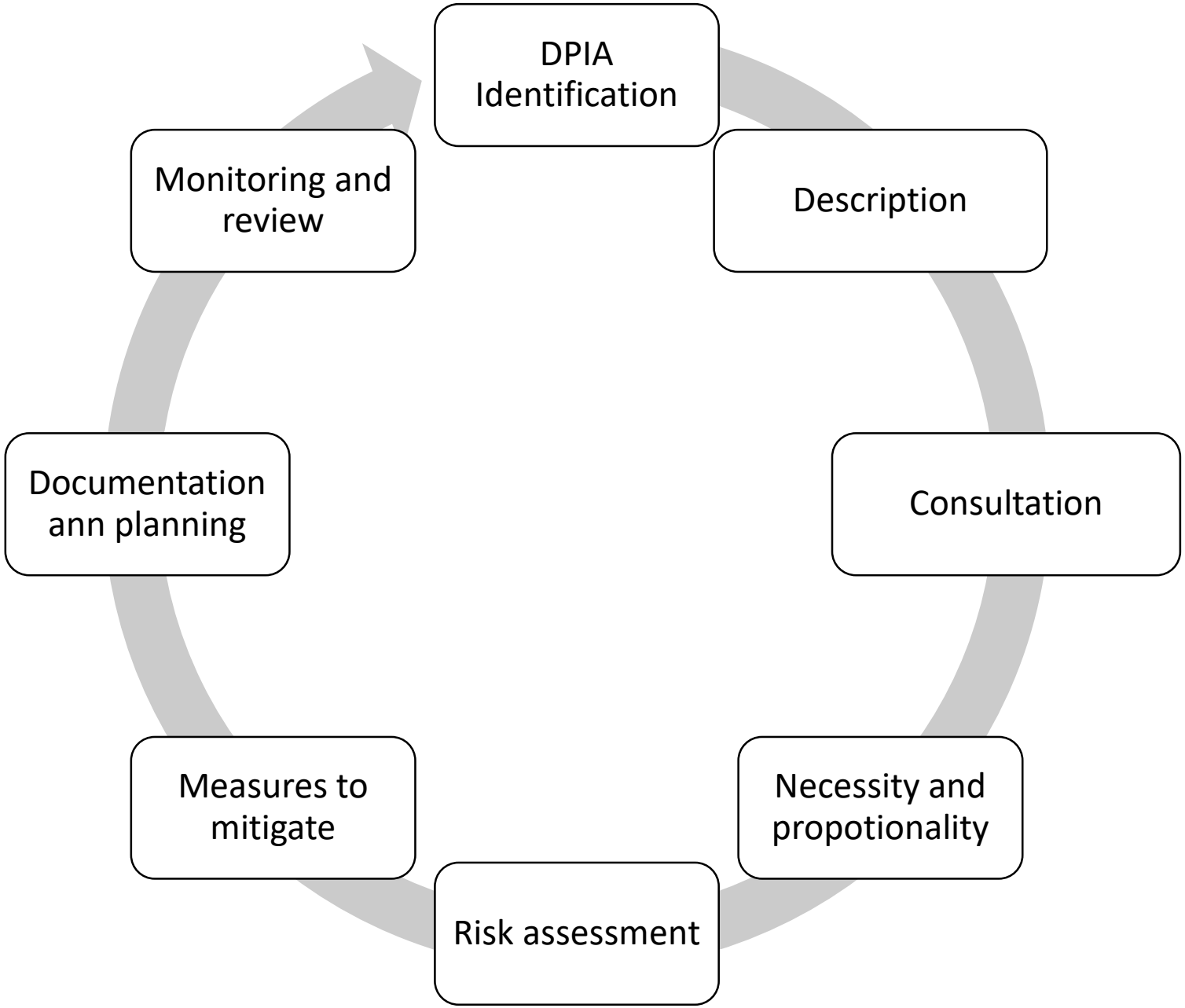
Combining datasets

Vulnerable data subjects

Innovative use

Prevent data subjects’ right or access

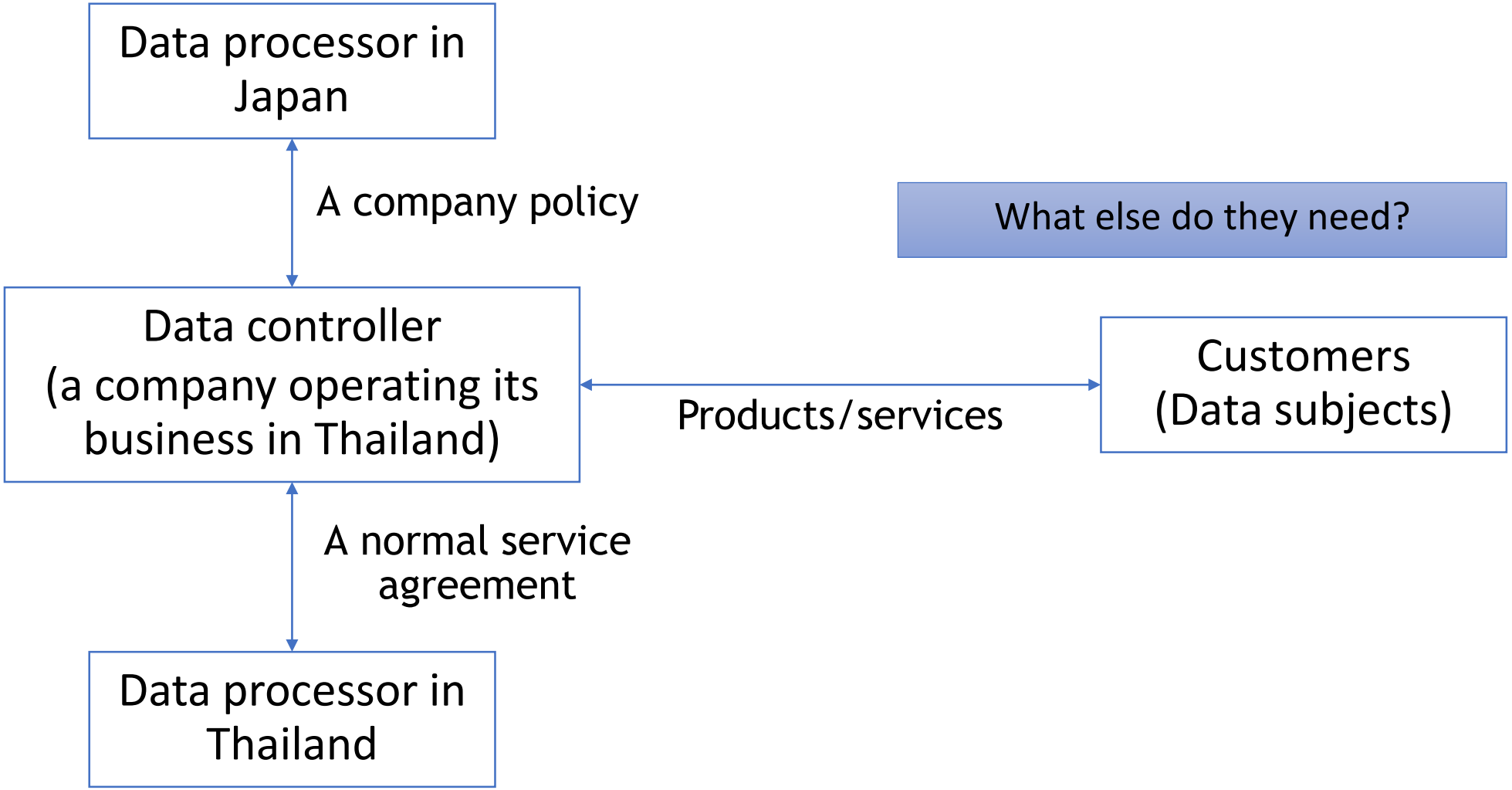
DPIA Process



Data Processing Agreement (DPA) & Cross-Border Transfer (BCRs)

Piti Eiamchamroonlarp

Overview


Data processor in Japan
A company policy
What else do they need?
Data controller (a company operating its business in Thailand)
Products/services
Customers (Data subjects)
A normal service agreement
Data processor in Thailand

DPA (Data Processing Agreement)

General provisions	• Serving as a part of the main service agreement (e.g. an annex) • Status of the parties (e.g. a service provider as a data processor) • Definition (including data breach)
Undertakings	• Processing only as legally instructed (e.g. the processing is done in accordance with the collection and processing objectives) • Suitability of the processor's security system • The processor's duty to handle a data breach • Data storage and deletion

Cross-border data transfer

1. Restricted transfer	• Definition of cross-border transferring • Transfer vs. Transit
2. Adequate level of protection	• Applicable law • Institutional framework • International obligation
3. Exceptions	(for example) • consent & contract • vital interest & legitimate interest
4. Binding corporate rules	(for example) • Binding corporate rules (BCRs)

The policy	▪ Legally binding effect ▪ Parties that are subject to the legally binding rules
Definitions	• Corporate control (and a list of affiliates) • Transmission and excluding transit
Protection	• Lawful basis for data processing (e.g. providing details in an annex) • Security of the system • Data storage

BCRs (Binding Corporate Rules)

BCRs (Binding Corporate Rules)

Rights of the data subject	• Those guaranteed by the PDPA (in absence of the local law)
Mechanisms	• Duties of a DPO (if applicable) • Data breach • Complaint • Investigation

Anonymisation

How to make the data query ‘safe’

Peerapat Chokesuwattanaskul

87%  

Use just what you need to use &
Most of the time, you don’t need to know or provide IIP.
Information from data is derived from inference.

Outlines

1. What is data anonymisation?
2. Who has to do it?
3. How to do it?

1. What?

Anonymisation?

กระบวนการ

ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูล

นั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญ

2. Who?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- มาตรา 37
  - (1 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป
  - (๒ ในกรณีที่ต้อง**ให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น**ที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้อง **ดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคล**โดยปราศจากอำนาจ หรือโดยมิชอบ
- มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
  - (๒ **จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล**โดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- มาตรา 4 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มี**การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน**ด้วย

3. How?


ข้อมูล
สภาพ
แวดล้อม
ข้อมูล
นิรนาม

Trade-offs

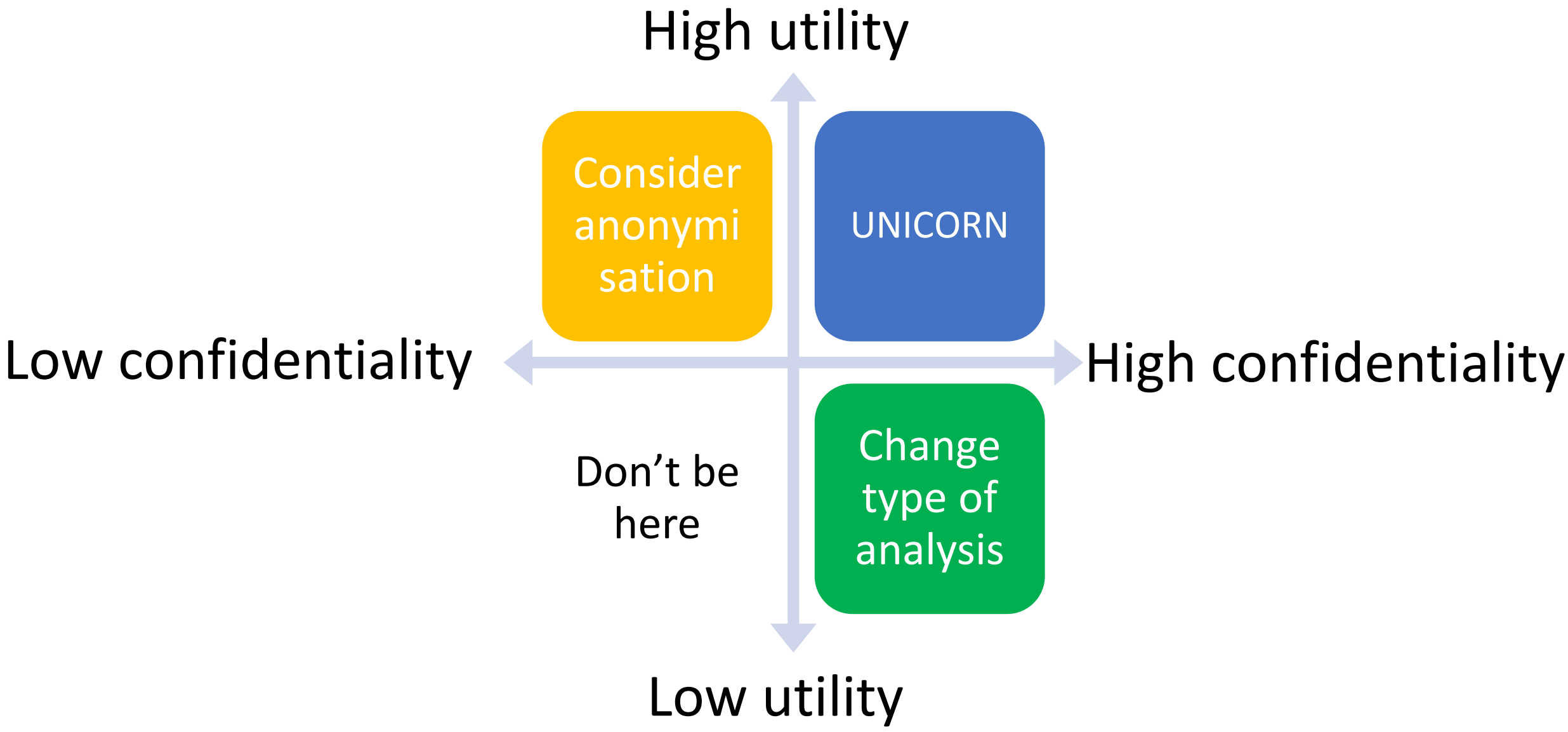
Utility

Type of analysis

Confidentiality

Data

Environment


High utility
Consider anonymi sation
UNICORN
Low confidentiality
High confidentiality
Don’t be here
Change type of analysis
Low utility

Utility 100%
Privacy 0%

ชื่อ	วันเกิด	คะแนน
ก	7 สิงหาคม 2550	A
ข	23 มีนาคม 2550	C
ค	25 มกราคม 2551	B

Utility 0%
Privacy 100%

ชื่อ	วันเกิด	คะแนน
ก	-	A-C
ข	-	A-C
ค	-	A-C

Utility 50%
Privacy 50%

ชื่อ	วันเกิด	คะแนน
ก	2550 - 2551	A
ข	-	-
ค	2550 - 2551	B

Data situation

- Data flowchart
- Controller/processor?
- Data characteristics
- All principles applied (legality, consent, etc.)

Risk

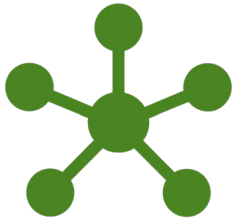
- Data evaluation
- Tests
  - Motivated intruder test
  - Precedent comparison
- Possible attacks
  - Linkage
  - Attribution
  - Subtraction
  - Etc.

Measures

- Change data
  - Meta-level > Micro-level
  - Aggregation
  - Drop
  - Sampling
  - Distortion
  - Differential privacy***
- Change environment
  - Who can access?
  - What analysis?
  - Mode of access?

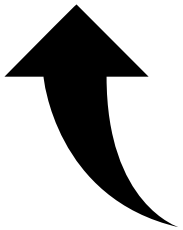
การจัดทำ
ข้อมูลนิรนาม
(Anonymisation)

การขจัดตัวตน
(De-
identification



การป้องกันการระบุ
ตัวตนโดยพิจารณา
ถึงสิ่งแวดล้อมของ
ข้อมูลด้วย

การแฝงข้อมูล
(Pseudony-
misation



ข้อมูลแบบรวมกลุ่ม
(Aggregation)

วิธีการอื่น ๆ

More concrete?

Privacy

Utility

Easiness

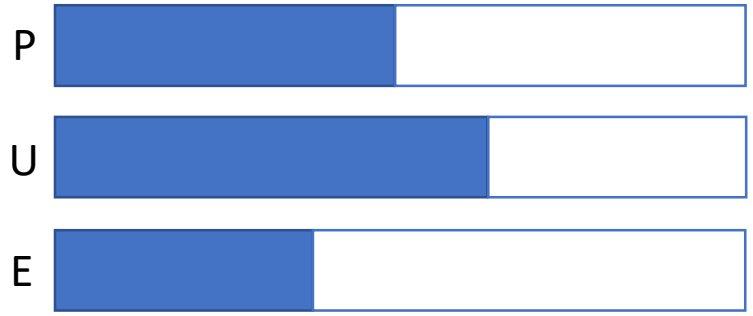
Which method should I choose then?

Pseudonymisation

User_id	Name	X
A00001	!@#EER	34
A00002	!e#$EW	48

K-anonymisation

User_id	Name	X
A000??	!?????	30 - 50
A000??	!?????	30 - 50



Differential privacy*

$$\theta + Z$$

Similar method at the record level is ‘synthetic’ data which doesn’t fall into DP

What this guideline will tell you in detail?

WHEN IS PSEUDONYMISATION SUFFICIENT?

K = ?

DIFFERENT PRIVACY EPSILON?