PDPA: Principles and Insights

Prapanpong Khumon

Advisor to Secretary-General of Personal Data Protection Commission, Thailand

5 February 2020

1. PDPA rational for protection

Why personal data needs protected:

Building trust

Getting trust from data subjects and consumers is vital. They will be more confident when the personal data management is transparent and proportionate.

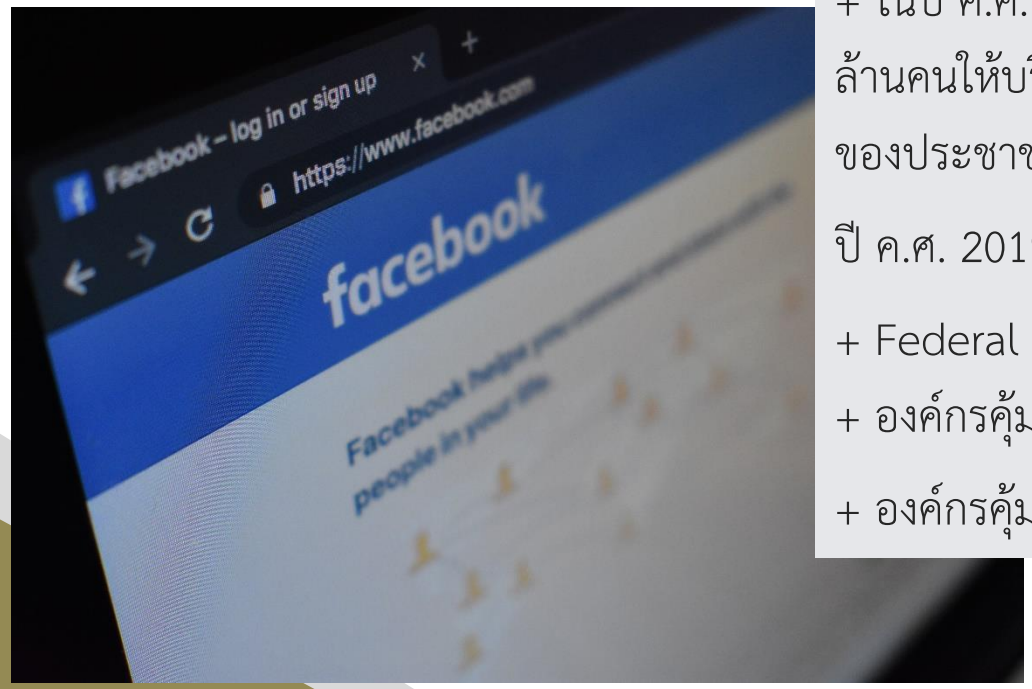
Better data governance

Good data governance is desirous in every organization. The more governance an organization has, the more likely they will gain trust from users and consumers.

Connecting with global standards

Global data transfer needs to connected with global standards of protection to foster free flows of data.

เหตุร้องเรียนจากทั่วโลก (กรณี Facebook – Cambridge Analytica)



+ ในปี ค.ศ. 2018 Facebook ส่งข้อมูลส่วนบุคคลของ User มากกว่า 50 ล้านคนให้บริษัท Cambridge Analytica ซึ่งเป็นบริษัทวิเคราะห์ความคิดเห็นของประชาชนด้านการเมือง โดยที่ไม่ได้ขอความยินยอมจาก User ก่อน

ปี ค.ศ. 2019 ประเทศต่างๆ มีคำตัดสินดังนี้

+ Federal Trade Commission ปรับ Facebook $5,000 ล้าน
+ องค์กรคุ้มครองข้อมูลส่วนบุคคลของอิตาลีปรับ Facebook € 1 ล้าน
+ องค์กรคุ้มครองข้อมูลส่วนบุคคลของอังกฤษปรับ Facebook £ 500,000

Photo by Con Karampelas on Unsplash

เหตุร้องเรียนจากทั่วโลก (กรณี Google – Right to be forgotten)

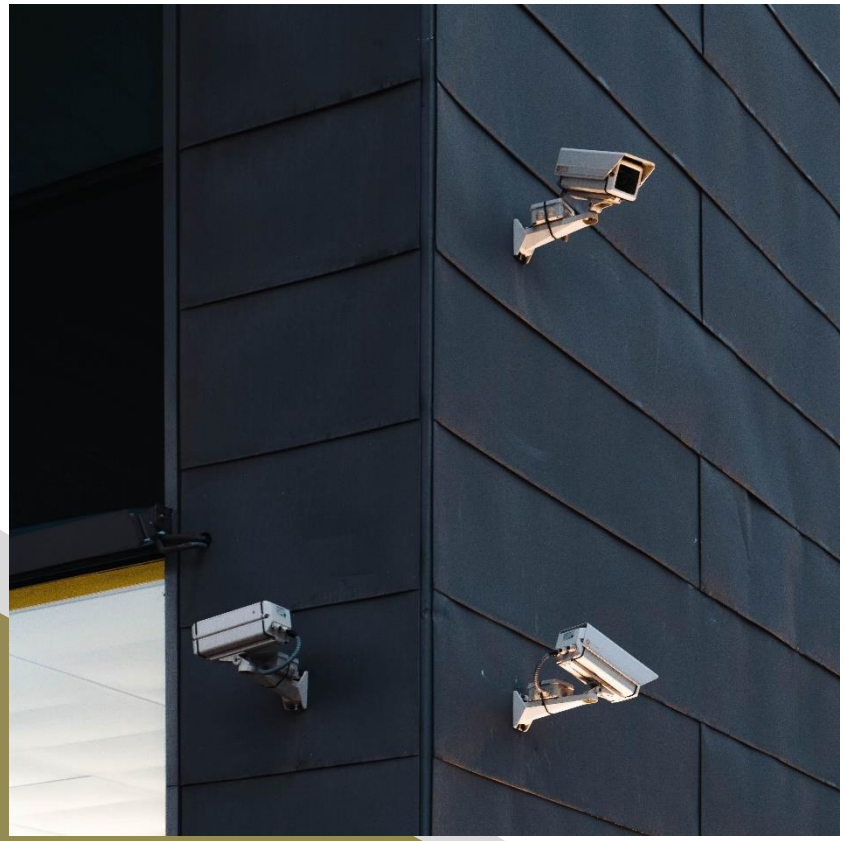
Google v. AEPD and Gonzáles 2014

ECJ Ruling C-131/12 (Right to be forgotten)

+ Gonzáles ขอศาลให้บริษัท Google ลบข้อมูลที่บ่งบอกว่า Gonzáles เป็นบุคคลที่อยู่ในกระบวนการพิจารณาล้มละลายซึ่งในปัจจุบันไม่เป็นความจริงอีกต่อไป

+ ศาลยุโรปตัดสินว่า บริษัท Google ในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องลบข้อมูลส่วนบุคคลที่ไม่ถูกต้อง หรือไม่ครบถ้วนตามจริง (inaccurate, inadequate, irreverent or excessive) ถ้าหากข้อมูลส่วนบุคคลเช่นว่านั้นสามารถนำไปประมวลผลได้ เมื่อบริษัท Google เพิกเฉยต่อหน้าที่นี้ ถือว่าละเมิดกฎหมายสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เหตุร้องเรียนจากทั่วโลก (กรณีการสอดแนมข้อมูล)



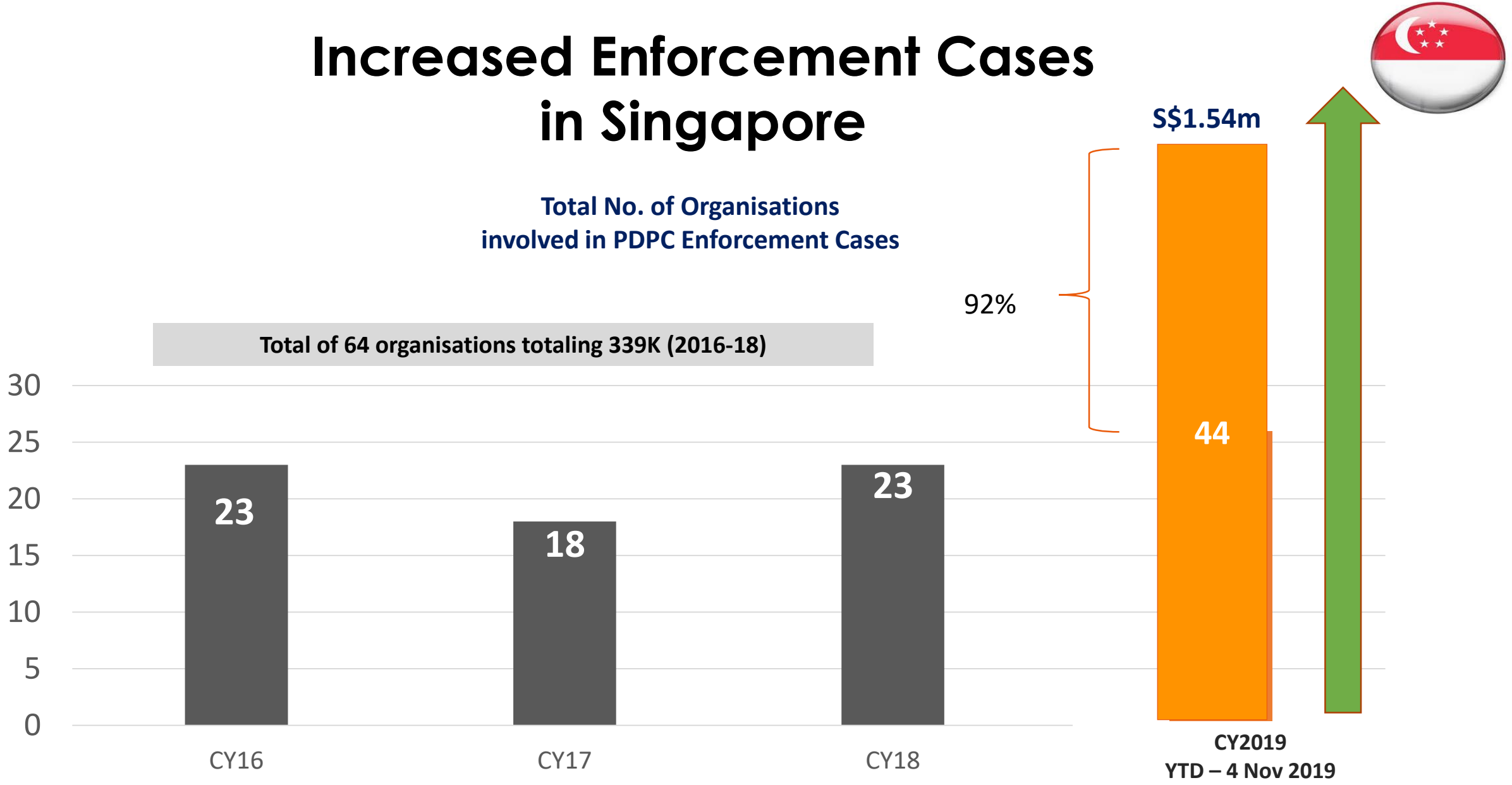
Maximillian Schrems v Data Protection Commissioner 2015 (ECJ C-362/14)

+ Schrems ในฐานะผู้ใช้บัญชี facebook เชื่อว่าข้อมูลที่เขาโพสต์ลงใน facebook ถูกสอดแนมโดยสำนักงานความมั่นคงของสหรัฐฯ

+ ศาลยุโรปตัดสินให้ความตกลง Safe Harbour (2001) ระหว่างยุโรปและสหรัฐฯ เป็นโมฆะเนื่องจากความตกลงฯ ไม่สามารถให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชนชาวยุโรปได้อย่างเพียงพอ

Photo by Ennio Dybeli on Unsplash

Increased Enforcement Cases in Singapore



Source: Straits Interactive 2020

Increased Enforcement Cases in Singapore

Vertical Industries	CY16	CY17	CY18	CY19	Total # of Companies	%
Consumer Services				2	2	2%
Education Services	1	2	3	3	9	8%
Educational Services				3	3	3%
Financial Services	2	4	5	6	17	15%
Food & Beverage	4	1	1	3	9	8%
Heatlhcare				2	2	2%
Industrial Goods & Services		2	2		4	3%
IT services	3			2	5	4%
Media & Entertainment	2		1	1	4	3%
Non-profit Organisation	3	1	5	1	10	9%
Professional Services		2	2	11	15	13%
Real Estate Services	1	2	1	1	5	4%
Retail	5	3	2	4	14	12%
Security Agency	1	1			2	2%
Telecommunications		1	1	3	5	4%
Transportation Services	1		1	2	4	3%
Travel & leisure	1	1	2	2	6	5%
Total # of Companies	**24**	**20**	**26**	**46**	**116**	**100%**

No Industry is spared from enforcement
(including non profit organisations)

Source: Straits Interactive 2020

Increased Enforcement Cases in Singapore

80% of all cases are due to a security lapse

Section/Year	CY16	CY17	CY18	CY19 YTD	Grand Total	%
11 (Compliance/DPO)	3	1	1	6	11	10%
12(a) Policies	3	1	5	13	22	20%
13 Consent	5	2	5	4	16	15%
18 Purpose Limitation	2		4	1	7	6%
20 Notification	4	1		3	8	7%
21 Access						0%
23 Accuracy						0%
24 Protection	18	16	17	35	86	80%
25 Retention		1		1	2	2%
26 Transfer				2	2	2%

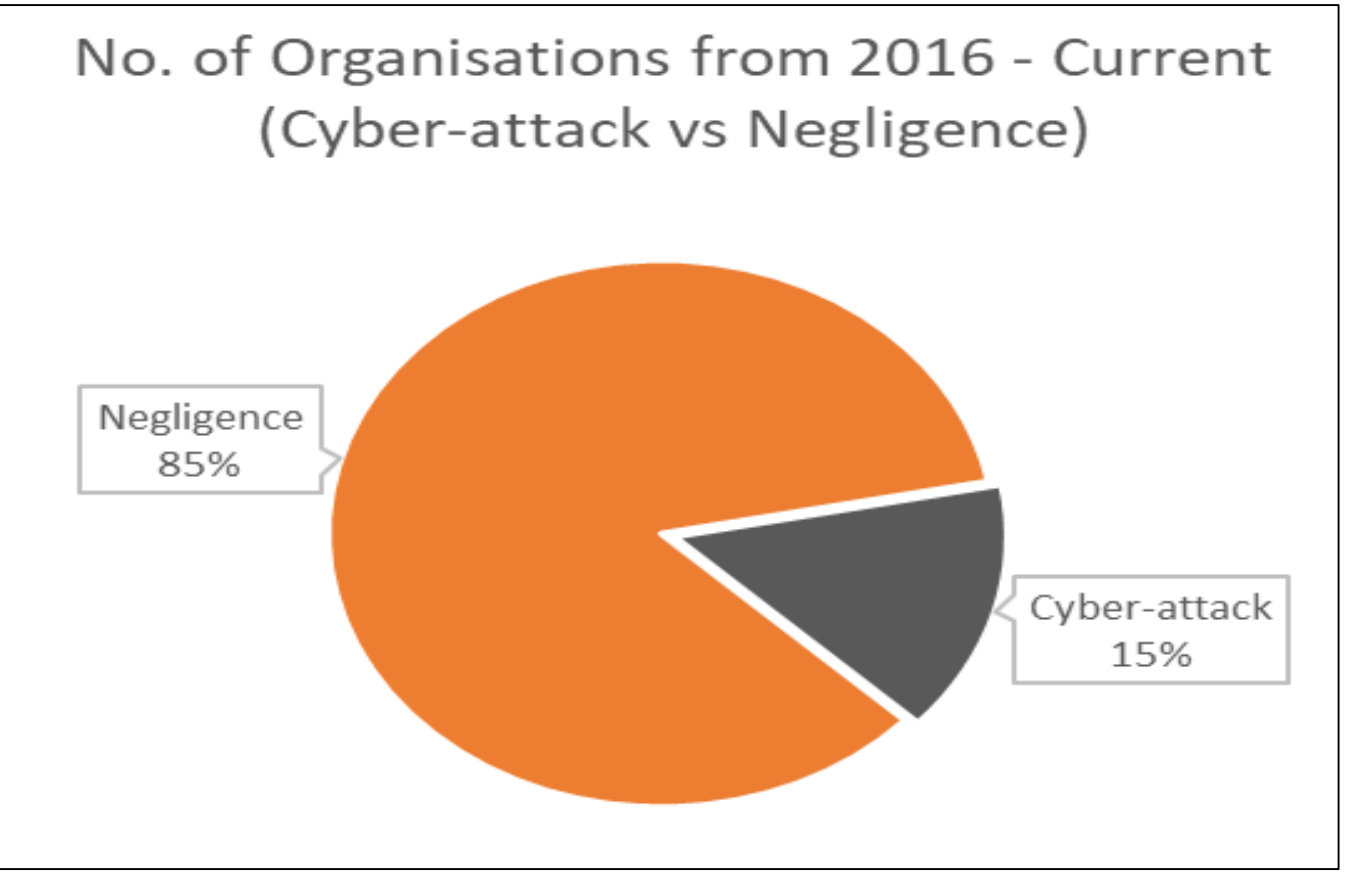
# Organisation	23	18	23	44	108

Note: One organisation can breach multiple obligations

Source: Straits Interactive 2020

Increased Enforcement Cases in Singapore

80% of all cases are due to a security lapse



Out of the companies that breached the Protection Obligation, only 15% were linked to an actual cyber attack/hacking

Protection Obligation	CY16	CY17	CY18	CY19 YTD	Grand Total
CYBER ATTACK/HACKED	8	1		3	12
NEGLIGENCE	10	15	17	22	64
Grand Total	**18**	**16**	**17**	**25**	**76**
%	44%	6%	0%	12%	16%

Source: Straits Interactive 2020

Both public and private sectors to grapple with data protection issues and new requirements

Public sector and Data Protection Requirements

Hong Kong (1995)

Philippines DPA (2012)

Thailand PDPA (2019)

Indonesia PDP Bill (2020*)

Malaysia PDPA (2010)

Singapore PDPA (2010)

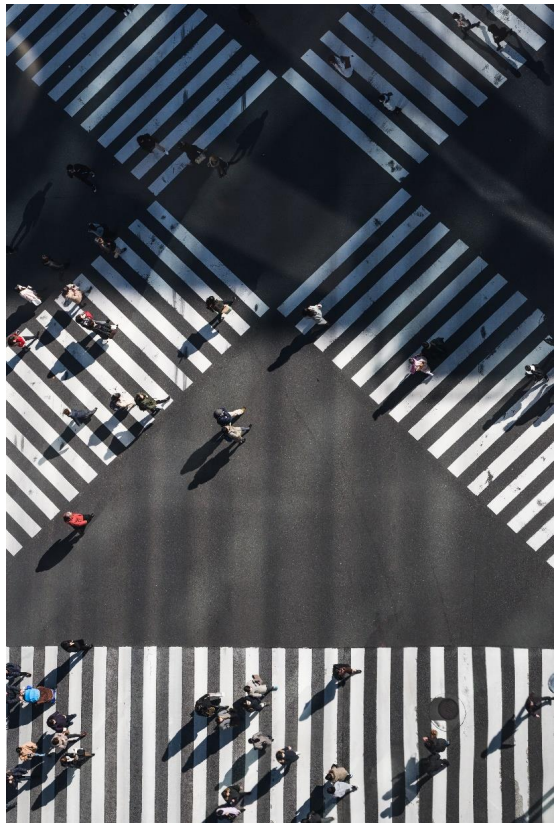
Countries with Comprehensive Laws covering the public sector

Review of PDPA – includes Applicability to public sector being evaluated

SG: Public Sector Data Security Review Committee: Recommendations to protect personal data

Source: Straits Interactive 2020

2. Thai PDPA: essential features



Comprehensive protection

- Covering both public and private entities
- Sanction-based approach: administrative fines

Adopting GDPR-Like model

- Transparency principle
- Lawful grounds of processing
- Rights of data subject to access and control the data

Extraterritorial reach

- For activities that offer goods or services to data subjects in Thailand
- or monitoring data subjects behavior in Thailand

Risked-based approach

- Scale of responsibility varies on size and functions of data processing
- DPO required for public bodies and organizations with large scale processing

Photo by Ryoji Iwata on Unsplash

อะไรคือข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data)

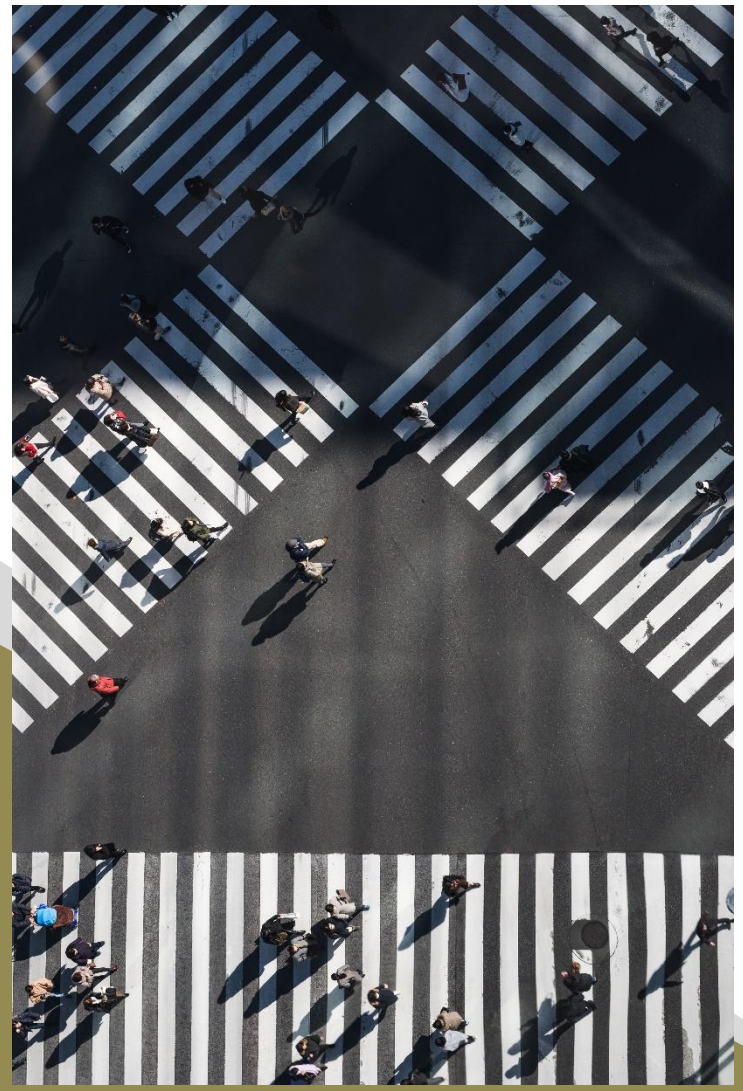
+ หมายถึงข้อมูลที่ทำให้สามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าโดยตรงหรือโดยอ้อม (สำหรับบุคคลที่ยังมีชีวิตอยู่) เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ location ฯลฯ

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

+ เป็นข้อมูลที่จะต้องให้ความระมัดระวังเป็นพิเศษในการเก็บรวบรวม/ประมวลผล เช่น ข้อมูลที่บอกชาติพันธุ์ เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา ข้อมูลพันธุกรรม รสนิยมทางเพศ ข้อมูลชีวภาพ

+ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

บังคับใช้กับใคร



+ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- หน่วยงานภาครัฐและเอกชนที่เก็บและใช้ข้อมูลส่วนบุคคล ยกเว้น การดำเนินงานที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ กิจการสื่อมวลชน งานศิลปกรรม งานวรรณกรรม และอื่นๆ ตามที่กำหนดในมาตรา 4 (แต่หน่วยงานเหล่านี้ยังต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย)

+ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

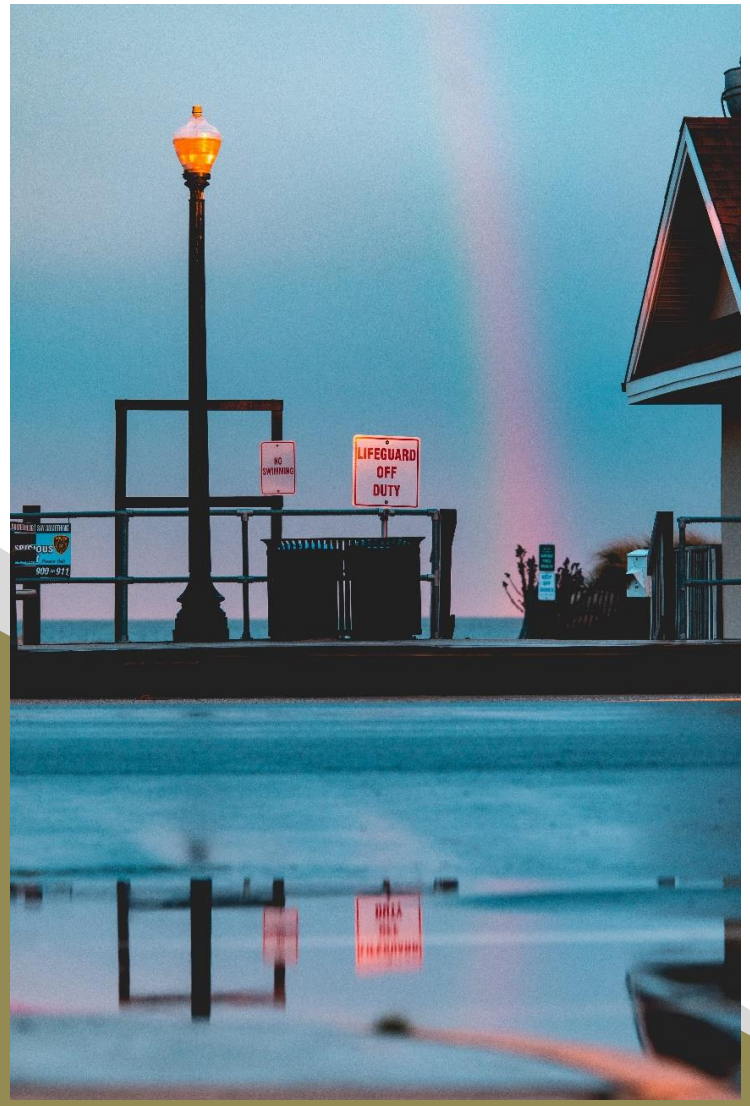
- หน่วยงานที่ผู้ควบคุมข้อมูลว่าจ้างให้ประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือของบุคคลใดๆ ตามคำสั่งของผู้ควบคุมข้อมูล

+ บังคับเฉพาะกับหน่วยงานในประเทศไทยใช่หรือไม่

- พรบ. นี้ใช้บังคับกับ Data Controller หรือ Data Processor ตั้งอยู่นอกประเทศไทย แต่เสนอสินค้า หรือบริการให้กับคนที่อยู่ในไทย หรือเฝ้าติดตามพฤติกรรม (monitor) ของคนที่อยู่ในไทย

Photo by Ryoji Iwata on Unsplash

คุ้มครองอะไรบ้าง



หลักการสำคัญ

+ การเก็บ รวบรวม ประมวลผลข้อมูลจะต้อง

- เป็นธรรม
- โปร่งใส
- เป็นไปตามวัตถุประสงค์ของหน่วยงานนั้น
- ดำเนินการตามเท่าที่จำเป็น

Photo by Ryan Loughlin on Unsplash

ฐานการประมวลผลที่ชอบธรรม (Lawfulness of processing) – มาตรา 24

ฐานการประมวลผลที่ชอบธรรมในการเก็บ รวบรวม ใช้ ประมวลผล และเปิดเผยข้อมูลส่วนบุคคล

1. ได้รับความ**ยินยอม**จากเจ้าของข้อมูล **(Consent)**
2. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ **(Scientific or research)**
3. เพื่อ**ป้องกันหรือระงับอันตราย**ต่อชีวิต **(Vital Interest)**
4. มีความ**จำเป็นเพื่อปฏิบัติตามสัญญา**ระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล **(Necessary for the performance of contracts)**
5. มีความจำเป็นเพื่อดำเนินการเพื่อ**ประโยชน์สาธารณะ**ของผู้ควบคุมข้อมูล หรือปฏิบัติหน้าที่ในการ**ใช้อำนาจรัฐที่ได้รับมอบหมาย**แก่ผู้คุ้มครองข้อมูลส่วนบุคคล **(Public Task)**
6. มีความจำเป็นในการดำเนินการเพื่อ**ผลประโยชน์อันชอบด้วยกฎหมาย**ของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล **(Legitimate Interest)**
7. เป็นการ**ปฏิบัติตามกฎหมาย**ของผู้คุ้มครองข้อมูลส่วนบุคคล **(Legal Obligation)**

3. Lawful basis for processing of personal data

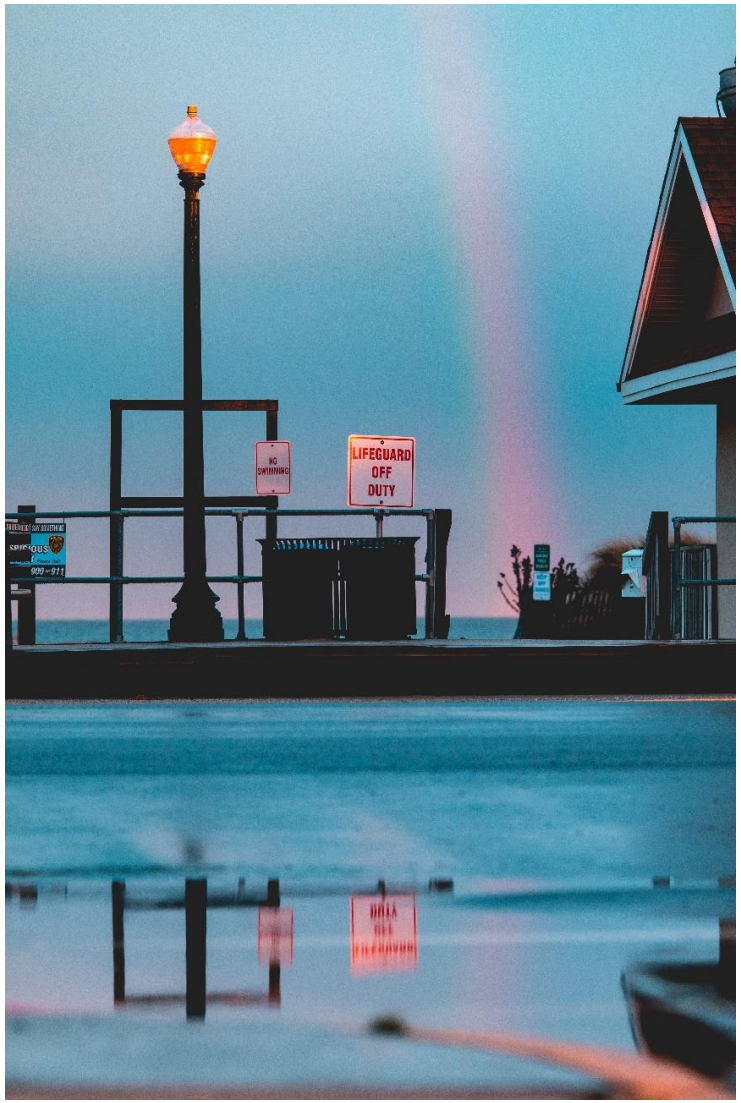
Basis	Consent	Vital interest	Scientific & Research	Necessary for performance of contract	Public task	Legitimate Interest	Legal compliance	Legitimate activities	Est. legal claim
Personal Data	✓	✓	✓	✓	✓	✓	✓		
Sensitive Personal data	✓	✓	✓		✓		✓	✓	✓
Remarks	Opt-in and must be unambiguous		For sensitivre personal data: only with legal power		For sensitivre personal data: only with legal power		For sensitivre personal data: only for certain sectors/activities		

+ หลักการให้ความยินยอม (Consent)

- ขอความยินยอมจากเจ้าของข้อมูล**<u>ในกรณีที่ไม่มีฐานกฎหมายอื่น (Legal basis)</u>** ในการเก็บ/รวบรวม/ใช้/ประมวลผลข้อมูลของเจ้าของข้อมูล
- การขอการยินยอมจะต้องแจ้งเจ้าของข้อมูลอย่างชัดเจน (informed) วัตถุประสงค์ของการขอข้อมูลต้องไม่คลุมเครือ (Unambiguous) และใช้ภาษาที่เข้าใจง่าย
- ให้อิสระแก่เจ้าของของมูลในการเลือกว่าจะให้การยินยอมหรือไม่ (Freely Given) และต้องเปิดโอกาสให้มีการถอนความยินยอมได้โดยง่าย

Photo by Fabian Gieske on Unsplash

4. Cross-border transfer of personal data



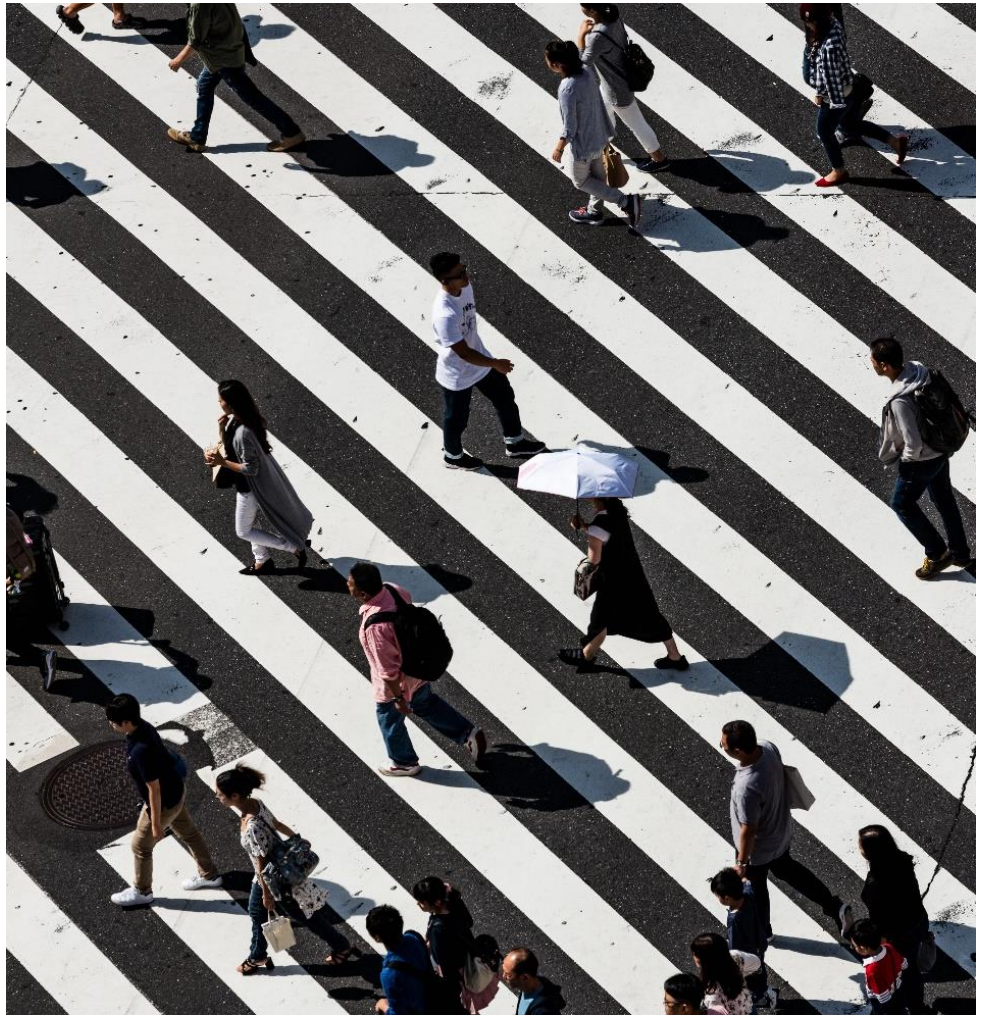
Cross-border transfer of personal data

Principle: Adequacy protection of a destination country required except falling in one or any of the following specific basis:

1. Consent
2. Vital interests
3. Necessary for the performance of contract
4. Public interests
5. Contracts
6. Legal obligations
7. Binding corporate rules (BCR) – for affiliate or intra-group companies

Photo by Ryan Loughlin on Unsplash

5. The rights of data subjects



- The right to request access to their personal data

- The right to request their personal data to be erased, destroyed, or become unidentifiable
- The right to object the collection, use, disclose of personal data
- The right of data portability (subject to further guideline)

Certain conditions apply and can be refused by controllers with reasons.

Photo by Ryoji Iwata on Unsplash

6. General duties of data controller and data processor

Data Controller

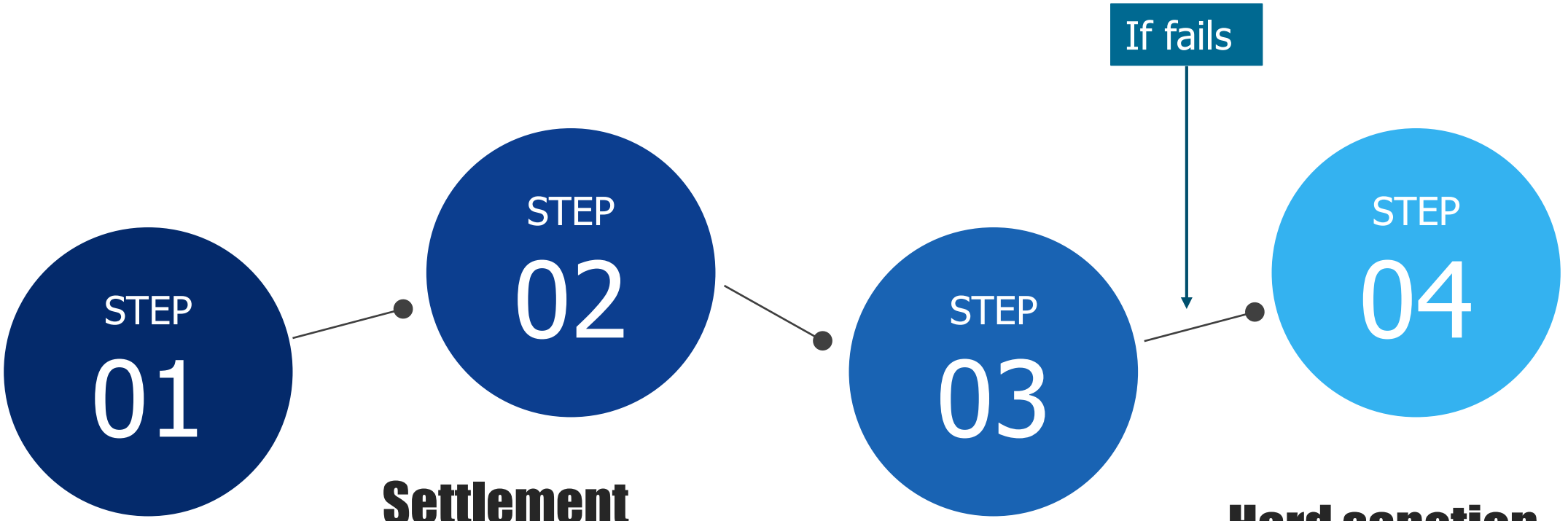
- Keep data up to date
- Provide appropriate security measures
- Notify data breach to PDPC
- Ensure transparency and keep records

Data processor

- Act as instructed by data controller
- Provide appropriate security measures
- Notify data breach to controller
- Ensure transparency and keep records

Data protection officer (DPO) to be appointed for gov. bodies and firms with large-scale data processing (guidelines to be issued).

7. Complaints and sanctions



Complaints

With in-built complaint handling unit, expert groups will review complains.

Settlement process

Parties are encouraged to settle disputes amicably.

Soft-enforcement

Non-compliant party will be ordered to rectify actions, or cease actions.

Hard sanction

Statutory fines will be imposed failing settlement.

Sanctions

Thailand's PDPA:
- Statutory sanctions (up to 5 million THB fine)
- Allow parties to seek recourse under criminal or civil liability

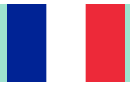
EU's GDPR		for severe violations up to € Million 20 or 4% of annual global turnover, whichever is higher
Singapore's PDPA		up to 1 million SG dollars ≈ 22 million THB
Thailand's PDPA		up to 5 million THB
Malaysia's PDPA		up to 500,000 RM ≈ 4 million THB

Sanctions

Featured cases of **GDPR Fines** by Data Protection Agencies in EU

British Airways fined by ICO  € Million 204

Basis: inadequate security measures to prevent large scale of user data's harvesting 07/2019

Google fined by CNIL  € Million 50

Basis: Forced consent and lack of transparency 01/2019

Hospital in Portugal fined by CBPD  € Million 0.4

Basis: deficient patient profile management/ access of patient's data to unsolicited personnel 07/2018

Skellefteå School fined by Swedish DPA  € 18,630

Basis: disproportioned facial recognition technology used toward school attendance 08/2019

Source: EU Commission 2019

Sanctions

Featured cases of fines in other countries

Facebook fined by FTC  $ Billion 5

Basis: "Cambridge Analytica Incident" – sharing user's data to a third party without affirmative consent 03/2018

Google fined by FTC  $ Million 170

Basis: mining children's data for targeted advertising without parent's consent 09/2019

Penalty under e-Privacy Directive (2002)

Facebook fined by ICO  £500,000

Basis: "Cambridge Analytica Incident" –
sharing user's data to a third party without affirmative consent 03/2018

Prospects for Thailand

Increased confidence between users, businesses, and public bodies.

Facilitating cross-border data transfer to benefit economy.

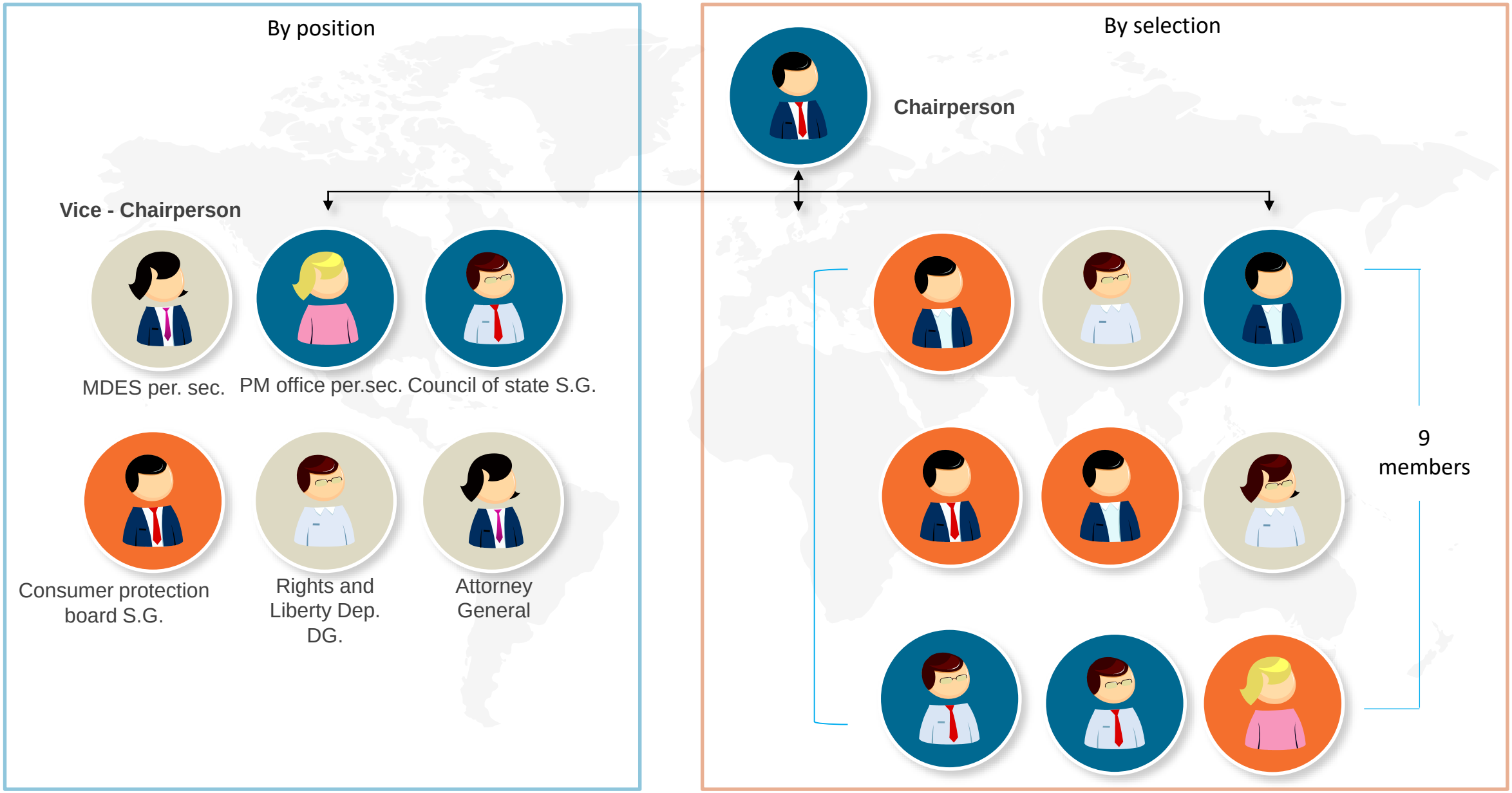
Attracting investment from increased data trust.

Enhancing data businesses and data analytics.

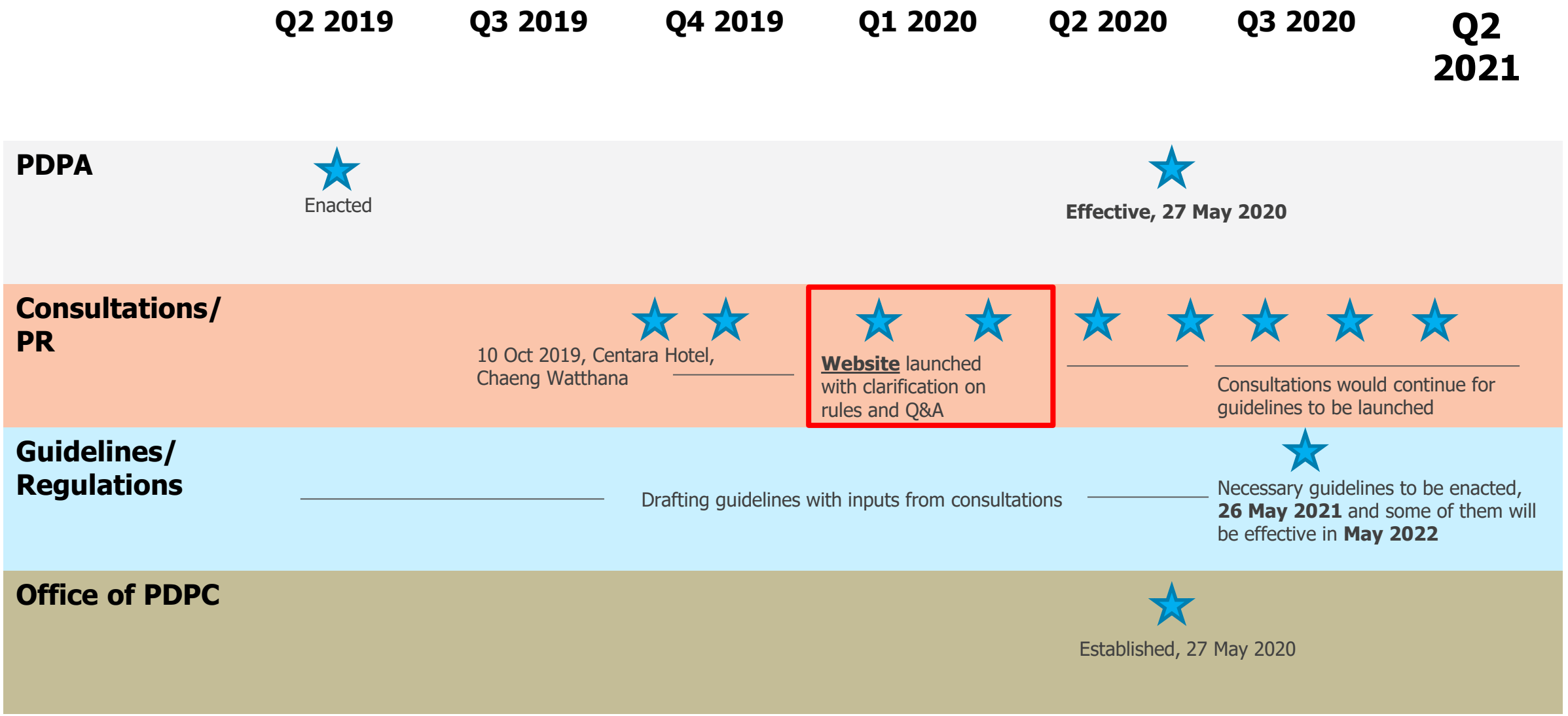
Moving toward becoming a data innovation hub in the region.

8. Composition of the personal data protection committee

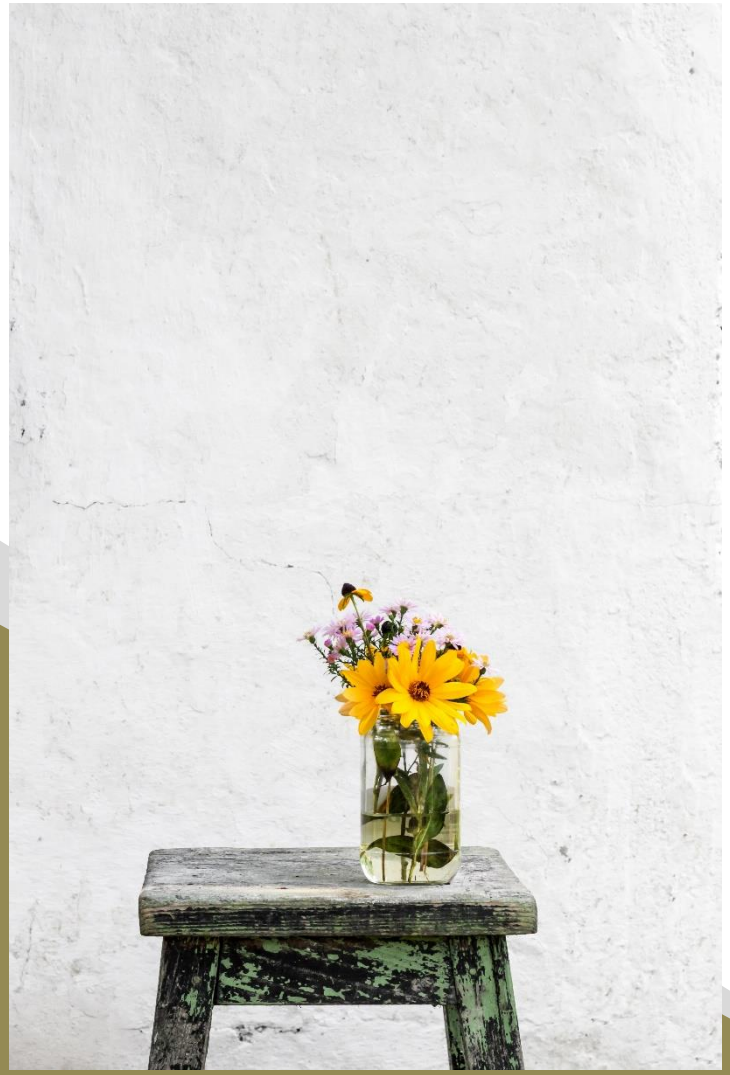
Selection progress: Ongoing



9. Essential timeline



Thank you



Prapanpong Khumon

Advisor to Secretary-General, Personal Data Protection Commission, Thailand

Website of PDPC Thailand (interim):
https://sites.google.com/view/pdpa-2019/pdpa-home

Contact:
pdpc@mdes.go.th

Photo by NordWood Themes on Unsplash