



# How to comply with Personal Data Protection ACT

By Paskorn Khotchapunsoontorn  
nForce Secure

# Agenda



สถานการณ์ปัจจุบันกับการบังคับใช้ทั่วโลก GDPR, PDPA



ภูมิภาคเอเชียกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล



7 ข้อที่ควรรู้เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



เราจะต้องทำอะไรบ้าง

สถานการณ์ปัจจุบันกับการบังคับใช้  
ทั่วโลก GDPR, PDPA

# All Data Breaches in 2019

At least 70 cases and 7.9 billion records including credit card numbers, home addresses, phone numbers and other highly sensitive information

- 2.4 Million – Wyze, December 30, 2019 (Smart camera provider)
- 267 Million – Facebook, December 19, 2019
- 15 Million – Lifelabs, December 17, 2019 (Medical Testing) largest breach in Canada
- 1 Million – T-Mobile, November 22, 2019
- 3 Million – UniCredit, October 28, 2019
- 20 Million – Novaestrat, September 16, 2019
- 14 Million – Hostinger, August 25, 2019
- 50 Million – Poshmark, August 1, 2019
- 100 Million – Capital One, July 29, 2019

<https://selfkey.org/data-breaches-in-2019/>



# Why Privacy and Personal Data Protection Matters

Some of the Reported Data/Privacy Breaches in 2018

April 15, 2018 By Pierluigi Paganini

## Commonwealth Bank customers' medical data exposed in potential privacy breach

Jakes, ABC Investigations  
3 Dec 2018, 8:40am

Commonwealth Bank is urgently gating a potential data breach that may have given its staff access to customers' medical information.

The breach was discovered around late July as the bank made preparations for the \$3.8 billion sale of its insurance arm, CommInsure, to the AIA group.

The information supplied by an unknown number of customers to CommInsure was made available to other arms of the bank, including to help it decide whether to approve or decline applications.

The bank said since the discovery of the potential



PHOTO: The CBA says it has no information about a potential data breach. (ABC News: Marga

## British Airways website suffers data breach; 380,000 payments affected

BRITISH AIRWAYS WEBSITE SUFFERS DATA BREACH; 380,000 PAYMENTS AFFECTED

2018-09-06 NEWSBOT BRITISH, CUSTOMERS, DATA, NEWS

TrueMove H, the biggest 4G mobile operator in Thailand suffered a data leak, 46000 people's data stored on an AWS bucket were left on accessible online, including driving licenses and passports.

Let's speak about a new data breach, this time the victim is TrueMove H, the biggest 4G mobile operator in Thailand.

The operator exposed online customers personal data that were stored in an Amazon AWS S3 bucket.

## Under Armour says data breach affected about 150 million MyFitnessPal accounts

- The breach affected an estimated 150 million users of its food and nutrition application, MyFitnessPal.
- The investigation indicates that affected information may include usernames, email addresses, and hashed passwords.

Chloe Aiello | @chlobo\_ilo  
Published 4:38 PM ET Thu, 29 March 2018 | Updated 8:20 PM ET Thu, 29 March 2018  
CNBC



MyFitnessPal app, website hit by data breach

8:19 PM ET Thu, 29 March 2018 | 00:45

OCT 22 MORE ON MEDICARE & MEDICAID

## CMS responds to data breach affecting 75,000 in federal ACA portal

Open enrollment, which begins November 1, will not be negatively impacted, CMS says.

Susan Morse, Senior Editor



## HALF BILLION Customers Data Stolen!



## SINGHEALTH PATIENTS' DATA STOLEN

**WHO'S AFFECTED:**  
1.5 MILLION PATIENTS WHO VISITED THESE SPECIALIST OUTPATIENT CLINICS AND POLYCLINICS BETWEEN MAY 1, 2015 AND JUL 4, 2018, INCLUDING PM LEE HSIEN LOONG

- |  |  |
|--|--|
| POLYCLINICS:<br>BEDOK<br>BUKIT MERAH<br>GEVLANG<br>MARINE PARADE<br>OUTRAM<br>PASIR RIS<br>PUNGGOL<br>SENGKANG<br>TAMPINES<br>QUEENSTOWN | SINGAPORE GENERAL HOSPITAL<br>CHANGI GENERAL HOSPITAL<br>SENGKANG GENERAL HOSPITAL<br>KK WOMEN'S AND CHILDREN'S HOSPITAL<br>NATIONAL CANCER CENTRE<br>NATIONAL HEART CENTRE<br>SINGAPORE NATIONAL EYE CENTRE<br>BRIGHT VISION HOSPITAL |
|--|--|

GEVLANG AND QUEENSTOWN POLYCLINICS ARE NO LONGER UNDER SINGHEALTH

## Cathay Pacific Suffers World's Largest Airline Data Breach

October 29, 2018







# Why Privacy and Personal Data Protection Matters

Some of the Reported Data/Privacy Breaches in 2018

Marriott to be fined nearly £10m for GDPR breach

ICO imposes fine after personal data stolen by hackers



3,500

BA faces £18m fine for data breach

ICO says personal data on website and mobile app



6,300

Equifax to pay \$700m to settle lawsuit over exposed data of 143 million

- Credit agency exposed social security numbers
- Settlement to provide up to \$400,000 per person



21,530

Facebook to pay \$5bn fine as regulator settles Cambridge Analytica complaint

Penalty by US government reflects scale of breach, first reported by the Observer

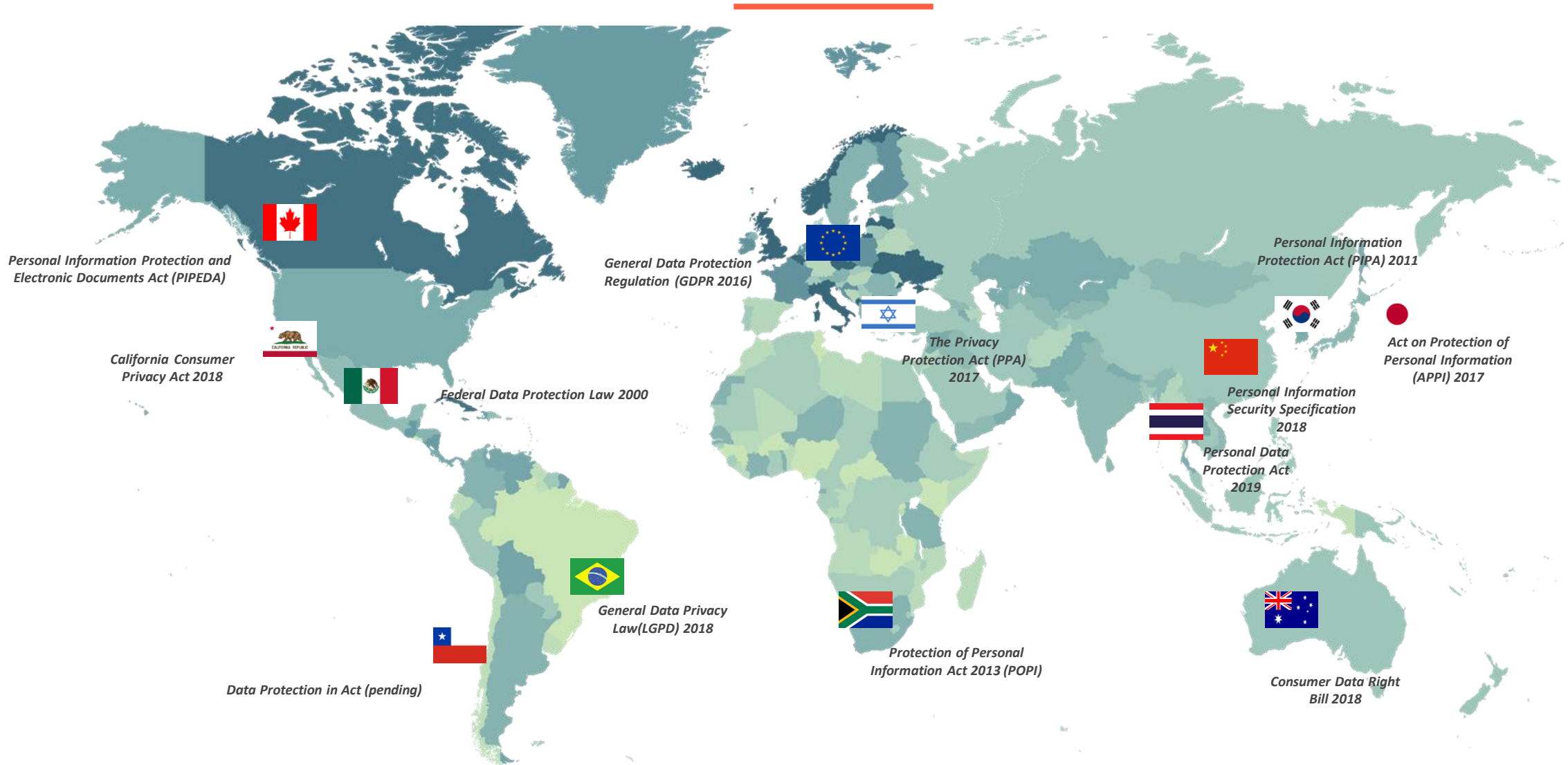


153,800 ล้านบาท

**ภูมิภาคเอเชียกับ พ.ร.บ.คุ้มครอง  
ข้อมูลส่วนบุคคล**



# Privacy Laws Coming Into Effect Across the Globe







# Privacy Laws Coming Into Effect Across APAC

*Personal Information Security Specification 2018*



*Law on Cybersecurity 2018*



*Personal Data Protection Bill 2018*



*Personal Data Protection Act 2019*



*Personal Data Protection Act 2010*



*Personal Data Protection Act (PDPA) 2012*



*Personal Data Protection Law (draft)*



*Personal Information Protection Act (PIPA) 2011*



*Act on Protection of Personal Information (APPI) 2017*



*Personal Information Protection Act 2015*



*Personal Data (Privacy) Ordinance 2018*



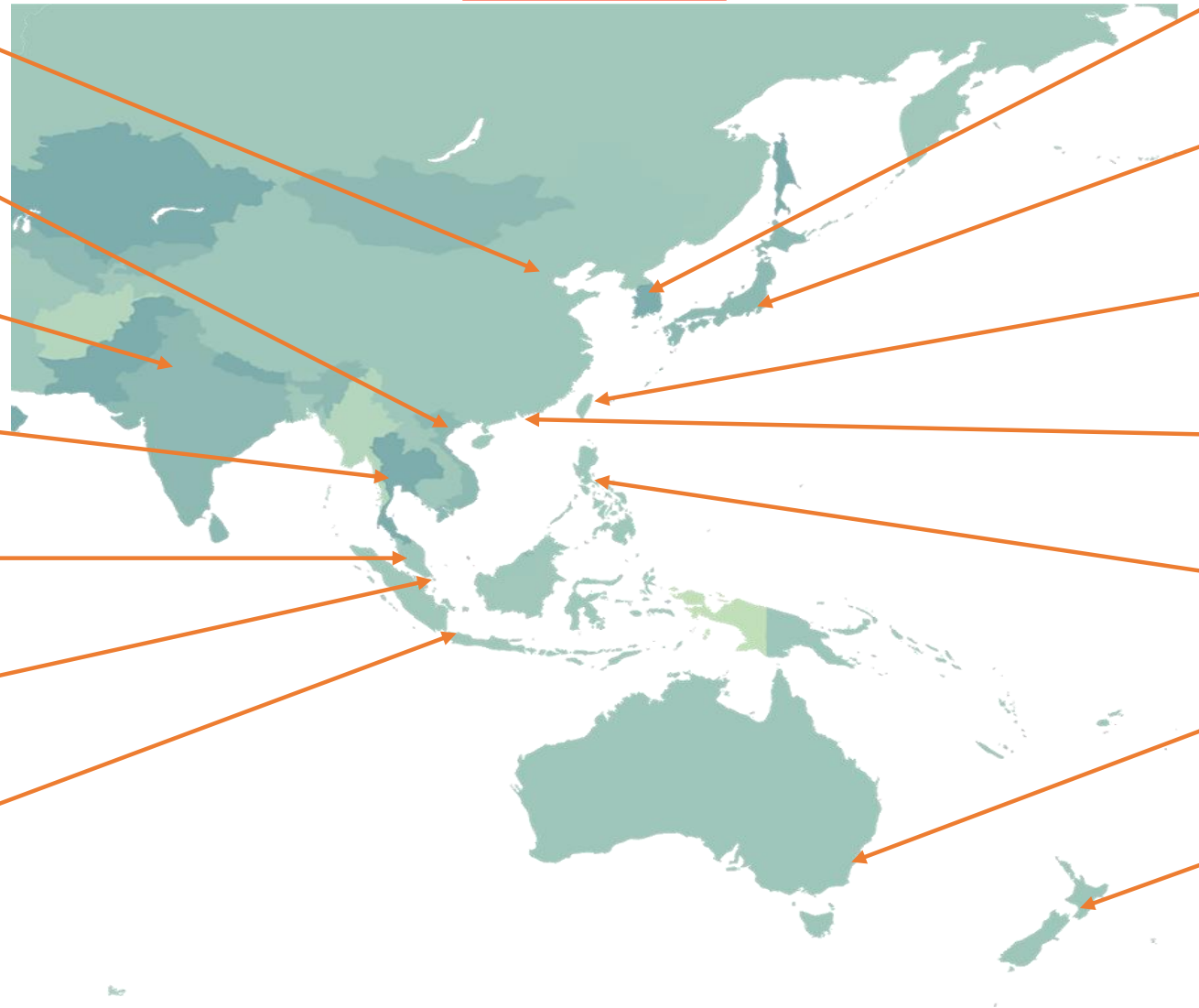
*Data Privacy Act 2012*



*Consumer Data Right Bill 2018*




*Privacy Act 1993*



7 ข้อที่ควรรู้เกี่ยวกับ พ.ร.บ

<https://www.bakermckenzie.com/>

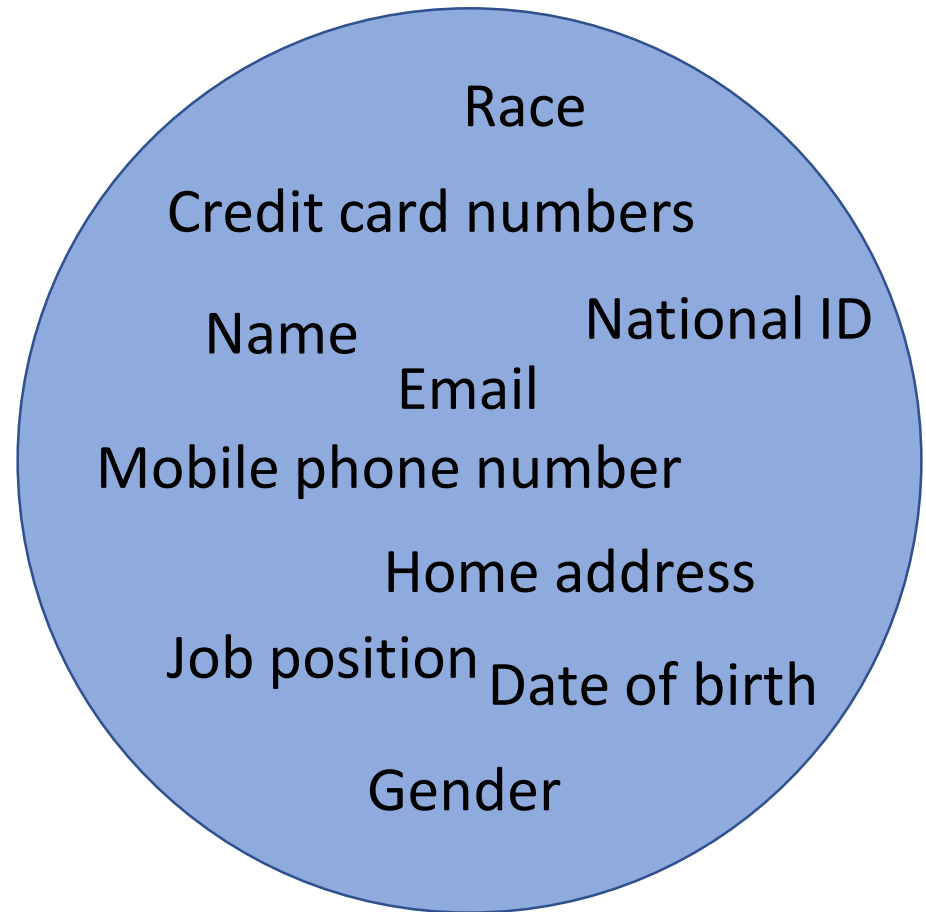


# 1. Personal Data (ข้อมูลส่วนบุคคล)

- ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม
-

# But What is Personal Data?

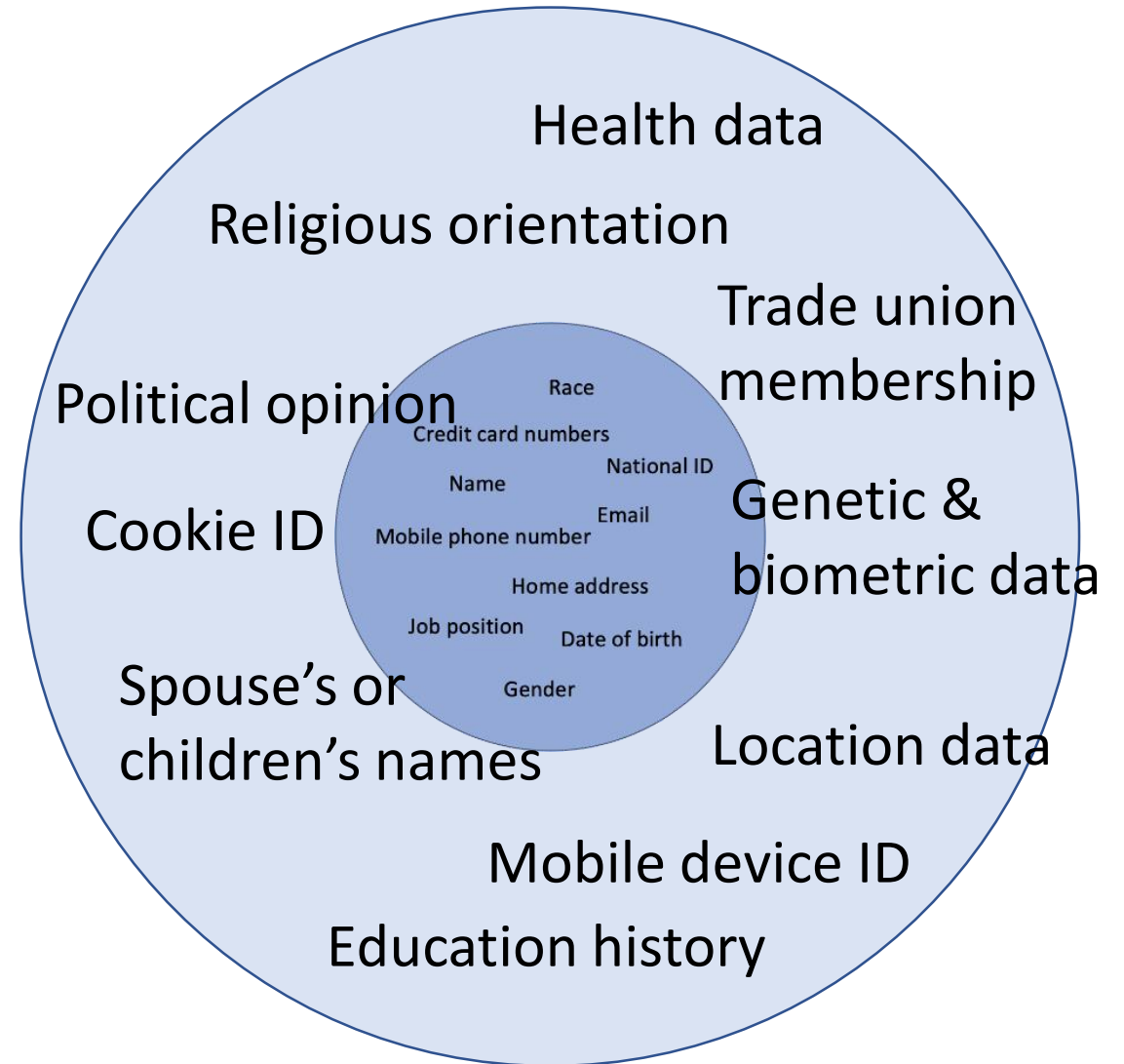
- First, there was ***Personally Identifiable Information (PII)*** – NIST definition:
  - PII is any information about an individual maintained by an agency, including (1) any information that ***can be used to distinguish or trace an individual's identity***, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is ***linked or linkable to an individual***, such as medical, educational, financial, and employment information.





# But What is Personal Data?

- Now, we have **Personal Data**, or **Personal Information (PI)** – GDPR definition:
  - **any information relating to an identified or identifiable natural person ('data subject')**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;





## 2. Players

- Data Subject (เจ้าของข้อมูลส่วนบุคคล)
  - Data Controller (ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล)
  - Data Processor (ผู้ประมวลผลข้อมูล ทำตามคำสั่ง ผู้ควบคุมข้อมูลส่วนบุคคล)
  - Personal Data Protection Committee (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล)
-



# 3. Applicability

- **Territorial** บริษัทในไทย ต้องปฏิบัติตาม PDPA
  - **Extra-Territorial** บริษัทหรือ **web** ต่างประเทศ ที่ขายของให้กับคนไทย เช่น ABnB เปิดให้คนไทยจองที่พักในต่างประเทศต้องปฏิบัติตาม PDPA
-



## 4. Legal basis

- **Consent** ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนนำไปใช้ และต้องทำให้ชัดเจน (ห้าม **force**, ห้าม **pre-tick**ไว้ก่อน), เช่น **AIS** ขอ **consent** ข้อมูลมาทำวิเคราะห์ข้อมูล พุ่งนี้เอาข้อมูลมาขาย **New Service** จะต้องกลับไปขอ **consent** จากลูกค้าใหม่
- **Legal Exceptions**
  - เอาข้อมูลมาปฏิบัติตามสัญญา เช่น **e-commerce** ต้องเอาชื่อ และที่อยู่ มาส่งของให้ลูกค้า เป็นข้อมูลที่เป็นต่อการทำงาน, **subscription service** ต้องขอข้อมูลบัตรเครดิต (**Contract**)
  - เก็บข้อมูลตามที่กฎหมายสั่งให้เก็บ เช่น โรงแรม ต้องเก็บข้อมูล **passport** เพื่อรายงาน ตม.
  - **vital interest** เช่น คนไข้ สลบอยู่ ไม่สามารถตื่นมาให้ **consent** ได้





## 5. Personnel

- บุคคลที่กฎหมายบังคับให้มีในองค์กร
    - **DPO (Data Protection Officer) auditor** คอยตรวจสอบ, ประสานงานระหว่างเจ้าของข้อมูลกับ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดย **DPO** จะได้รับความคุ้มครองทางกฎหมายระดับหนึ่ง เช่น ไปรายงานต่อคณะกรรมการ บริษัทห้ามไล่ออก, กฎหมายลูกในอนาคต จะมีเกณฑ์ออกมาว่าปริมาณข้อมูลเท่าไร ต้องมี **DPO** กี่คน
    - **Representative** เชื่อมกับบริษัทเมืองนอกที่ต้องทำตามกฎหมายไทย โดยบริษัทต่างประเทศ ต้องตั้ง **representative** ด้านข้อมูลส่วนบุคคลโดยเฉพาะในไทย
-



## 6. Rights of data subjects.

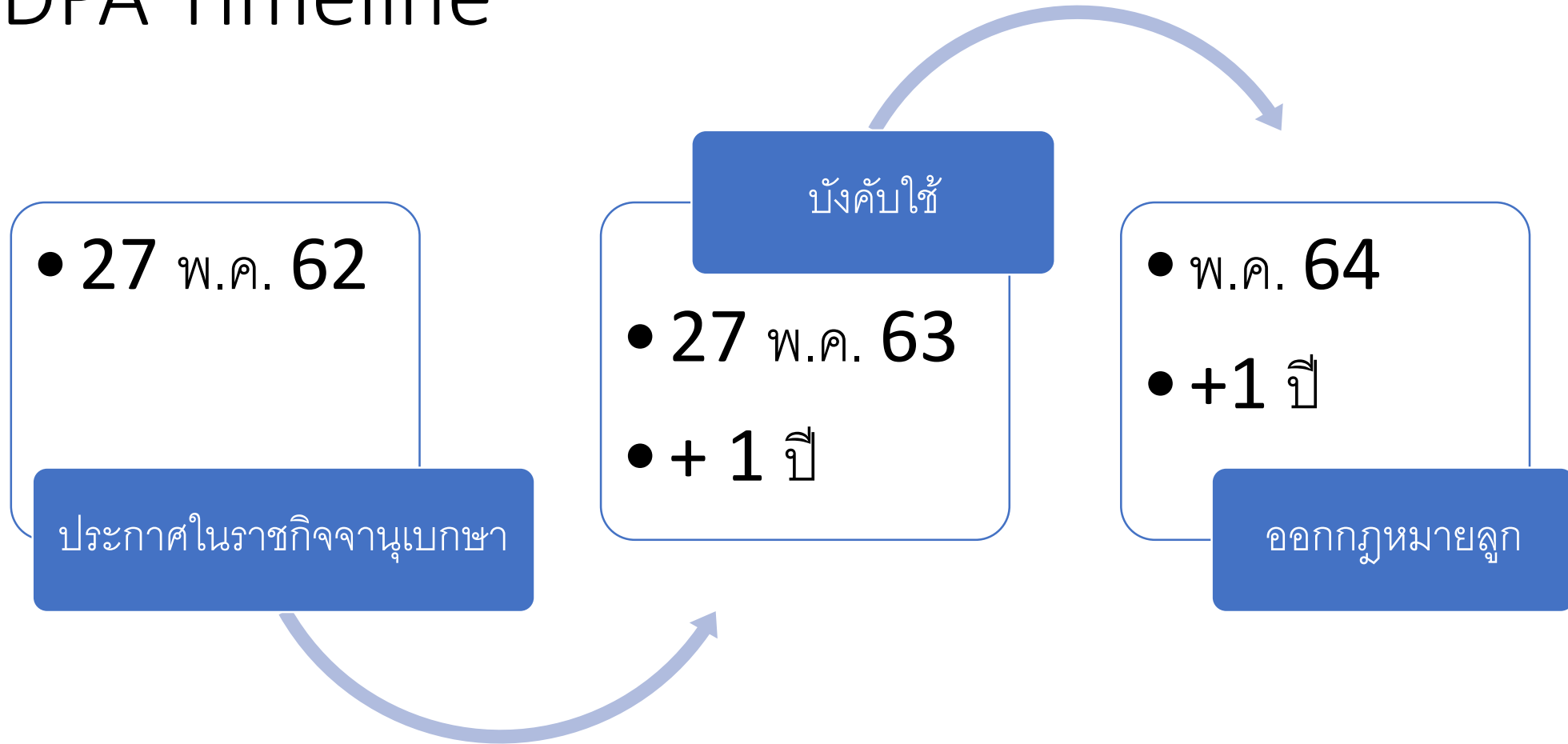
- สิทธิของเจ้าของข้อมูล ที่ผู้ควบคุมข้อมูลต้องทำตาม เช่น สิทธิที่จะได้รับแจ้ง สิทธิในการเข้าถึง สิทธิในการแก้ไข สิทธิในการลบล้าง สิทธิในการจำกัดการประมวลผลข้อมูล สิทธิในการถ่ายโอนข้อมูล สิทธิในการปฏิเสธไม่ให้ใช้ข้อมูล สิทธิที่จะไม่ใช้การตัดสินใจโดยอัตโนมัติในการประมวลผลข้อมูล
- สิทธิในการรับแจ้ง เช่น เก็บข้อมูลอะไรไปบ้าง ขอคืนหน่อย
- สิทธิในการลบ ขอให้ลบ (ต้องลบทุก BUs, ไม่ใช่แผนก A ลบ วันรุ่งขึ้น แผนก B โทรมไปขายของ → พ้องได้เลย),
- สิทธิในการโอนย้ายข้อมูล ขอให้ทำ **data portability** คือ ลูกค้าใช้ **service** ของ A อยู่ อยากจะ **switch** ไปใช้ **service** ของ B จึงขอให้ A โอนข้อมูลลูกค้าไป B ให้หน่อย ซึ่ง A ต้องทำให้ ภายใน 30 วัน ถ้าทำไม่ได้ จะต้องแจ้งเหตุผลกับลูกค้า
- \*\* ดังนั้น เจ้าของ **platform** ต้องเข้าใจ **rights of data subjects** เพื่อนำไปออกแบบระบบ \*\*

# 7. Penalties

- **แพ่ง**
  - ระบุขอบเขตของการละเมิดข้อมูล เน้นเป็นการฝ่าฝืนหรือไม่ปฏิบัติตาม บทบัญญัติ
  - กำหนดความรับผิดของ ผู้ควบคุมข้อมูลหรือ ผู้ประมวลผลข้อมูลเป็น ความรับผิดโดยเคร่งครัด (**Strict Liability**)
  - ให้อำนาจศาลสั่งให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ชดใช้ค่า สิ้นไหมทดแทนได้ไม่เกินสองเท่าของค่าสินไหม ทดแทนที่แท้จริง
  - กำหนดอายุความฟ้องคดีเป็นการเฉพาะ เมื่อพ้นสามปีนับแต่วันที่ ผู้เสียหายรู้ถึงความเสียหายและ รู้ตัวผู้ควบคุมข้อมูลหรือผู้ ประมวลผลข้อมูลที่ต้องรับผิดหรือเมื่อพ้นสิบปีนับแต่วันที่มีการ ละเมิดข้อมูลส่วนบุคคล
- อาญา **Data Subject** ไปฟ้องศาล เพื่อเรียกร้องความเสียหายจาก บริษัท
- บทลงโทษ โทษปรับทางปกครอง ไม่เกิน **5,000,000** บาท

บทลงโทษทางอาญา	ปรับ	จำคุก	ทั้งสอง
ม.79 ผู้ควบคุมข้อมูล ฝ่าฝืนหรือ ไม่ปฏิบัติตาม	<= 500,000	<=6 เดือน	ใช่ หรือ ยอมความได้
ม.80 ผู้ใดล่วงรู้ข้อมูลของบุคคลอื่นและนำไปเปิดเผย	<=1,000,000	<= 1 ปี	ใช่ หรือ ยอมความได้
ม.81 นิติบุคคล	<=500,000	<=6 เดือน	ใช่

# PDPA Timeline







# Concerns

- No toolsets or method to “forget” data
  - No clear understanding of where the data is or who owns it
  - No system to respond to huge numbers of customer/consumer/employee complaints
  - Increase focus on transparency and consent
  - How to handle data breach?
  - Engaging with data protection regulators (e.g. Committee, Expert Committee, Office)
  - Required legal documents for compliance
  - Unidentified legal basis for collection, use, or disclosure of personal data
-

เราจะต้องทำอะไรบ้าง

<https://www.bakermckenzie.com/>

# What to do next?



conduct data mapping,



determine legal basis  
and applicable  
obligations,



revisit privacy notice  
and create relevant  
legal documents,

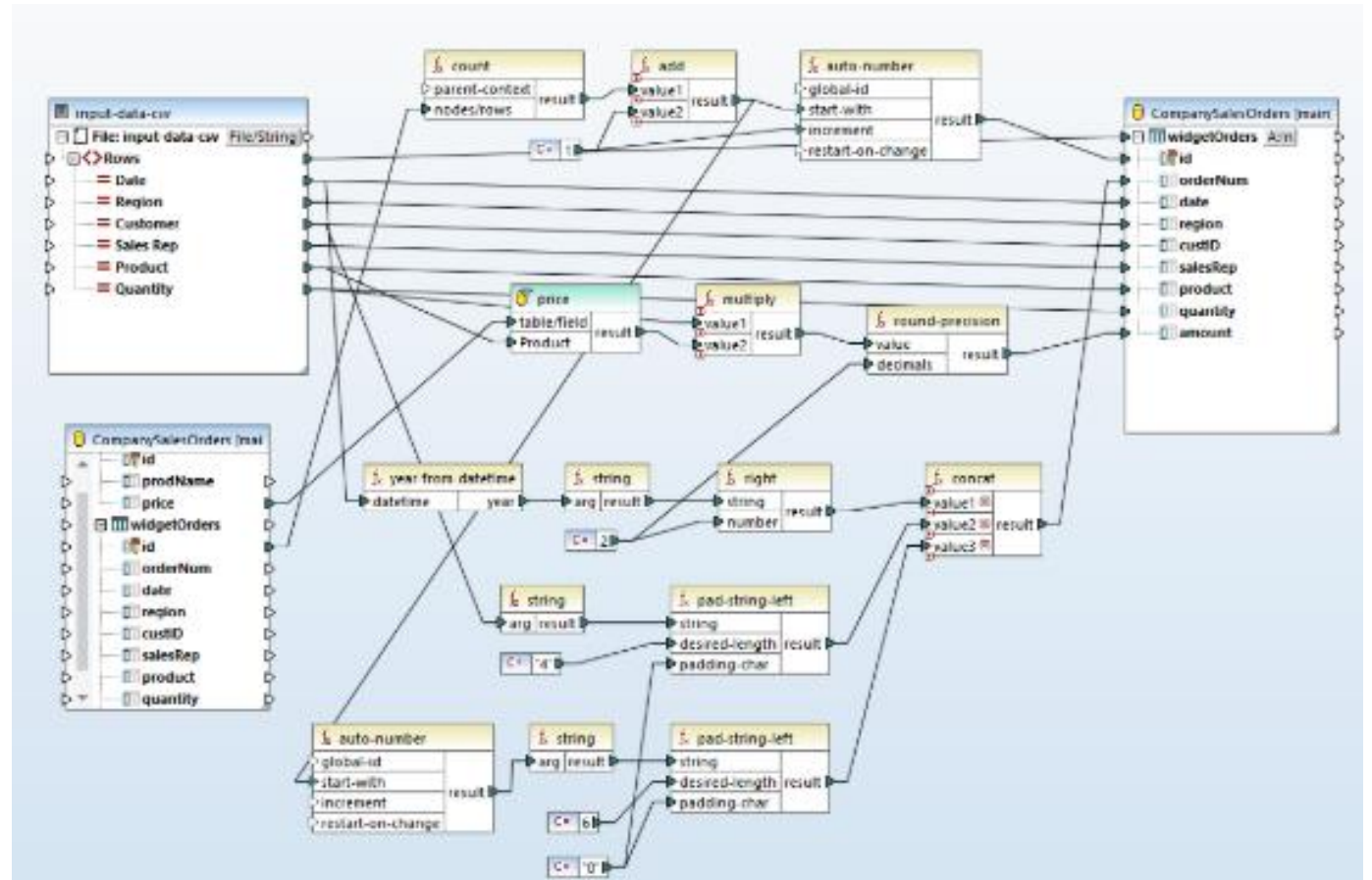


implement data  
management process  
and operation system,



maintain compliance  
with the PDPA.

# Conduct Data Mapping



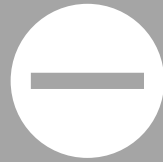
👤 5W (What, When, Where, Why, Whom)

🕒 1H (How)

determine  
legal basis  
and  
applicable  
obligations



Consent



Contractual necessity



Legal interest?

revisit privacy  
notice and  
create  
relevant legal  
documents,



Purpose of processing and legal basis



Collected personal data



Legal obligation/contract/impact



Data retention period (or expected period)



Categories of persons/entities to whom personal data may be disclosed to ?



Contact details of controller/DPO/representative



Rights to data subject

implement  
data  
management  
process and  
operation  
system,



Internal Policies



Procedure



Record Keeping

maintain  
compliance  
with the  
PDPA.

