SINGAPORE

Part 3 – Singapore

Processing grounds and mandatory data breach notification

Data portability and innovative uses of data

DPO Competency Framework and Training Roadmap

Regulatory sandbox

AI Governance Framework

Enforcement trends

Consultations on amendments (Part 1)

(a) PDPC's proposed changes to processing grounds

Notification of Purpose

Notifying individuals of the purpose can be an appropriate basis for data processing where:

- such processing is **unlikely to have any adverse impact** on the individual

Legitimate Interest

Data may be processed without consent for a legal or business purpose where:

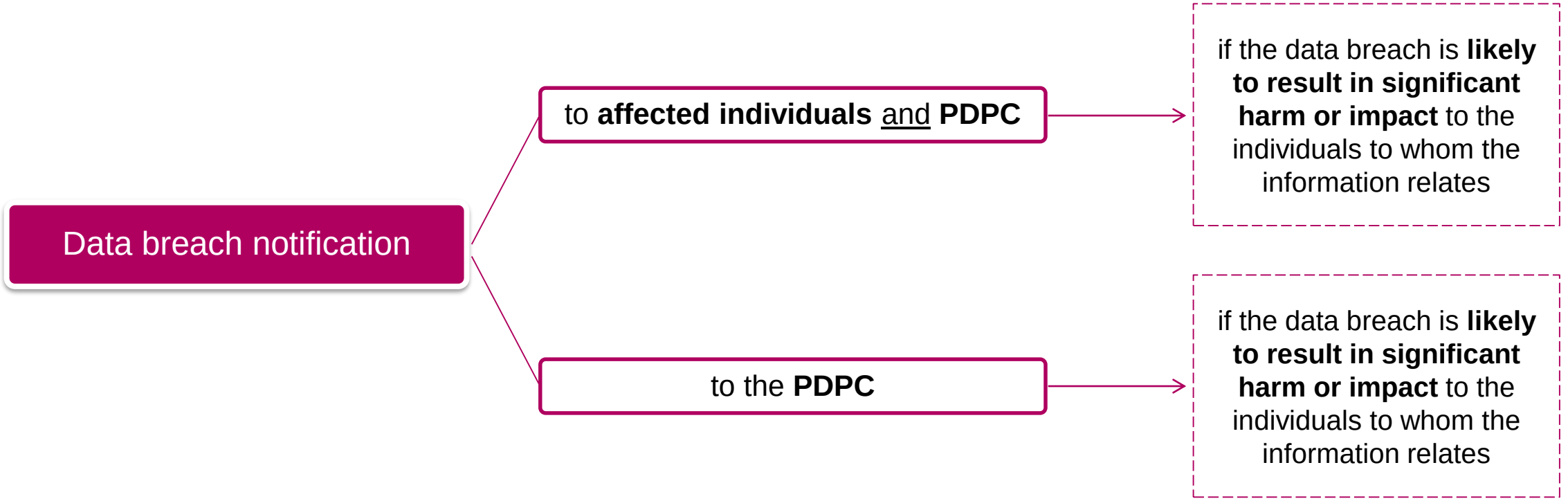
- **benefits to the public** (or a section thereof) **outweigh** any **adverse impact** to the individual

+

organisations must conduct a **risk and impact assessment** and put in place **measures to identify and mitigate the risks**

Consultations on amendments (Part 1)

(b) PDPC's proposed mandatory data breach notification regime



Time frame: **72 hours** (from time the organisation determines that the breach is eligible for reporting)

Consultations on amendments (Part 2)

Proposed data portability obligations	Proposed data innovation provisions
an organisation must, at the request of an individual, **provide the individual's data** that is in the organisation's possession or under its control, **to be transmitted to another organisation** in a commonly used machine readable format	an organisation can use personal data (collected in compliance with the PDPA) for the purpose of: (i) operational efficiency and service improvements (ii) product and service development; or (iii) knowing customers better ("**business innovation purposes**") without the requirement to notify the individuals of and seek consent to use their data for these purposes
to apply only to data in the possession or control of organisations that is held **in electronic form**	where individuals **withdraw consent**, organisation may **continue to use such data** for business innovation purposes

promote business innovation

empower individuals

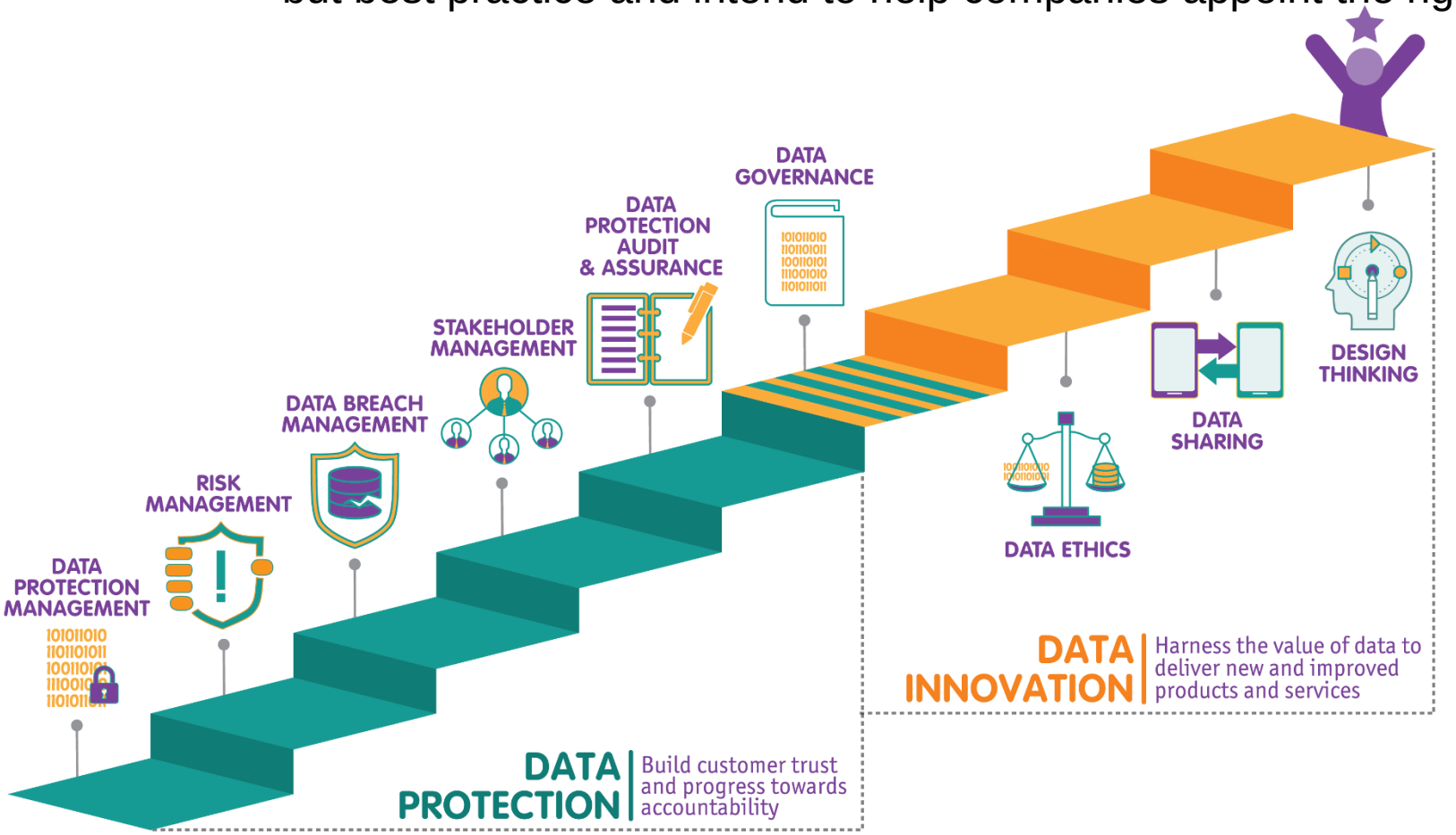
boost the flows of data

support greater data sharing

DPO Competency Framework and Training Roadmap

not mandatory

but best practice and intend to help companies appoint the right DPO



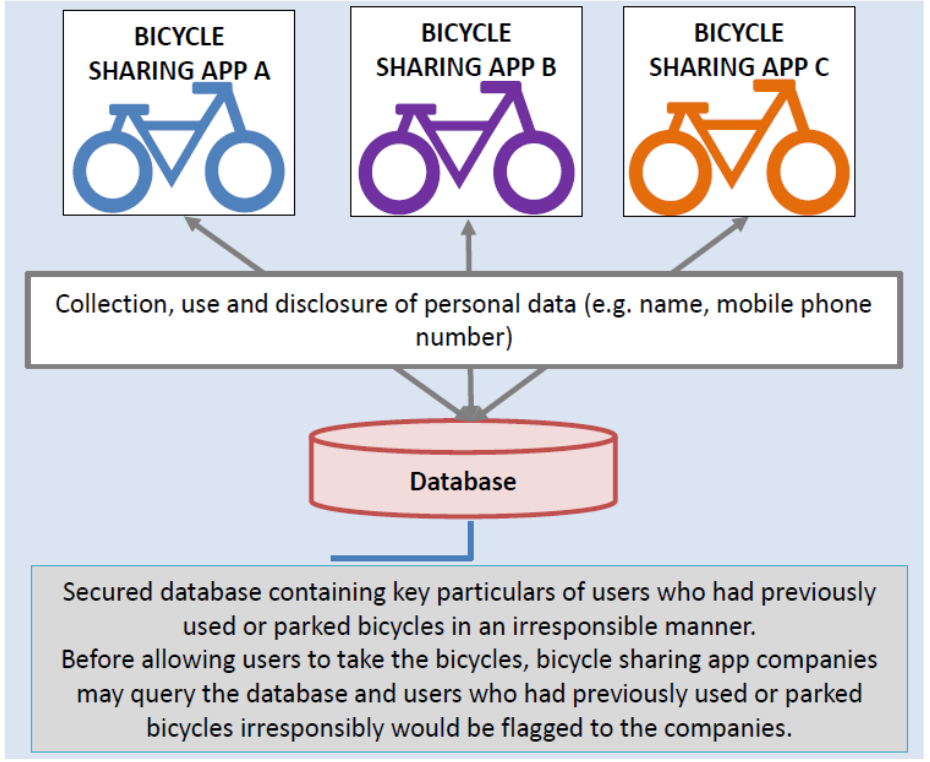
- Sets out the **competency** and **proficiency** levels **expected from DPOs**
- Identifies **courses** that would **help data professionals** achieve the various levels of proficiency

Regulatory sandbox

> **The Data Collaborative Programme**

- Aim is to encourage organisations that are exploring **innovative uses** of personal data (that is regulated under the PDPA) to offer new products or services to their customers.
- Have to fall under circumstances where sharing of data:
  a) is not likely to have adverse impact on individuals, or
  b) where there is need to protect legitimate interests and benefits for the public outweigh adverse impact to individuals.

Example

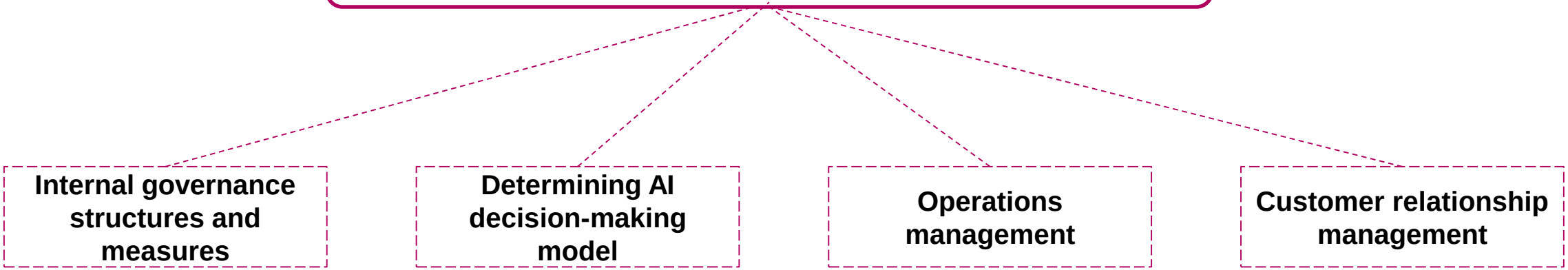


Source: Infocomm Media Development Authority

AI governance framework

In 2019 PDPC released the first edition of a **Model AI Governance Framework** for consultation.

The **Model AI Governance Framework** maps out key ethical principles and practices that apply to common AI deployment processes in **four areas**.



Enforcement trends

- **Over S$1.29 million** in fines issues so far this year
- 30 enforcement cases **in 2018**
- 36 enforcement cases **in 2019** (so far)

- **2019**
  - Fines: 22
  - Warnings/Directions only: 11
  - Found not to be in breach: 3
  - The majority of enforcement cases (21) were due to organisations **failing to put in place reasonable security arrangements** to protect the personal data of its customers from unauthorised disclosure

Fines issued by personal data watchdog

Annually

Year	Amount
2019*	$1,295,000
2018	$177,500
2017	$93,000
2016	$123,500

NOTE: *Till mid-Sept

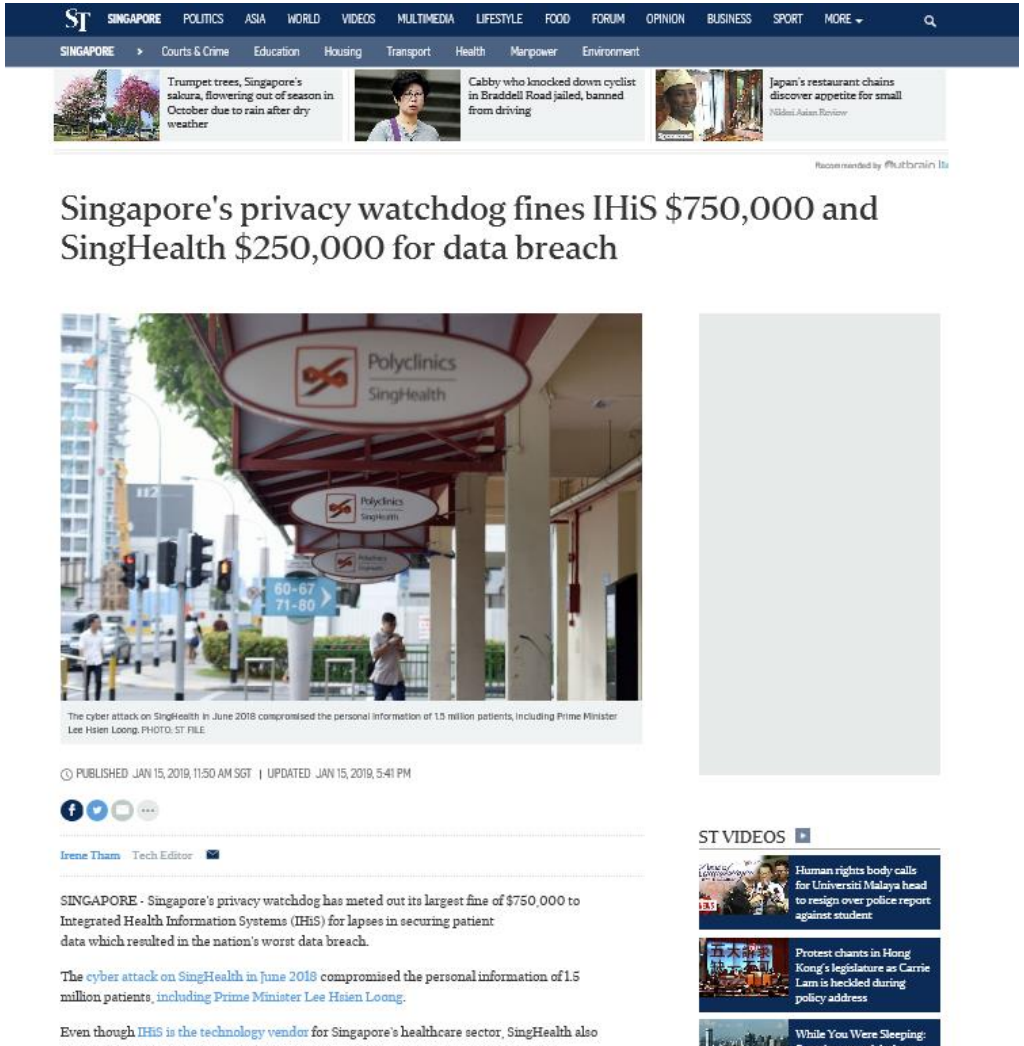
The highest five

	Company	Year	Amount
1	Integrated Health Information Systems	2019	$750,000
2	SingHealth	2019	$250,000
3	Horizon Fast Ferry	2019	$54,000
4	K Box Entertainment Group	2016	$50,000
5	DS Human Resource	2019	$33,000

Source: Personal Data Protection Commission website SUNDAY TIMES GRAPHICS

2019 Fines	
S$1,000 - 5,000	6
S$6,000 - 10,000	4
S$11,000 - 20,000	6
S$21,000 - 70,000	5
>S$70,000	1

Enforcement trends



ST SINGAPORE POLITICS ASIA WORLD VIDEOS MULTIMEDIA LIFESTYLE FOOD FORUM OPINION BUSINESS SPORT MORE

SINGAPORE > Courts & Crime Education Housing Transport Health Manpower Environment

Trumpet trees, Singapore's sakura, flowering out of season in October due to rain after dry weather

Cabby who knocked down cyclist in Braddell Road jailed, banned from driving

Japan's restaurant chains discover appetite for small

Nikkei Asian Review

Recommended by outbrain

Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach

The cyber attack on SingHealth in June 2018 compromised the personal information of 1.5 million patients, including Prime Minister Lee Hsien Loong. PHOTO: ST FILE

PUBLISHED JAN 15, 2019, 11:50 AM SGT | UPDATED JAN 15, 2019, 5:41 PM

Irene Tham Tech Editor

SINGAPORE - Singapore's privacy watchdog has meted out its largest fine of $750,000 to Integrated Health Information Systems (IHiS) for lapses in securing patient data which resulted in the nation's worst data breach.

The cyber attack on SingHealth in June 2018 compromised the personal information of 1.5 million patients, including Prime Minister Lee Hsien Loong.

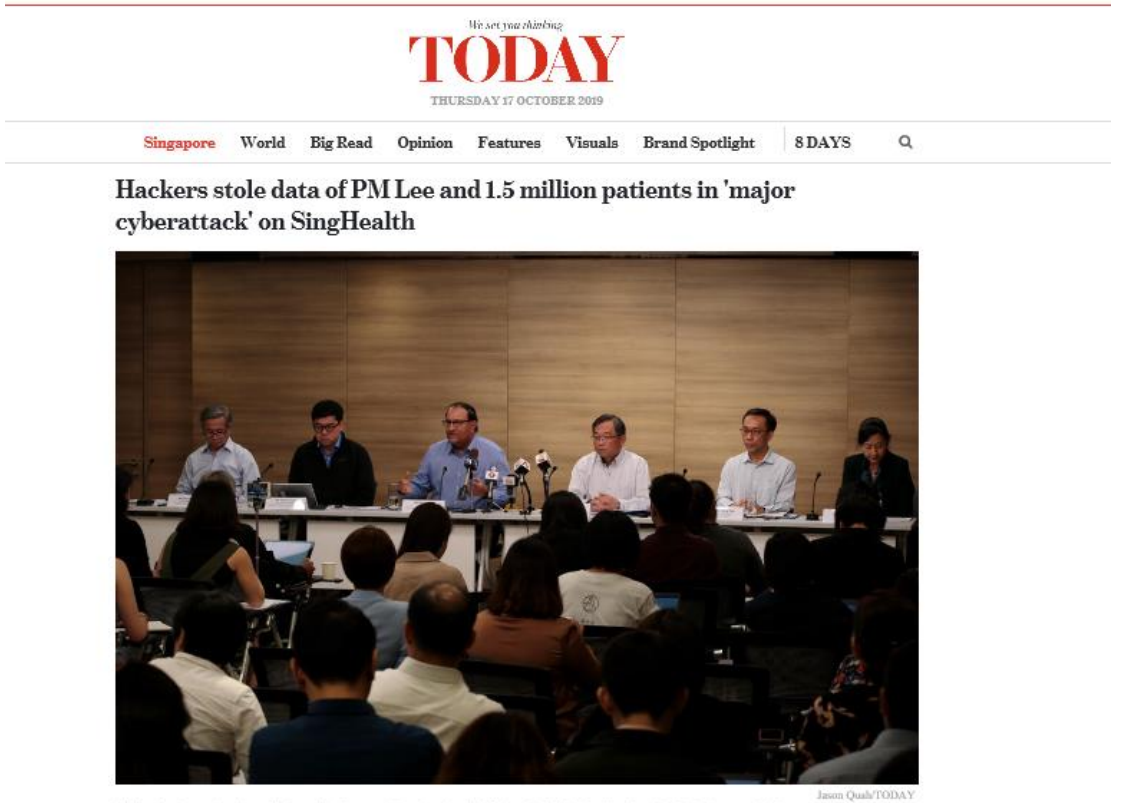
Even though IHiS is the technology vendor for Singapore's healthcare sector, SingHealth also

ST VIDEOS

Human rights body calls for Universiti Malaya head to resign over police report against student

Protest chants in Hong Kong's legislature as Carrie Lam is heckled during policy address

While You Were Sleeping:



We set you thinking

TODAY

THURSDAY 17 OCTOBER 2019

Singapore World Big Read Opinion Features Visuals Brand Spotlight 8 DAYS

Hackers stole data of PM Lee and 1.5 million patients in 'major cyberattack' on SingHealth

Jason Quah/TODAY

Minister for Communications and Information S Iswaran (C) speaks alongside Minister for Health Gan Kim Yong (3rd R) during a press briefing on a 'major cyber attack' on SingHealth, July 20, 2018.

Published 20 JULY, 2018 UPDATED 17 SEPTEMBER, 2019

2134 Shares

SINGAPORE — In the biggest and most serious cyberattack yet on Singapore, hackers last month broke into SingHealth's IT systems to steal the data of 1.5 million patients and records of the outpatient medication given to Prime Minister Lee Hsien Loong, the authorities said on Friday (July 20).

[ADPL Ch 10 ‘Singapore – Uncertain scope, strong powers’]

Singapore

- 2019 Update pp. 21-22.
- *Context:* Stable, somewhat authoritarian, and prosperous quasi-democracy; high standard rule of law
- APEC and ASEAN member; not OECD; APEC-CBPRs; CPTPP party
- Minimal protections in the general law
  - No constitutional or treaty-based privacy protections
  - No significant tort protections (harassment legislation)
  - Some sectoral privacy protections (eg banking law)
- *Personal Data Protection Act* (PDPA) 2012
  - Data privacy aspects in force July 2014
  - Almost all privacy protection in Singapore depends on this Act
  - Personal Data Protection Commission (PDPC) is not independent – a branch of a government department

Singapore
PDPA Scope & exemptions

- Public sector excluded, but boundaries uncertain
  - Also companies acting for government (but no disclosure)
  - Public sector has a privacy code, but content unknown, and unenforceable
- Private sector scope covered is uncertain
  - Both regulations and PDPC can exclude any private sector bodies, or any types of activities, from scope of PDPA (has not occured)
  - Any other law (legislation or other) also overrides PDPA (Many other Singaporean laws have some effect on privacy and confidentiality: at least 161)
  - Lengthy lists of specific exemptions in PDPA (p296)
  - 'Personal data' excludes any publicly available data
  - Some limited exemptions in favour of media
- Result: Scope of PDPA is a 'known unknown'

Singapore - PDPA Principles

- Principles appear to cover all OECD basics
  - Additions: necessary collection; deletion/de-ID; data exports
  - Omissions: ‘sensitive data’, MDB; direct marketing opt-out
- Collection, use & disclosure appear to be based on notice & consent, but are really ‘exception based’
- 4 factors make exceptions dominate (p298):
  i. Deemed consent by voluntary provision of data, wherever this is reasonable.
  ii. If deemed consent, no notice required.
  iii. Neither consent nor notice wherever lengthy 2nd-4th Schedules of exemptions apply
  iv. Any other law can override need for notice or consent

Result: Look at exceptions first, then if out of luck …

Singapore – Proposed 'Reforms'

- 2019 update p. 20; 2018 Update pp. 13-14; See Greenleaf Chapter in Chesterman (2018) for details
- Anonymisation standard – Appears more permissive than EU – 'regulatory sandbox' for Big Data?
- Consent – Proposed further weakening by deeming; will destroy most limits on use & disclosure (2018 chapter, [14.29])
- Mandatory data breach notification (DBN) proposed and likely to be enacted (now in APEC Framework)

Result: Little beyond 1980's OECD standards;

- GDPR has no effect, but nor has 'data sovereignty';
- 'minimalist' model of Asian data protection (with Japan).

Singapore – Enforcement

- Personal Data Protection Commission (PDPC)
  - A government authority, not an independent DPA
  - 6 members as yet – from InfoComm Development Authority) + Advisory Committee
  - Powers to issue Guidelines (does so), as well as enforce Act
- Strong PDPC enforcement powers
  - Can investigate on complaint or own motion
  - Broad powers to direct compliance; can fine up to S$1M; fines often S$10K-30K, sometimes S$50K;
  - 2019 fines of SingHealth (S$250K) & IHIS (S$750K) for data breaches affecting 1.5M people (highest Asian fines except Korea)
  - PDPC cannot award compensation (courts can: over)
  - Appeals on all grounds are to 3 person appeal committees of the Data Protection Appeal Panel; then to District Court etc
  - Transparency: 2015 Regulations allow publication of decisions, publication is very regular, and respondents are always named (‘name and shame’)
  - For examples of enforcement action, see See 2017 *Update* pp. 25-26; 2018 Update p. 13; 2019 Update p.21.

Singapore – Enforcement (2)

- Offences usually require dishonest intent to be shown
- Actions before courts for compensation, injunctions or other remedies for breaches of Principles
  - PDPA requires any appeals against PDPC completed first
  - Plaintiffs will bear risks of ‘costs against’ in Singapore’s expensive courts – unrealistic to expect many such actions
  - No such actions known
- Personal & vicarious liabilities increase risks
  - Employers have vicarious civil liability for acts of employees
  - Company officers have personal liability for offences involving their consent, connivance or neglect (like Korea).

Singapore – Data exports (1)

Personal Data Protection Regs. (2014)

- S26(1) requires data exporters to ensure a 'comparable' standard of protection to PDPA
- Exporter must comply with PDPA, wherever data located, if it retains possession/control (R9(1)(a))
- Exporter must ensure recipient also has a 'legally enforceable obligation' to provide comparable protection (R9(1)(b))
  - Can be via legislation (no 'WhiteList' provisions), contracts, BCRs etc:
  - Failure to do so a breach by exporter: PDPC penalties
  - Data subject's remedies against importer will have to arise under this 'legally enforceable obligation' (if aware of it!!)

Singapore – Data exports (2)

Singapore's multi-faceted approach to exports

– 2019 update p. 22; 2018 Update p. 14

1. PDPC's recommended Standard Contract Clauses
   – Possible future ASEAN and perhaps EU consistency?
2. Joining APEC-CBPRs; application approved
   – Non-functioning until Accountabilty Agent appointed
3. Data Protection Trustmark Certification Scheme (DPTM Cert)
   – 3 assessment bodies appointed by IMDA
   – If Singapore deems APEC-CBPRs standards are 'comparable' to Singapore, then some type of joint certification is possible (but has not occurred)
   – US APEC-CBPRs certified companies are not yet regarded as DPTM Cert
4. Singapore's *Cybersecurity Act* 2018
   – allows designation of 'critical information infrastructure' (CII)
   – does not involve data localisation

Result: Singapore is exploring many avenues of 'mutual recognition'