HKGCC Legal Committee Meeting

Proposed legislative amendments to the Personal Data (Privacy) Ordinance (PDPO)

17 July 2020

Stephen Kai-yi WONG, Barrister
Privacy Commissioner for Personal Data,
Hong Kong, China

The Change of Global Privacy Landscape

Technology (e.g. AI, Big Data, cloud, IoT, social media) is increasingly making impact on personal data privacy

Many jurisdictions have passed or proposed **new/revised personal data protection law**

The adoption of data protection and privacy legislation **increased by 11%** between 2015 and 2020#

66% of nations of the world have data protection legislation#

EU GDPR (effective May 2018) raised the benchmark of personal data protection and people's **privacy expectation** to new heights

#Source: United Nations Conference on Trade and Development (UNCTAD)

New Laws/Bills

Jurisdiction	Status	Law (Amendments shown in bracket [non-exhaustive])
Australia	Amendment | Implemented in Feb 2018	The Privacy Act 1988 *(Mandatory Data Breach Notification)*
Brazil	New | Passed in Aug 2018 (date for implementation T.B.D.)	General Data Protection Law (LGPD)
California, US	New | Implemented in Jan 2020	California Consumer Privacy Act (CCPA)
Canada	Amendment | Implemented in Nov 2018	Personal Information Protection and Electronic Documents Act (PIPEDA) *(Mandatory Data Breach Notification)*
India	New | Proposed in Dec 2019	Personal Data Protection Bill, 2019
Japan	Amendment | Passed in Jun 2020 (expected effective in Q4 2021 or Q1 2022)	Amendments to the Act on the Personal Information Protection Law (APPI) *(Mandatory Data Breach Notification)*

New Laws/Bills(cont.)

Jurisdiction	Status	Law (Amendments shown in bracket [non-exhaustive])
New Zealand	Amendment | Passed in Jun 2020 (will be implemented in Dec 2020)	New Privacy Bill to replace The Privacy Act 1993 *(Mandatory Data Breach Notification)* *(Extra-territorial application)*
Singapore	Amendment | Proposed in May 2020	Personal Data Protection Act 2012 (PDPA) *(Mandatory Data Breach Notification)* *(Accountability)* *(New legal basis for data processing - legitimate interest)* *(Data portability)*
South Korea	Amendment | Passed in Jan 2020	Amendments to the Personal Information Protection Act (PIPA) *(Permit the use of pseudonymised data without obtaining data subjects' consent)* *(Permit the use of personal data to an extent reasonably related to the original purpose)*
Thailand	New | Passed in May 2019 (most provisions effective from May 2021)	Personal Data Protection Act (PDPA)

Common requirements in new data protection laws/bills

Jurisdiction	Accountability requirements	Mandatory Data Breach Notification	Right To Be Forgotten	Administrative Fines	Extra-territorial Application
EU	✓	✓	✓	✓	✓
Australia	✓	✓	✗	✗	✓
Brazil (not yet implemented)	✓	✓	✗	✓	✓
California, US	✗	✓	✓	✗	✓
Canada	✓	✓	✗	✗	✗
India (proposed)	✓	✓	✓	✓	✓
Japan	✗	✓ (not yet implemented)	✗	✗	✓
New Zealand	✗	✓ (not yet implemented)	✗	✗	✓ (not yet implemented)
Singapore	✓	✓ (proposed)	✗	✓	✓
South Korea	✓	✓	✓	✓	✗
Thailand (not yet implemented)	✗	✓	✓	✓	✓

(considered "yes" by regulators, tough no explicit provision in the laws)

Data breach of an airline based in Hong Kong affecting 9.4m passengers

- Suspicious activities on its network detected in March 2018
- Data breach notification not lodged to PCPD until 24 Oct 2018
- 9.4 million passengers from over 260 countries / jurisdictions / locations affected
- Personal data involved consisted mainly of name, flight number and date, email address, membership number, address, phone number

Call for amendment of PDPO

The Government presented amendment directions for the PDPO to Legislative Council in January 2020:

I. Mandatory data breach notification mechanism
II. Requirements on setting out data retention policy
III. Increasing PCPD's sanctioning powers
IV. Regulating data processors directly
V. Clarifying the definition of 'personal data'
VI. Regulation of doxxing

What is a 'data breach'?

- ***Data Protection Principle 4:*** Data users shall take all practicable steps to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data.

- ***Definition of "personal data breach":*** A data breach is a suspected breach of security exposing personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

Existing Issues

(I) Mandatory Breach Notification Mechanism

Leakage of personal data on the internet is common in information age

Number of data breaches in Hong Kong has been increasing steadily in recent years

No. of data breach notifications received by PCPD **reached a record-high of 139 in 2019**, almost double that in 2014

Existing Issues

(I) Mandatory Breach Notification Mechanism

Some data users **took months to voluntarily report a data breach**, falling short of society's expectations

Prompt notifications are important for **mitigating measures** to be taken to prevent further damage

The **global data protection landscape** has moved towards a mandatory breach notification regime

(I) Mandatory Breach Notification Mechanism

Notification threshold

Jurisdiction	Notification Threshold
Australia	"likely to result in serious harm" (for notifying DPA and impacted individuals)
Canada	"a real risk of significant harm" (for notifying DPA and impacted individuals)
EU	notifying DPA unless "unlikely to result in a risk to the rights and freedoms of natural persons" notifying impacted individuals if "likely to result in a high risk to the rights and freedoms of natural persons"
New Zealand	"has caused or is likely to cause serious harm to the impacted individuals" (for notifying DPA and impacted individuals)

(I) Mandatory Breach Notification Mechanism

Notification timeframe

Jurisdiction	Notification timeframe
Australia	'as soon as practicable' (for notifying DPA and impacted individuals)
Canada	'as soon as feasible' (for notifying DPA and impacted individuals)
EU	'without undue delay and, where feasible, no later than 72 hours' (for notifying DPA) 'without undue delay' (for notifying impacted individuals)
New Zealand	'as soon as practicable' (for notifying DPA and impacted individuals)

(I) Mandatory Breach Notification Mechanism

Investigation timeframe for suspected breach

Jurisdiction	Investigation timeframe
Australia	Risk assessment is required to be undertaken and completed within 30 days of a suspected data security incident

(I) Mandatory Breach Notification Mechanism

Consequences for failure to make notification

Jurisdiction	Consequences
Australia	Civil penalties up to AU$2.1 million
Canada	Criminal fine up to CA $100,000 imposed by court
EU	Fines up to €10 million or 2% of the organisation's total worldwide annual turnover, whichever is higher
New Zealand	Criminal fine of up to NZ$10,000 imposed by court

Possible Amendments

(I) Mandatory Breach Notification Mechanism

- Notify both the **PCPD** and the **impacted individuals**
- Notification threshold – "***real risk of significant harm***"
- Set **time limit** – e.g. 5 business days for notifying PCPD
- May allow for investigation period for 'suspected breach' before notification (e.g. 30 days)
- PCPD may direct data user to notify impacted individuals
- Failure to make notification may result in administrative fine imposed by PCPD.

Existing Issues

(II) Additional regulation on retention of personal data

Current provisions:

Data Protection Principle 2:

Personal data is **not kept longer than is necessary** for the fulfilment of the purpose for which the data is or is to be used

Does not define when personal data is "no longer necessary"

No fixed retention period requirements

No requirements for setting data retention policy

But there is no one-size-fit-all approach to data retention

Data retention – Overseas provisions

Generally do not spell out the definite retention period for personal data:

EU GDPR: Personal data kept **no longer than necessary**

Canada PIPEDA: …personal data shall be retained **only as long as it is necessary** for the fulfilment of the collection purposes

Australia APA: …destroy the personal data that the entity **"no longer needs"** for the allowed purposes

New Zealand NZPA: "**shall not keep [personal data] for longer than is required**" for the purposes for which the information may lawfully be used

Singapore PDPA: **cease to retain personal data "as soon as it is reasonable"** […] "no longer necessary" for any legal, business or other collection purposes

Risky data retention practices by data users:

Existing Issues

- Value of personal data increased in the digital age
- Cost of data storage decreased
- Low transparency regarding data retention policies
- Data users did not regularly erase unnecessary personal data
- Risk of data breach increases

Possible Amendments

(II) Additional regulation on the retention of personal data

- Amend DPP5(a) to expressly include the retention policy in the information to be made available
- Data users to formulate and disclose personal data **retention policy**
- Disclose **maximum retention** period for different categories of personal data

Data retention policy – A well-balanced direction

Stronger **privacy protection** and **data security** to all stakeholders

Greater **flexibility** to data users

Higher **transparency** to the public

(III) PCPD's Sanctioning Powers

Existing Issues

PCPD has no authority to impose administrative fines, or carry out criminal investigation and prosecution

Current penalty provisions in the PDPO:

- Contravention of DPPs is not an offence
- PCPD may issue an enforcement notice, non-compliance with which is a criminal offence
- Offences under S.64 (e.g. criminal doxxing) and Part 6A (direct marketing) may attract higher penalties

Penalty levels may not reflect the seriousness of the offence and the harm suffered by affected data subjects:

- From 1996 to June 2020: only 35 cases resulted in conviction by court (mostly direct marketing-related), fines imposed were all relatively low

PDPO criticised for its weak deterrent effect

(III) PCPD's Sanctioning Powers

Not uncommon for local and overseas non-judicial bodies to have the power to impose monetary penalties

- Overseas examples:
  EU Data Protection Authorities [@GDPR]; UK ICO [@DPA 2018]; Singapore PDPC [@PDPA]
- Local examples:
  Hong Kong Monetary Authority; Securities and Futures Commission

Administrative fine is an effective and efficient alternative to criminal prosecution

- Less onerous legal requirements than criminal court proceedings
- More expeditious and cost-effective enforcement tool
- Less stigma than criminal conviction by court

Possible Amendments

(III) PCPD's Sanctioning Powers

- Confer additional powers on the PCPD to impose **administrative fines**
- Maximum level of fine may be a **fixed amount or a percentage of the annual turnover**, whichever is higher
- Administrative fines **credited to the HKSAR Government** and not the coffers of the PCPD

Procedures for imposing administrative fines

Recommendations alleviating concerns that the PCPD may arbitrarily impose administrative fine:

- **Procedure** – The PCPD to provide an **administrative fine notice** to the data user or data processor of its intent to impose an administrative fine, the circumstances of any breach, the investigation findings and the indicative level of fine, along with a rationale for the fine.
- **Right to representation** – Upon receipt of the aforesaid notice, the data user or data processor should be given no less than **21 calendar days to make representation**.
- **Right to appeal against the administrative fine notice** – once an administrative fine notice is issued to a data user or data processor, it has the **right to appeal to court** or the Administrative Appeals Board against the notice within **28 calendar days**.

(IV) Regulate data processors directly

Existing Issues

Outsourcing data activities are becoming more common

The PDPO does not regulate data processors

- Data processor acting purely on behalf of an overseas data user is not subjected to regulatory oversight of PDPO, i,e, PCPD cannot investigate breaches of DPPs.
- The apportionment of responsibility between data users and data processors is often unclear, resulting in insufficient data protection
- Hong Kong's reputation as a regional or international data centre is compromised if the PCPD has no *locus standi* to investigate data security incidents involving processors (e.g. cloud service providers)

(IV) Regulate data processors directly

Many **overseas regulatory models** adopt direct regulation on data processors:

- Australia APA, Canada PIPEDA, New Zealand NZPA:
  Both data user and processor are directly regulated
- EU GDPR, Singapore PDPA:
  Data processors directly regulated and indirectly regulated through data users

(IV) Regulate data processors directly

Direct regulation of data processors can…

- Eliminate legal loopholes in existing provisions
- Ensure **fair share of responsibilities** between data users and data processors
- Enhance protection for personal data during processing

Improve the cloud readiness and reputation of Hong Kong by attaining a **satisfactory regulatory environment**

Possible Amendments

(IV) Regulate data processors directly

Data processors' obligations on:

- **retention period** of personal data
- **security** of personal data
- **notification to data users and PCPD** of data breaches without undue delay

(V) Clarify the definition of 'personal data'

Existing Issues

The concept of "personal data" under the PDPO has been challenged by ICT developments

PDPO currently only applies to data that can be practicably used to ascertain the identity of a person

New technologies causing new privacy concerns

E.g. Metadata and IP address are not 'personal data' under PDPO, but they could be used to conduct profiling

Many overseas judicial authorities extended their data protection regimes to cover IP address and other online identifiers

E.g. EU's GDPR

Definitions of "personal data"

PDPO	Overseas (e.g. AU, CA, EU)
Criteria: • Practicable to ascertain identity	**Criteria:** • Relating to or about an identifiable individual
Meaning: • Knowing who a person is	**Meaning:** • Able to single out a person, not necessarily knowing who the person is
Result: • Narrower scope of personal data and less protection to privacy	**Result:** • Wider scope of personal data and stronger protection to privacy

Possible Amendments

(V) Expand the definition of 'personal data'

Personal data may include:

- Information practicable to ***ascertain an identity*** (direct/indirect); and
- Information ***relating to an identifiable*** person

Large scale criminal doxxing incidents

Existing Issues

- Around **5,000** doxxing cases since June 2019

- Current provisions: It is an offence to disclose any personal data of a data subject which was obtained from a data user without the data user's consent and if the disclosure causes psychological harm to the data subject. (Section 64(2))

Large scale criminal doxxing incidents

Existing Issues

Actions taken by the PCPD so far:

- Approached and written to operators of platforms **over 180 times**
- Requested removal of **over 3,000 links** to doxxing posts, 60% of which have been removed
- Investigated and referred **over 1,400 cases** to the Police

First conviction arising from doxxing in June 2020

- Not under PDPO
- Contempt of court – contravention of court injunction against doxxing of police officers
- 28 days of imprisonment, suspended for a year

Difficulties the PCPD encountered when handling doxxing cases:

No criminal investigation and prosecution powers

Difficult to trace the identities of doxxers

Difficult to prove the doxxing materials are obtained from a data user without the data user's consent

Most of the doxxing posts are hosted by overseas social media platforms

Doxxing regulation in other jurisdictions

- Major jurisdictions usually do not have specific provision for doxxing in data protection laws
- *Network Enforcement Act* of Germany provides administrative measures to compel social media platforms to remove improper online materials
- *Harmful Digital Communications Act of New Zealand allows victims of cyberbullying to apply for court order against social media platforms to take down unlawful materials*
- Singapore amended the *Protection from Harassment Act* in 2019 to prohibit disclosure of identity information with an intent to cause alarm or distress to the target persons or related persons (i.e. doxxing)

Possible Amendments

(VI) Regulation of doxxing

- Introduce legislative amendments to specifically address doxxing
- Confer on the Privacy Commissioner statutory powers to:
  - ✓ Compel the **removal of doxxing contents** from platforms/websites
  - ✓ Carry out **criminal investigation and prosecution**

Addressing public concerns

More opportunities for businesses

Increase consumers' willingness to use new technologies, products and services

Stronger privacy laws will allay the public's privacy concerns

Example 1:
Concerns about personal data leakage was the major reason for not using mobile payment for **62%** consumers.

-HKPC and Alipay Survey 2019

Example 2:
48% consumers cited **'data privacy'** as the primary reason for not adopting wearable devices.

-HKPC Survey 2020

Compliance, Ethics and Trust:

Edelman Trust Barometer 2020

The public tend to trust ethical behaviours more than competence:

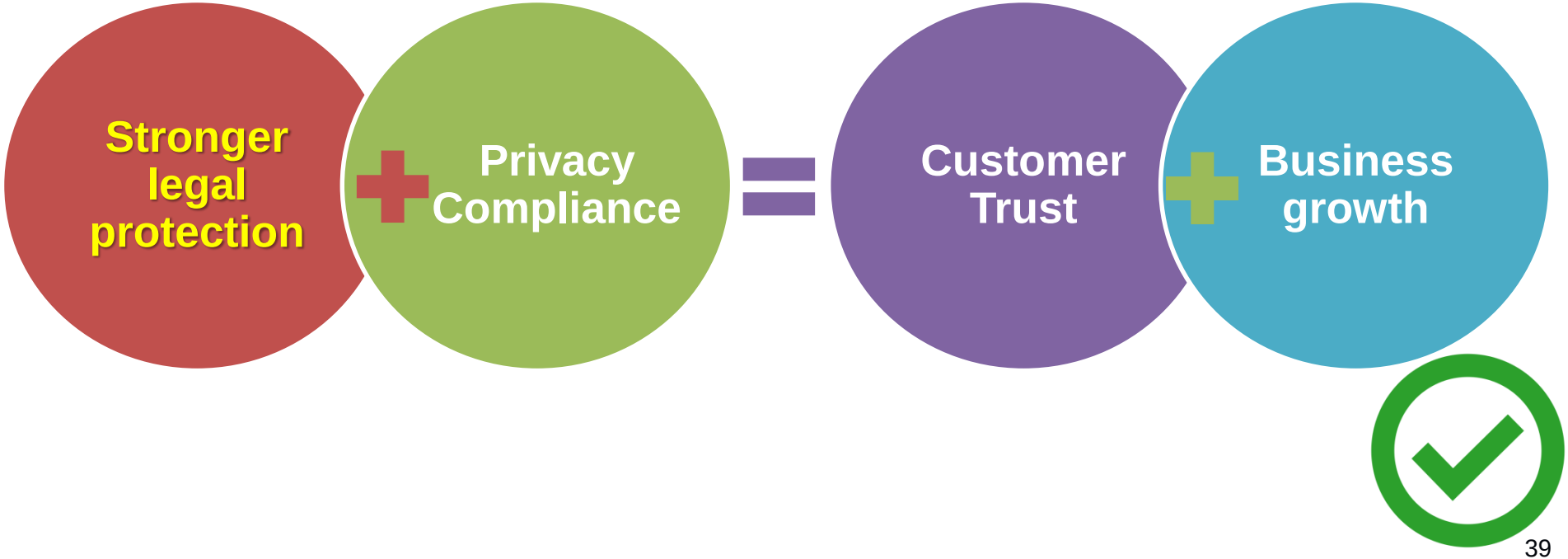
For institutions to drive trust, ethical behaviours of an organisation are **3 times more important** than its competence.

Edelman Trust Barometer 2018

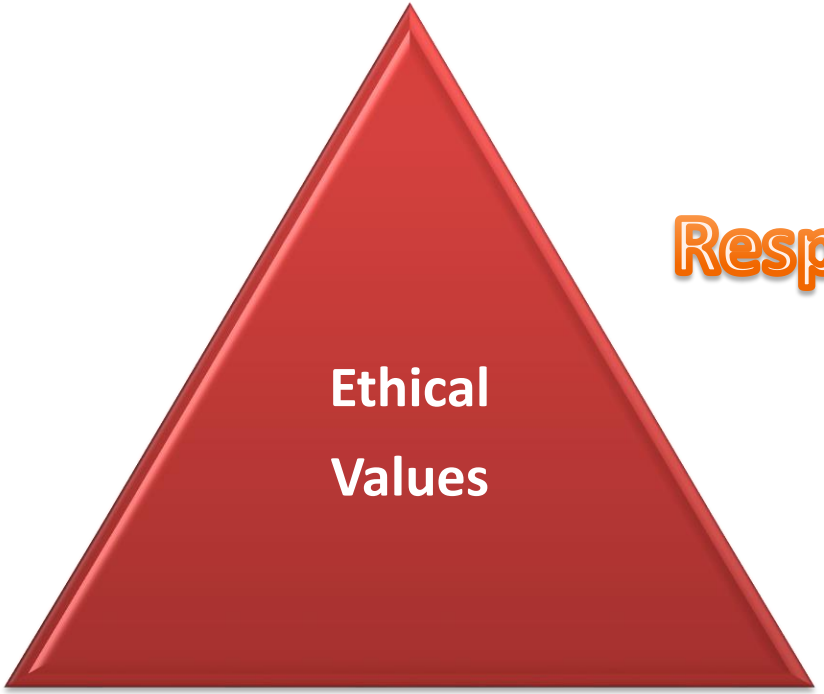
Consumers have high expectations for brands' compliance with privacy laws:

83% respondents think **protection of privacy** and personal information is **one of the most important obligations** for business.

With heightened privacy expectation of consumers…



PCPD's Ethical Accountability Framework



Respectful

Beneficial

Fair

Download Our Publications

JOIN

Data Protection Officers' Club

(Membership Application)

保障資料主任聯會 DATA PROTECTION OFFICERS' CLUB

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK$350 per year
Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/enrol.html

JOIN today!

Contact Us

Hotline 2827 2827

Fax 2877 7026

Website www.pcpd.org.hk

E-mail communications@pcpd.org.hk

Address 1303, 13/F, Sunlight Tower,
248 Queen's Road East,
Wanchai, HK