Cyber Attack Hong Kong 2020

Proposed legislative amendments to the Personal Data (Privacy) Ordinance (PDPO) – Reviewing, Developing and Strengthening Hong Kong's Personal Data Privacy

15 September 2020

Tony LAM
Deputy Privacy Commissioner for Personal Data,
Hong Kong, China

Landscape and Context

- Increasing expectation of individuals on personal data protection in recent years → enabling trust is a must and trust is built upon visible systems, practices and behaviours
- Changes in the global privacy landscape (spearheaded by GDPR)
- Major data breach incidents in Hong Kong (e.g. airline, credit reference agency, hotel chain, etc, in 2018)
- Rapid technological development (e.g. prevalence of the Internet, big data, development and use of AI)

The possible amendment directions can be categorized into 4 areas:

SCOPE

(1) Definition of personal data

(2) Direct regulation on data processors

RIGHTS OF INDIVIDUALS

(3) Requiring organizational data users for providing retention policy and maximum retention period for personal data

DETERRENT EFFECT

(4) Instituting a mandatory data breach notification system

(5) Empowering the Privacy Commissioner to administer administrative fines

PROCESS

(6) Vesting criminal investigation and prosecution powers with the Privacy Commissioner, including enhanced powers to deal with offences like doxxing

SCOPE

(1) Definition of personal data
(2) Direct regulation on data processors

Possible Amendments

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

Possible Amendments

Regulate data processors directly

Data processors' obligations on:

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

RIGHT OF INDIVIDUALS

(3) Requiring organizational data users for providing retention policy and maximum retention period for personal data

Possible Amendments

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

DETERRENT EFFECT

(4) Instituting a mandatory data breach notification system

(5) Empowering the Privacy Commissioner to administer administrative fines

Possible Amendments

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
- PCPD may direct data user to notify impacted individuals

PCPD's Sanctioning Powers

Possible Amendments

- 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
- Mechanism: issue **administrative fine notice** specifying the circumstances of any breach, the investigation findings and the indicative level of fine, along with a rationale for the fine; give data user a **right to make representation** and a **right to appeal**
- **Raise the relevant criminal fine levels** for offences under the PDPO

PROCESS

(6) Vesting criminal investigation powers and prosecution powers with the Privacy Commissioner, including enhanced powers to deal with offences like doxxing

Possible Amendments

(6) Vesting criminal investigation powers and prosecution powers

- Confer powers on the Privacy Commissioner to carry out criminal investigation and prosecution in her own name
- Introduce legislative amendments to specifically address doxxing and confer powers on the Privacy Commissioner to request the removal of doxxing contents from platforms/websites and apply for injunction orders

Trust: The fundamental for human interactions

- Trust is the very social fabrics of society
- Trust is faltering

Cybersecurity Expectations

- **Data breach is not a matter of “if”**
- **Data breach is a matter of “when”**

Human error is a leading cause of data breaches!

- **According to a survey in U.S.[1] (in June 2019), around 53% of data breaches were attributable to human errors. It also revealed that due to lack of training, employees pay less attention to information security policies and procedures.**

- **Another survey in UK[2] (in March 2020) showed that 60% of UK businesses have experienced a cyber-attack and/or data breach caused by human error.**

1. The online survey is conducted by Ipsos on behalf of Shred-it (an information security service provider).
2. The survey was conducted by Gallagher, a global insurance company, polling 1,000 UK business leaders to find out more about their exposure to cyber-risk.

Resolution to address the role of human error in personal data breaches

- Adopted at the 41st International Conference of Data Protection & Privacy Commissioner in October 2019 (now renamed as Global Privacy Assembly)

- Recognized that personal data breaches often involve human error, specifically, employees unintentionally disclosing personal data to unauthorised recipients or individuals being deceived into compromising user credentials that allow access to information and systems

Resolution to address the role of human error in personal data breaches

- **The Resolution called upon, among others, data protection authorities to promote appropriate security safeguards to prevent human error that can result in personal data breaches, such as**
  - Building workplace cultures where privacy and personal data security are organisational priorities through training and education
  - Establishing robust and effective data protection and privacy practices, procedures and systems
  - Evaluating privacy practices, procedures and systems to ensure continued effectiveness

- **ISO hailed it as the world's first international standard for managing privacy information**
- **Building on ISO 27001 and ISO 27002**
- **Assisting in compliance with personal data protection laws**

- **Four core parts:**
  - ❖ Personal information management system
  - ❖ Information security techniques and good practices
  - ❖ Guidance for PII controllers (i.e. data users)
  - ❖ Guidance for PII processors (i.e. data processors)

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/files/AppForm_1920_NewMembers.pdf

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

PCPD.org.hk 香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong