The University of Hong Kong

Personal Data Protection and Security Measures

April 2021

Agenda

- Personal Data (Privacy) Ordinance (presented by Mr. Joe Poon, In-House Legal Counsel / Data Protection Officer)
- Security Measures in HKU (presented by Mr. Kelvin Chan, Information Technology Services)
- Q & A Session

Will you graduate after this presentation?

Privacy, Personal Data Protection and Confidentiality

- Confidentiality obligations under common law (special circumstances and / or relationship,

  e.g. employer / employees;
  school / students;
  principal / agents;
  public office holders)

- Contractual obligations: express or implied term on confidentiality

Privacy, Personal Data Protection and Confidentiality

- Statutory obligations: Personal Data (Privacy) Ordinance ("PD(P)O") – Protection of personal data
- Professional rules or codes of conduct

Remedies for Breach of Obligations

- Injunction
- Damages
- Sanctions under PD(P)O

Personal Data (Privacy) Ordinance

Training Materials:

- The videos in the training kit of the Privacy Commissioner's Office / Personal Data Protection Slides: http://www.its.hku.hk/services/training/infosec/personal-data-protection (ITS Training Web Page)

Certain Highlights of the Personal Data (Privacy) Ordinance

Personal Data (Privacy) Ordinance

What is "*personal data*"?

- non personal data is not protected under the PD(P)O
- but note other general obligations of confidentiality

Personal Data (Privacy) Ordinance

"personal data" (個人資料)
means any data:

- relating directly or indirectly to a living individual
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained
- in a form in which access to or processing of the data is practicable

Personal Data (Privacy) Ordinance

"data" (資料)

means any representation of information (including an expression of opinion) in any document, and includes a personal identifier

Personal Data (Privacy) Ordinance

"personal identifier" (個人身分標識符) means an identifier:

- that is assigned to an individual by a data user for the purpose of the operations of the user
- that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual

Personal Data (Privacy) Ordinance

Examples of personal data

Student, Staff, Patient and Research

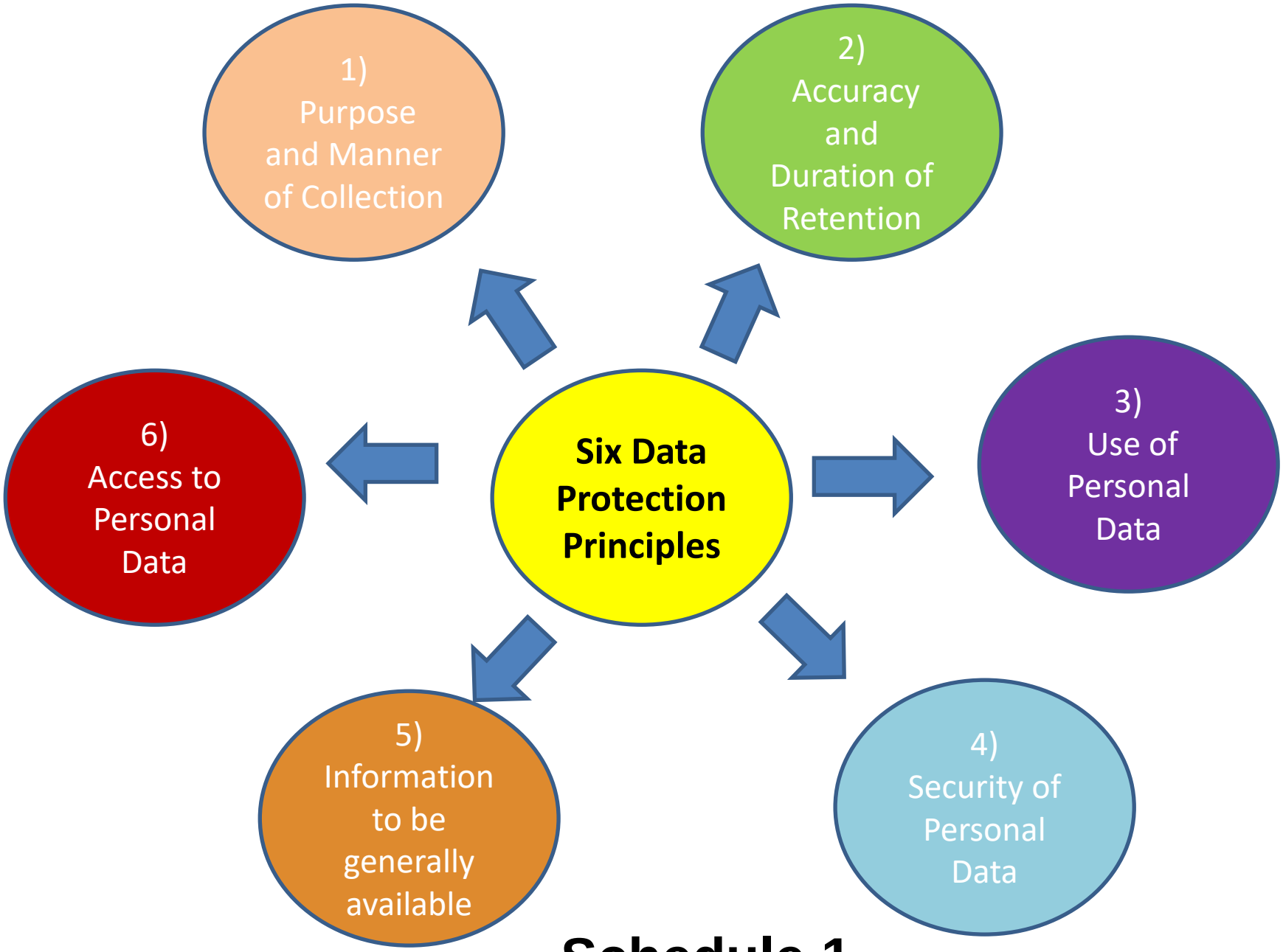
- Name, Address, Phone No., and HKID/UID No.
- “Expression of Opinion” – Comments made by referees
- Examination paper – Comments made by markers

Note : Email / IP Address

The Six Data Protection Principles

Section 4

"A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance."


1)
Purpose
and Manner
of Collection
2)
Accuracy
and
Duration of
Retention
6)
Access to
Personal
Data
Six Data
Protection
Principles
3)
Use of
Personal
Data
5)
Information
to be
generally
available
4)
Security of
Personal
Data

Schedule 1

Data Protection Principles

Schedule 1

Principle 1 - purpose and manner of collection of personal data

Principle 2 - accuracy and duration of retention of personal data

Principle 3 - use of personal data

Principle 4 - security of personal data

Principle 5 - information to be generally available

Principle 6 - access to personal data

Data Protection Principles

Data Collection (DPP1)

- Lawful, related, necessary, not excessive and fair
- Data collection statement

Examples: Application Forms, CCTV, etc.

Data Protection Principles

Use of Personal Data (DPP3)

- Prescribed consent – need not be in writing, but note the problem of evidence
- Not for a "new purpose": purpose of collection (or a directly related purpose) – how to interpret the purpose / directly related purpose

Data Protection Principles

Exemption for DPP3 (Section 58)

(1) Personal data held for the purposes of:

(a) the prevention or detection of crime

…

(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons

…

Data Protection Principles

(2) Personal data is exempt from the provisions of data protection principle 3 in any case in which:

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data is held for any of those purposes); and

Data Protection Principles

(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show *that he had reasonable grounds for believing that* failure to so use the data would have been likely to prejudice any of those matters

Data Protection Principles

Exemption for DPP3 (Section 59)

(1) Personal data relating to the physical or mental health of the data subject is exempt from the provisions of either or both of:

Data Protection Principles

…

(b) data protection principle 3,

in any case in which the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of:

(i) the data subject; or

(ii) any other individual

Data Protection Principles

(2) Personal data relating to the identity or location of a data subject is exempt from the provisions of data protection principle 3 if the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of:

(i) the data subject; or

(ii) any other individual

Data Protection Principles

Exemption for DPP3 (Section 62)

- Personal data is exempt from the provisions of data protection principle 3 where-

(a) the data is to be used for preparing statistics or carrying out research

(b) the data is not to be used for any other purpose; and

(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them

Data Protection Principles

Security of Personal Data (DPP4)

"All practicable steps shall be taken to ensure that personal data… are protected against unauthorized or accidental access, processing, erasure, loss or use…"

Data Protection Principles

Key Requirements of the University

- The University's Code of Practice (revised version 2019)
- Guidelines issued by ITS
- The Registrar's email circulars
- Recommendations of the Investigation Committee (Data Breach Incident 2011)

Data Protection Principles

Statutory Data Access Request (DPP6 and Section 18)

- Entitlement of a data subject to be supplied by the data user with a copy of the requested personal data
- An indirect way to obtain information for other purposes

Data Protection Principles

Data Correction Request
(DPP6 and Section 22)

- Entitlement of a data subject to make a request for data correction

Data Protection Principles

Compliance Requirements

- The 40-day statutory period and compliance process

Data Protection Principles

Questions:

- *What should be collected and retained, and for how long?*

- *Any alternative to the DAR process?*

Amendments to PD(P)O

- Personal Data (Privacy) Amendment Ordinance 2012 (gazetted on July 6, 2012)
- Comprehensive amendments
- Implementation timeline

Amendments to PD(P)O

- Provisions unrelated to direct marketing or the legal assistance scheme effective from October 1, 2012
- Provisions relating to direct marketing effective from April 1, 2013
- Provisions relating to the legal assistance scheme effective from April 1, 2013

Key Amendments

- Use of personal data in direct marketing (including solicitation of donations)
- Disclosure of personal data obtained without data user's consent
- Legal assistance to aggrieved individuals

Key Amendments

- Strengthening the powers of PCPD
- More offences created and heavier penalties (e.g. unauthorized disclosure of personal data causing psychological harm to the data subject: HK$ 1,000,000 and imprisonment for 5 years; repeated contravention of an enforcement notice: imprisonment and fine)

Key Amendments

- Contractual and other requirements for outsourcing personal data processing

Direct Marketing Activities

- Part VIA of PD(P)O – New Regulatory Regime (including donation activities)
- New Guidance on Direct Marketing: http://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

Outsourcing Personal Data Processing

Revised DPP2 and DPP4

"data processor" (資料處理者) means a person who:

- (a) processes personal data on behalf of another person; and
- (b) does not process the data for any of the person's own purposes

Outsourcing Personal Data Processing

The obligations of data user to adopt contractual means or other means to prevent any personal data transferred from:

- (a) being kept longer than is necessary; and
- (b) unauthorized or accidental access, processing, erasure, loss or use

Outsourcing Personal Data Processing

Contractual means:

- All practicable security measures
- Timely return, destruction or deletion of data
- Prohibition against any use or disclosure for other purposes
- Prohibition against sub-contracting
- Right to audit and inspect

Outsourcing Personal Data Processing

Other means:

- Select a reputable data processor
- Select a data processor with robust policies and procedures
- Audit and inspect

Note: Information Leaflet of PCPD:

http://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

General Data Protection Regulation (GDPR) of the European Union (EU)

- Effective from 25 May 2018
- Note the extra-territorial effect
- Any EU presence and activities / EU data subjects elements (see Recitals (22) to (24))

  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- See the University's internal GDPR website:

  https://intraweb.hku.hk/reserved_2/gdpr/index.html


Common Questions
and
Issues

What and when personal data should be collected?

- Note DPP1 and, in particular the non-excessive/alternative principle
- For example, HKID Card and Number
- Other data: health and family data
- Check the Code of Practice on Human Resource Management: https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

What data and how long such data should be retained?

- Note DPP2 and Section 26: the principle of purpose/directly related purpose, necessity and legal obligation (employment records, tax returns, litigation, etc.)
- Job applicants' information (what is stated in the collection statement – the two-year rule)
- Note the exception of public interest (including historical interest)

Under what circumstances personal data can be used, disclosed, shared and transferred?

- Note DPP3: the principles of prescribed consent, and purpose/directly related purpose
- A matter of interpretation and judgment: the reasonable/commonsense approach
- Note the requirements of direct marketing

What security measures should be taken?

- Note DPP4
- Proper measures should be taken to ensure personal data will not be accessed, tampered, disclosed, released, transferred and destroyed
- Handling of data, authorized access, security control and monitoring, use of IT equipment and devices (e.g. portable storage devices, mobile phones, etc.)

What security measures should be taken?

- Guidelines, process, training, awareness and supervision
- Dealings with third parties (proper agreement and audit)
- Privacy Impact Assessment

What is a statutory data access request?

- Note DPP6 and Section 18
- The prescribed form should be used
- Only personal data are subject to the request, but not “documents”
- Expression of opinion (e.g. comments on performance) falls within the definition of personal data

What are the points to note for data breach?

- Guidance Note of the Privacy Commissioner
- Damage control (e.g. identity theft or fraud)
- Notifications to the affected data subjects and the relevant authorities

What is the General Data Protection Regulation of the European Union?

- Note the extra-territorial effect
- Any EU presence and activities / EU data subjects elements (see Recitals (22) to (24))

  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- See the University's internal GDPR website:

  https://intraweb.hku.hk/reserved_2/gdpr/index.html

The System and Practices in the University

- **Information Security and Data Management Policy:** https://isdm.hku.hk/
- **The Privacy Policy Statement :** http://www.hku.hk/privacy_policy/
- **Code of Practice (revised version 2019):** https://intraweb.hku.hk/reserved_1/gsabc/pdpo_cop.pdf (portable storage devices, incident handling / reporting and other guidelines)

The System and Practices in the University

- Data Collection Statement
- Statutory Data Access / Correction Request Process
- Central Compliance Team (compliance/monitoring)
- University Data Protection Officer and Personal Data Protection Coordinators
- Information Technology Services (advice / security measures / guidelines / training information): http://www.its.hku.hk/services/training/infosec/personal-data-protection

The System and Practices in the University

The Public Expectation

Awareness and Education

GOOD PRACTICE


YOU CAN
NOW
GRADUATE

Q & A