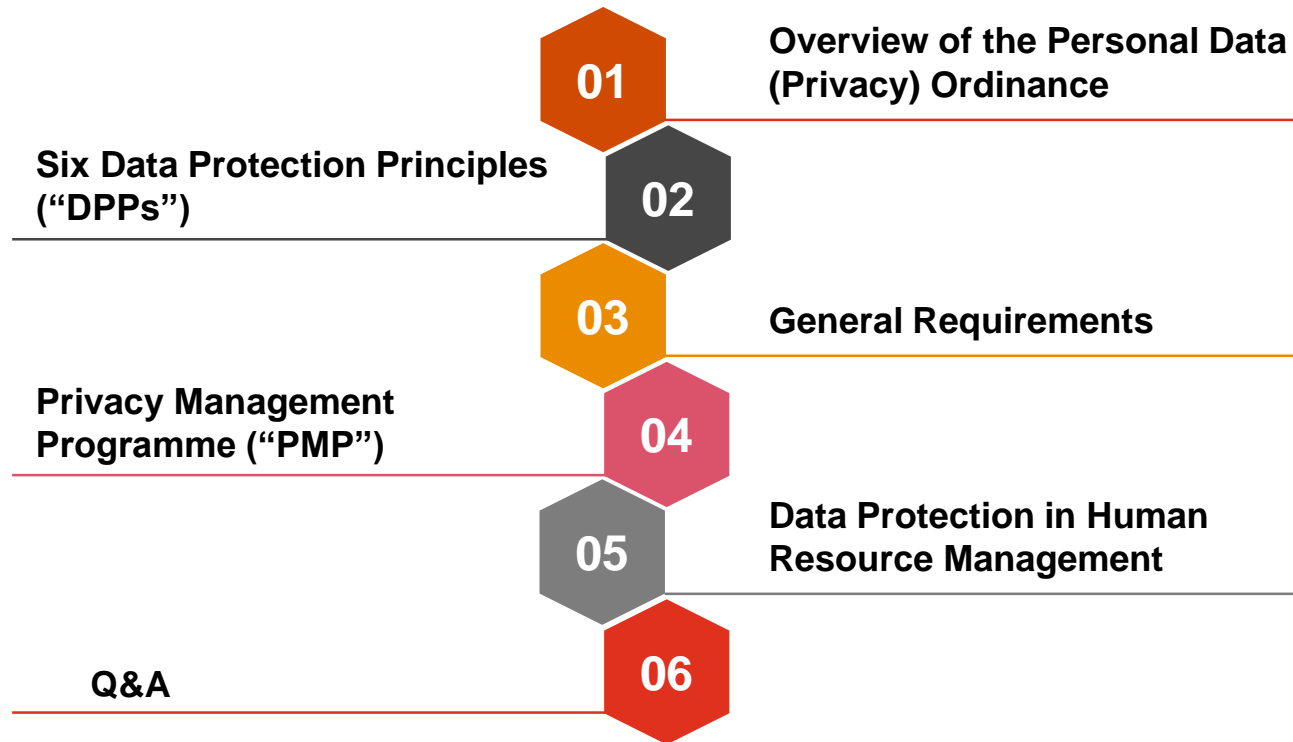


Data Protection Training to Data Protection Officers

Lingnan University
2 May 2019



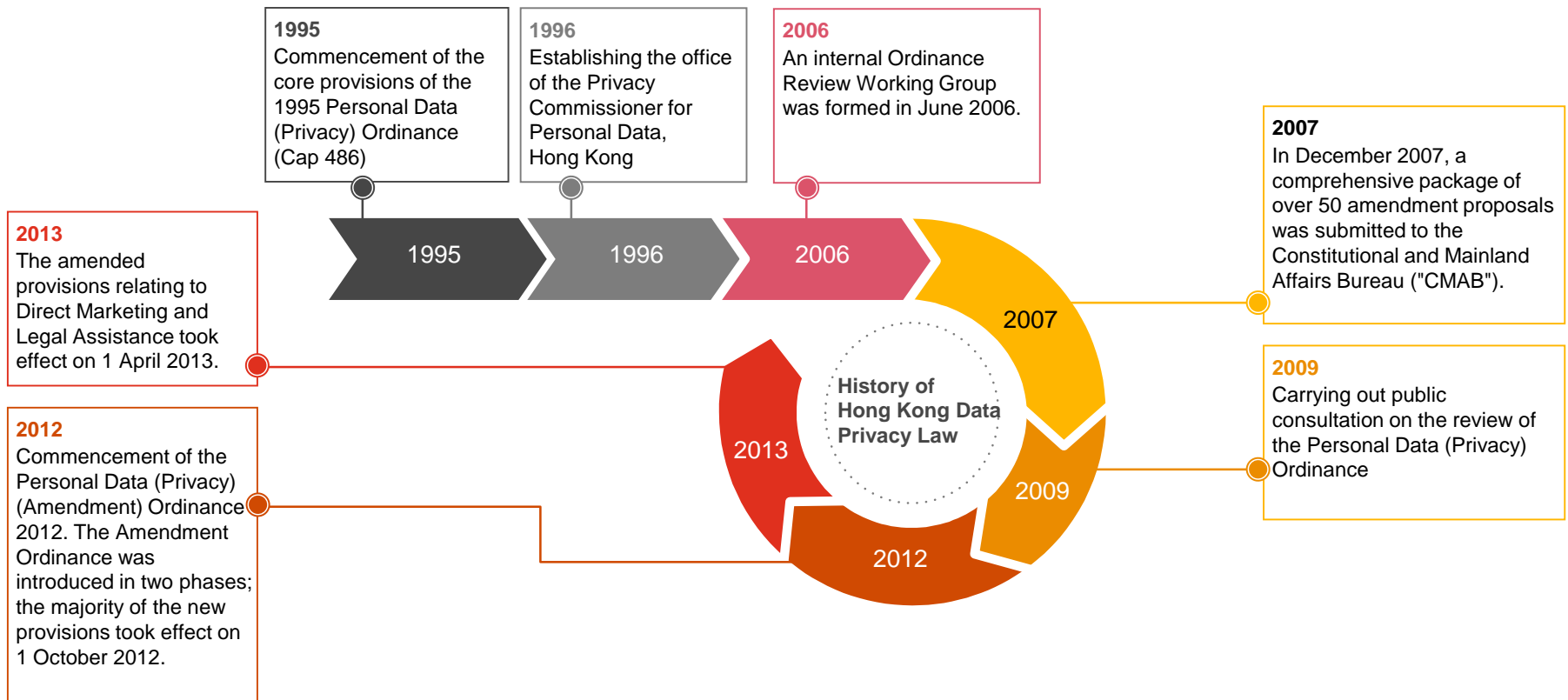
Agenda



1

Overview of the Personal Data (Privacy) Ordinance

History of Hong Kong Data Privacy Law



Hong Kong Data Privacy Law



The Office of the Privacy Commissioner for Personal Data (“PCPD”)

The PCPD is an independent statutory body set up **to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) (“Ordinance”)** which came into force on 20th December, 1996. Its mission is to secure the protection of privacy of individuals with respect to personal data through promotion, monitoring and supervision of compliance with the Ordinance.



The Personal Data (Privacy) Ordinance

The objective of the Ordinance is to protect the privacy rights of a person in relation to personal data (Data Subject). The Ordinance covers definitions and principles, such as:

- Define key terms such as “personal data”, “data subject” and “data user”, etc.
- Outline the “Six Data Protection Principles” (See Section 2)
- State a data user’s obligations and responsibilities under the Ordinance
- State the rights of a person (data subject) in relation to personal data
- State offences, compensation and exemptions to the Ordinance

Hong Kong Data Privacy Law



Key Highlights of the 2012 Amendment Ordinance relevant to the University

The **Amendment Ordinance** sets out **enhanced rules to govern Direct Marketing activities** under the Ordinance

- **Direct marketing**
 - Regulating the handling of personal data in the course of carrying out direct marketing activities
- **Outsourcing the processing of personal data**
 - The Amendment Ordinance does not directly regulate data processors
 - Requires data users to use contractual and other means to ensure that the personal data handled by a data processor is protected
- **Section 64**
 - Regulate the disclosure of personal data of a data subject obtained without consent from the data user under certain conditions (e.g. sale, disclosure or uploading of personal data, academic records or photos of a famous alumni without the consent of the University, with financial gain or causing psychological harm to the alumni)

Personal Data (Privacy) Ordinance (“the Ordinance”)

An Ordinance to protect the privacy of individual in relation to personal data, and to provide for matters incidental thereto or connected therewith:

Protecting the privacy right of a “**data subject**” in respect of “**personal data**”, but not the general privacy issues.

Data Subject	= The living individual who is the subject of the “personal data” concerned.
Data	= Any representation of information in any document , including expression of opinion or personal identifier.
Personal Data	= Personal data should satisfy three conditions: (1) relating directly or indirectly to a living individual ; (2) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (3) in a form in which “ access to ” or “ processing of ” the data is practicable.

Example Name: Chan Siu Ming HKID Card Number: Y0012xx(x)
:
Address: Flat A, 5th Floor, XXX Court, Hong Kong
Telephone number: 9222 XXXX Date of Birth: 8
November 19xx

What is personal data?

Personal Data

= Personal data should satisfy three conditions:





- (1) relating directly or indirectly to a **living individual**;
- (2) from which it is practicable for the **identity of the individual** to be **directly** or **indirectly** ascertained; and
- (3) in a form in which “**access to**” or “**processing of**” the data is practicable.

Examine the list of data below. Which of the following can identify an individual in itself?




- Lingnan University, Tuen Mun
- 2616 8750
- registry@LN.edu.hk
- Chan Siu Ming
- Chan Siu Ming, Lingnan University, Tuen Mun
- Chan Siu Ming with IP address 12.202.222.13
- chansiuming@LN.edu.hk

What is personal data? (Cont'd.)

The following examples are not specific enough to identify an individual, hence not considered as personal data:

- Lingnan University, Tuen Mun  A business address
- 2616 8750  A set of numbers without other personal identifier
- registry@LN.edu.hk  A business email address
- Chan Siu Ming  Generally speaking, a name alone is not personal data as it can be referred to a different person with the same name

These examples are personal data and can be used to identify a specific individual:

- Chan Siu Ming, Lingnan University, Tuen Mun  A business address combined with individual's name
- Chan Siu Ming with IP address 12.202.222.13  IP address relates to a specific device an individual used to access the internet combined with individual's name
- chansiuming@LN.edu.hk  An email address linked to an individual

2

Six Data Protection Principles

The Six Data Protection Principles

DPP1 - Collection

- For a lawful purpose, in a lawful and fair means
- Avoid collecting excessive data
- Consequence of not providing such data

DPP6 - Access & Correction

Provide the channel(s) and rights for data subjects to access and correct their own personal data

DPP5 - Openness & transparency of Privacy Policy and practices

- The kinds of personal data you hold and purpose for which data is being used
- Communication externally & internally

DPP2 - Accuracy & Retention

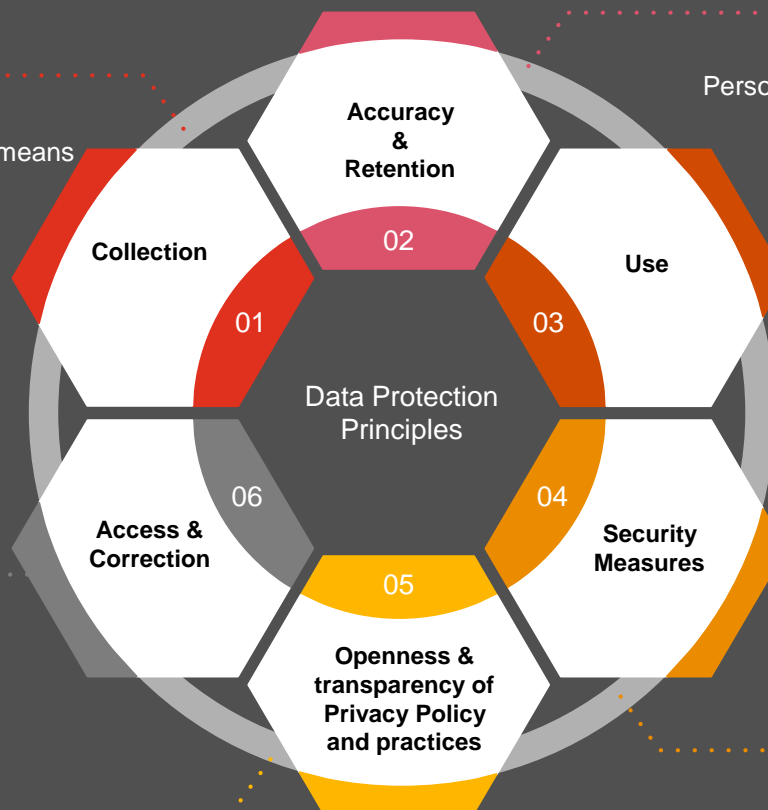
Personal data should be accurate and up-to-date, do not keep longer than necessary

DPP3 - Use

- Data collected can only be used for a specific purpose of collection
- Consent is required for other or new purposes e.g. direct marketing / transfer etc.

DPP4 - Security Measures

Personal data should be protected by appropriate and sufficient safeguards



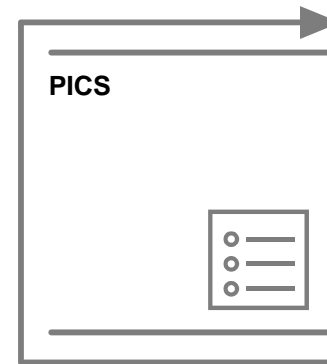
DPP1 Data Collection Principle



- Collection is **NECESSARY** but not **EXCESSIVE**.
- Collected in a **LAWFUL** and **FAIR** way, for a purpose directly related to a function or an activity of the data user.



- Notify the data subjects of the **PURPOSE** of data collection and the classes of persons to whom the data may be transferred



- Provide data subjects with a **Personal Information Collection Statement ("PICS")**.

Knowledge check #1

Which of the following kinds of personal data collected during registration to participate in a **training programme organised by the University may be excessive?**

(You may choose more than one answer)

- A. Date of Birth
- B. Copies of identity card
- C. Name
- D. Mobile phone number

Knowledge check #1 (Cont'd.)

Answer and explanation:

The answers are A and B

DPP1 provides that personal data collected from applicants should not be excessive in relation to the application to events / training programmes.

For the purpose of ascertaining the identity of individual, the University **may physically inspect** the applicant's identification document.




In addition, the training programme **does not offer privileges or benefits** to applicants associated with their date of birth. The collection of such data would be excessive in relation to the purpose of collection.

In general, University should not collect copies of identify cards from student applicants.

DPP2 - Data Accuracy & Retention Principle

Personal Data



-  Accurate
-  Should be disposed of when it is no longer required for the purpose for which it was originally collected.
-  Guidance on records disposal

DPP2 - Data Accuracy & Retention Principle

Personal data collected and maintained by the University should be as **accurate, complete, and up-to-date** as is necessary for the purpose for which it is to be used.

Questions to consider when assessing the compliance with the Ordinance:



Whether information in the personal data inventory is up-to-date to monitor and keep track of the retention period of records that contain personal data?



Has a **data retention schedule** been defined for different types of personal data collected?



Has **disposal of records** containing personal data in both physical and hardcopy been arranged in accordance with internal records management guidelines and procedures?



If a data processor is engaged, is contractual terms or other means in place to prevent personal data transferred to the data processor from being kept **longer than is necessary**?

Case study #2

Background

- Company A has opened a job application to potential job candidates.
- During application submission, Company A has requested for the applicant's information, including contact number, address, certificates / transcripts, etc.
- The information collected is solely for processing the job application and applicants are well-informed of the purpose of collection.
- However, Company A has a practice of retaining personal data of unsuccessful applicants for an indefinite period of time.

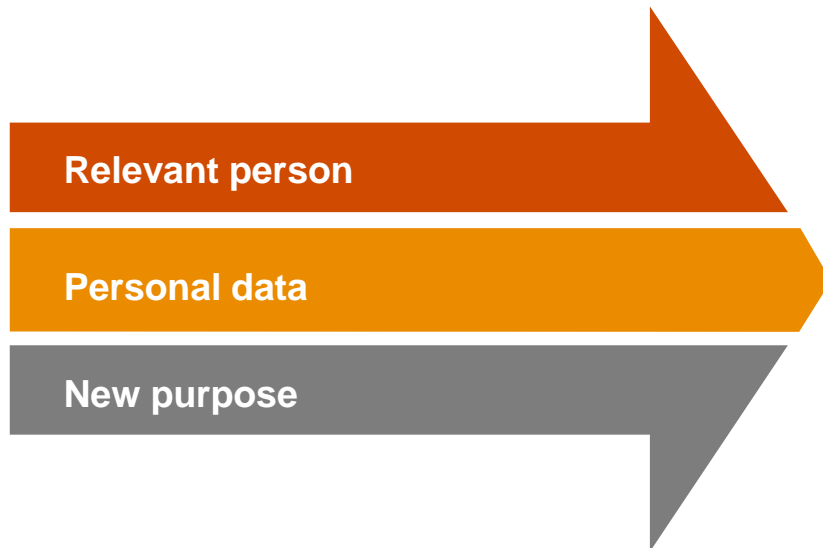
Answer and explanation:

The Code of Practice on Human Resource Management issued by the Commissioner stipulates that an employer should implement a written data retention policy that specifies a retention period of:

- **No longer than two years** in respect of recruitment-related data held about a job applicant from the date of **rejecting the applicant**;
- **No longer than seven years** in respect of employment-related data held about an employee from the date the **employee leaves employment**.

In regards of this case, personal data of unsuccessful applicants should not be retained for an indefinite period of time.

DPP3 - Data Use Principle



Relevant person

Give **PRESCRIBED CONSENT** for the data subject under specified conditions

Personal data

Only be used for the **PURPOSE** for which the data is collected or for a **DIRECTLY RELATED** purpose, unless voluntary and explicit consent for a **NEW** purpose is obtained from the data subject.

New purpose

Purpose **OTHER THAN** the purposes for which they were collected or directly related purposes

Case study #3

Background

- Person A lodged a complaint with a regulatory authority against Organisation A. (Case A)
- Person A lodged another complaint with the regulatory authority against Organisation B. (Case B)
- Person A decided to withdraw her complaint in Case B.
- Subsequent to withdrawal of the complaint in Case B, the regulatory authority sent a closing letter, in which Case A was mentioned, to Person A to conclude Case B. A copy of the closing letter was provided to Organisation B, therefore Organisation B became aware of the fact that Person A had also lodged a complaint with the regulatory authority against Organisation A.

Answer and explanation:

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used (including disclosed or transferred) for any purpose other than the purpose for which the data was to be used at the time of collection of the data, or for a directly related purpose.

Before disclosing the personal data of an individual to any third party, a data user should carefully consider whether it is necessary for the third party to be aware of the relevant data (i.e. disclosure should only be made on a need-to-know basis). A data user should not disclose personal data simply for the sake of convenience.

In this case, it was considered unnecessary for the regulatory authority to mention Case A in the closing letter sent to Organisation B. Hence, the regulatory authority is likely to be in breach of DPP3.

DPP4 - Data Security Principle



Data user

Safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

Data processor

- Data user engages a data processor
- Must adopt **contractual** or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Security measures for protection personal data

The University shall take all practicable steps to safeguard personal data against unauthorised or accidental access, processing, erasure, loss or use

Some considerations to note:

Awareness	<ul style="list-style-type: none"> A person handling the personal data must not discuss in public areas of any such personal data Documents containing personal data must not be left unattended 	Restricted Access to carry out work for "permitted purpose"	<ul style="list-style-type: none"> collection, processing and use of personal data should be restricted to HoD and authorised personnel
Storage	<ul style="list-style-type: none"> Personal data should be kept in confidential files locked in cabinets located in a controlled area accessible only to authorised staff "Clear Desk" policy should be in place 	Disposal of personal data	<ul style="list-style-type: none"> Personal data no longer required for the purpose for which they were to be used shall be destroyed in accordance with the code and ordinance must ensure that the physical destruction of personal data held on paper or other non-erasable medium is undertaken with appropriate security measures Data disposal record should be constructed to document data disposal activities. The data disposal record should at least include the following information: <ul style="list-style-type: none"> Department / Unit / Team Record Name / Format / Medium / Location Record reference number Reason for Disposal Method of Disposal / Destruction Whether all copied, including backups, are disposed Preparer and approver (name, position and contacts) Date of disposal
Transmission of personal data	<ul style="list-style-type: none"> "Need to know" principle should be applied – only circulate/ use the personal data not wider than what is required for the specific purpose No private copies of or communication to unauthorised parties Paper-based information sent out should be sealed in envelope and to be opened by the addressee or authorized person only 		

Safeguarding of data on electronic information on system

Good practices:



Data on
computer system

- ☐ All electronic files containing personal data, whether exported or manually created on personal computers, must be password protected as far as possible
- ☐ Ensure possible audit trail or a warning feature that could deter unauthorised attempts to access the data
- ☐ Eliminate all unofficial documents as soon as practical



Internet/Net
work Usage

- ☐ Ensure a secure network channel such as VPN connection before data transmission is carried out
- ☐ Employ WPA2 encryption for WiFi connection before data are transmitted through the air
- ☐ Avoid transmission of sensitive data in public access computers such as public computers in Internet cafés or public libraries



Emails

- ☐ Take adequate steps to protect and dispose of properly all personal data that they include in, or attach to, any email to be sent on a network
- ☐ Encrypt the email using certain methods are only protected during transmission but may be read by any person having access to the sender's or the recipient's computer
- ☐ Always use LU Campus Email to avoid sending sensitive data over public internet email



Data storage

- ☐ Store sensitive data on a secure network drive instead of a mobile device to prevent data leakage in case of losing the device
- ☐ Encrypt sensitive data before transferred into removable media or via email
- ☐ Conduct virus scanning to prevent data leakage

Knowledge check #4

What do you think?

What should be taken note of when using USB flash drives to save personal data?

- A. Use USB flash drives with built in encryption feature to ensure that personal data will not be leaked accidentally
- B. Sensitive personal data should not be saved in USB flash drives to avoid accidental leakage
- C. All of the above.

Source: <https://www.pcpd.org.hk/misc/training/index.html>

Knowledge check #4 (Cont'd.)

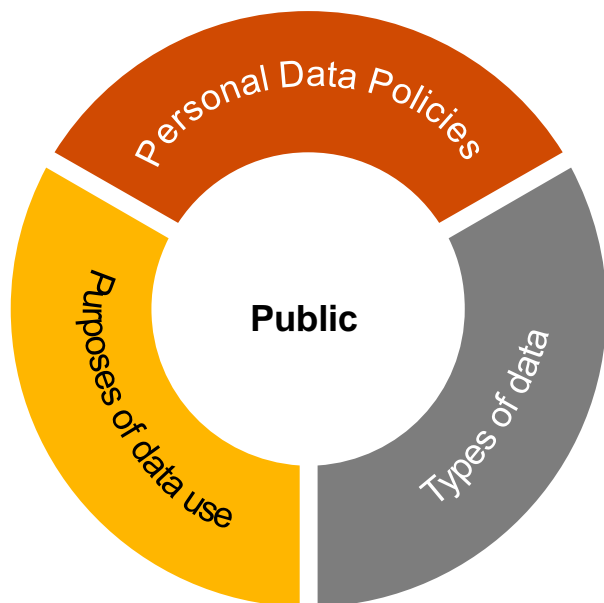
Answer and explanation:

The answer is C.

Although USB flash drives offers portability and large storage capacity, they are easily lost which may result in personal data leakage.

In complying with DPP4, data users should therefore adopt appropriate security measures to prevent accidental leakage of personal data, e.g. using USB flash drives with built in encryption feature and avoid saving sensitive personal data in USB flash drives.

DPP5 - Openness Principle



Data protection principle 5

DPP5 ensures that individuals are aware of the personal data privacy policy made by the University. This includes:

- statement of policy which expresses a data user's overall commitment in protecting the privacy interests of the individuals who provide information about themselves to the data user; and
- Statement of practices which include the kind of personal data held by the data user and the purposes of use.

The University may inform its clients of the "Privacy Policy Statement" through its website and pamphlets in order to comply with the requirements of DPP5.

The Privacy Policy Statement should include:

- Categories of personal data
- Purpose of collection and use of personal data
- Data retention policy
- Data securities measures
- Data breach handling
- Use of special tools such as cookies on websites
- Contact details for data access and data correction request

Knowledge check #5

Background

- To support daily company operations, staff A is arranged with a computer by the employer, and login password is only known by staff A. There is only one brief notice in the company stating that company computers could only be used for business by staff.
- Other than work / business, staff A also uses the computer for personal usage (e.g. browsing website, playing online games).
- On an urgent occasion staff A offered the login password to his/her supervisor.
- Supervisor of staff A suspects that staff A has used the company computer for personal use, hence investigated and collected the browsing history data and cookies without notifying staff A.

What do you think?

What could be the cause of violating DPP5 in this case?

- A. There was only one brief notice in the Organization stating that the computers of the Organisation could only be used for business by staff.
- B. The brief notice did not mention that the Organisation would log in employees' computers with their passwords to collect their browsing record.
- C. Staff A was not notified of the purpose of employee monitoring, monitoring activities that might be taken, or the use of data collected.
- D. All of the above.

Source: https://www.pcpd.org.hk/english/enforcement/case_notes/casenotes_2.php?id=2006C14&content_type=17&content_nature=0&msg_id2=318

Knowledge check #5 (Cont'd.)

Answer and explanation:

The answer is D.

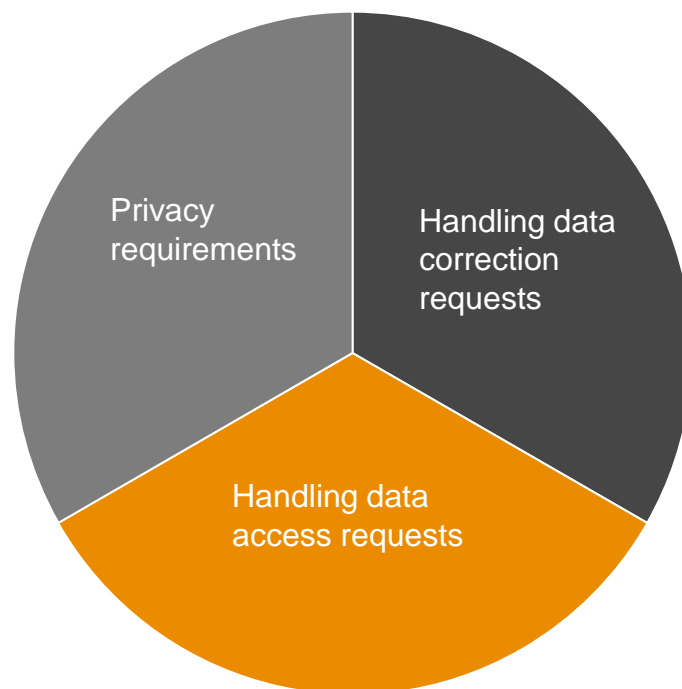
Although there was a brief notice, there was no policy nor notification on the employee monitoring arrangement; and instruction is limited that company computers could only be used for business by staff.

In complying with DPP5, data users should therefore take all the practicable steps to ensure that staff are made aware of the policy and practices of the company on employees monitoring by the employer. For instance:

- Establish the employee monitoring policy, including purpose of employee monitoring, the monitoring activities that might be taken, or the use of the data collected
- Inform employee on such arrangement and ensure the policy is readily available

DPP6 - Data Access & Correction Principle

According to DPP6 - Data Access & Correction Principle, an individual has the right to (i) **request access** to his/her own personal data held by a data user, and (ii) **request the correction** of personal data if the data is inaccurate



Knowledge check #6

What do you think?

What is the period that the data user should comply with the data access request upon receiving the data subject's request?

- A. Within 30 calendar days
- B. Within 40 calendar days
- C. Within 30 working days
- D. Within 40 working days

Source: <https://www.pcpd.org.hk/misc/training/index.html>

Answer and explanation:

The answer is B.

According to Section 19(1) of the Ordinance, a data user must comply with a data access request within 40 calendar days after receiving the request by –

- Informing the requestor in writing that the data user holds the data; and
- Supplying a copy of the data.

If the data user does not hold any personal data which is the subject of the request, the data user should inform the requestor in writing that the data user does not hold the data within 40 calendar days.

If the data user holds the requested personal data, but can rely on a ground under Section 20 of the Ordinance to refuse to comply with the data access request, the data user should inform the requestor in writing within 40 days of the refusal and the reasons of the refusal.

3

General Requirements

1. Personal Information Collection Statement
2. Data Access and Correction Management

Example of Application of the DPPs

During data collection, as a data subject, what do you want to know?

What kind of data?

What will the data to be used for?

Who will access the data?

How long will the data be kept?

Will my data be used for Direct Marketing?



Personal Information Collection Statement (“PICS”)

1 Purpose Statement

The personal data collected in this application form will be used by LU for recruitment and other employment-related purposes.

2 Obligatory or optional to provide data

Your provision of the personal data requested in the application forms is obligatory, except for the items marked as optional. **The application will not be considered if you fail to provide all of the required information.**

3 Classes of transferees

It may be provided to other organisations or agencies authorised by LU to process information for the purposes relating to recruitment by and employment

4 Access & correction right

Under the Ordinance, **you have a right to request access to and correction of your personal data held by LU.** Such request should be made in writing to the Data Privacy Officer of LU at the email address: dpo@LN.edu.hk.

Reminders – PICS

Reminders on Presentation of PICS:



Make sure the PICS is provided to the data subject on or before collecting his/her personal data.



The purpose statement is not too vague or too wide in scope.



User-friendly language and presentation are used.



The layout and presentation of PICS (including font size, spacing, underlining, use of headings, highlights and contrast) has been designed such that it is easily readable to individuals.



The PICS is presented in a conspicuous manner (e.g. the PICS is a stand-alone section and its contents are not buried among other information).

Preparation of the PICS

DPOs to ensure PICS prepared by his/her department/Faculty/unit is consistent with the requires under the Personal Data (Privacy) Ordinance, and submitting the PICS to the Chief DPO for review before adoption for use



Be transparent on the purpose of data collection and arrangement on personal data handling.



Personal data must be **used for the purpose for which the data is collected or for a directly related purpose**, hence before the usage of the personal data for a new purpose, the University should obtain voluntary and explicit consent from the data subjects by providing a separate PICS.

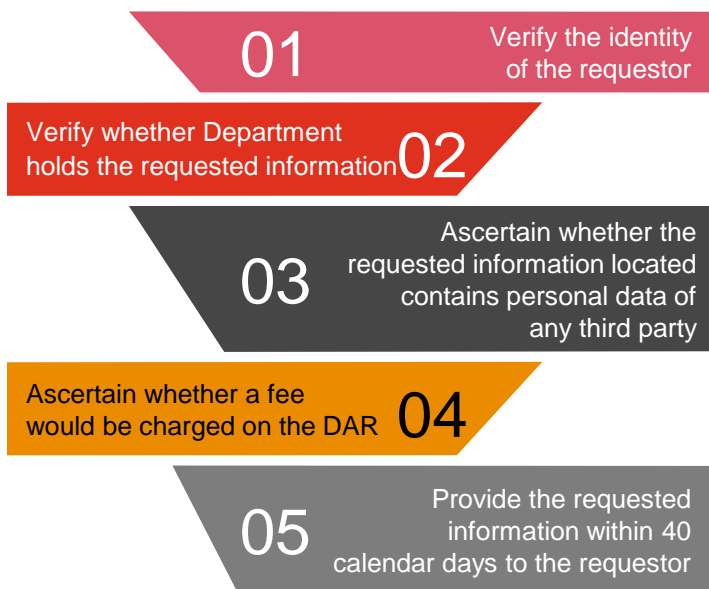
Respective DPOs should be responsible to ensure the existing PICS covers all current purposes of usage by the University/respective department/team.



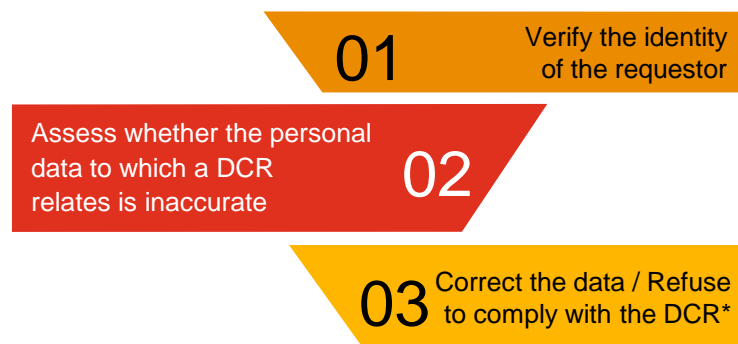
Please refer to the “Code of Practice for Handling Personal Data” for guidance and PICS sample.

Data Access and Correction Management

Steps for handling of Data Access Requests (DARs)



Steps for handling of Data Correction Requests (DCRs)



* For example, when the personal data relates to an “expression of opinion” and the data user is not satisfied that the opinion is inaccurate, the data user should make a note of the said data and attach a copy of the note to the notice of refusal to the requestor of the DCR.

Please refer to Guidance Note on “Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users” issued by the PCPD.

What can you do after receiving a data access / correction request?

Refer to Annex 4 of the Code of Practice on Handling Personal Data and communicate with the Chief DPO:

Procedures for Applications for Personal Data Access Request

1. The Chief Data Protection Officer maintains application procedures for access to and/or correction of personal data held by the University according to the provisions of the Personal Data (Privacy) Ordinance.
2. All enquiries concerning personal data access should be addressed to the Chief Data Protection Officer.
3. A data subject who wishes to make a request for access to or correction of his own personal data held by the University under the provisions of the Ordinance should complete an "Application for Personal Data Access Request" form (<http://www.ln.edu.hk/fupload/21018/Procedures-and-Applications-Form-for-Personal-Data-Access-Request.pdf>) obtainable from the ITSC, MB401, Patrick Lee Wan Keung Academic Building, Lingnan University, Tuen Mun, N.T., Hong Kong
4. The data subject should return the completed application form to the Chief Data Protection Officer in person, showing his student/staff card, and if not available, his HKID or passport for identification. Any requests on behalf of the data subject should be submitted with a written authorization and a copy of the data subject's Student/Staff ID card or HKID card/passport.
5. For data access request, the data subject is required to pay an application fee of \$150 at the Comptroller's Office and to complete a proforma indicating clearly the specific areas of data or documents to which they want to have access.
6. Upon showing the receipt of payment to the Chief Data Protection Officer, an acknowledgement slip will be issued to the data subject indicating that the request is accepted and the search will proceed.
7. The Chief Data Protection Officer will notify the data subject in writing of the outcome and/or progress of the request within 40 days from the date of submission.
8. A charge will be levied on the data subject for each request in accordance with the following schedule:

Photocopy of printed documents	\$5 per page
--------------------------------	--------------

9. If the request cannot be completed within the 40-day period, the data subject will be advised of the reasons for the delay and notified of a revised completion date.

Steps to Take in Refusing to Comply with a DAR

Examples where the University shall consider to refuse to comply with a DAR:

- (a) the data user is **not supplied with information** to satisfy the data user as to the **identity of the requestor**
- (b) the data user cannot comply with the request **without disclosing the personal data of a third party** – consider whether third party personal data can be redacted
- (c) where compliance with the request is for the time **being prohibited** under the Ordinance or any other ordinance

Step 1

- Give **written notice** and **reasons for refusal** to the requestor **within 40 calendar days**

Step 2

- Inform the requestor of the **name and address of the other data user** concerned in the notification of refusal, if there is another data user that controls the use of the data which prohibits the University from complying with the request

Step 3

- Keep a **log entry** containing the particulars of the reasons for the refusal of the request for **four years**

In addition, the University may also consider / rely on the following grounds to refuse to comply with a DAR under Section 20(3):

- (a) The request is **not in writing**
- (b) The University is **not supplied with information to locate** the requested data
- (c) The request is **not made in the DAR form** specified by the PCPD
- (d) the request follows two or more similar requests, and it is **unreasonable** for the University to comply with the request in the circumstances
- (e) another party **controls the use** of the requested data in a way that prohibits the University from complying with the request
- (f) The University is **entitled** under the Ordinance or any other ordinance not to comply with the request; or there is an **applicable exemption** provided for in the Ordinance from the requirement to comply with the request

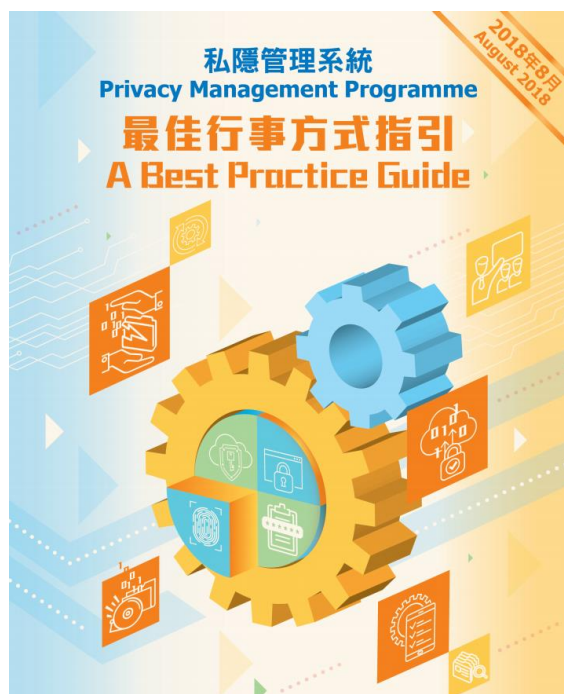
“



4

Privacy Management
Programme (“PMP”)

Privacy Management Programme

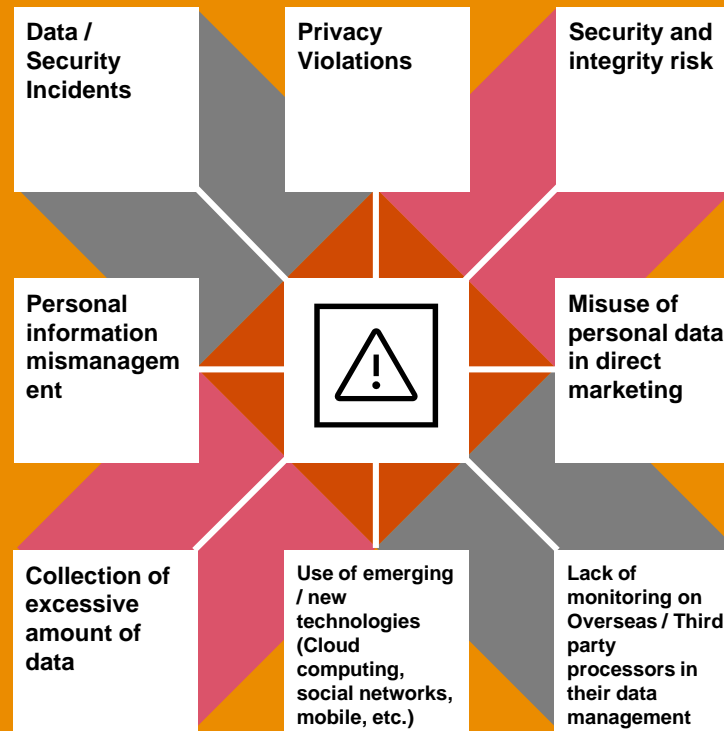


The PCPD published the **Privacy Management Programme – A Best Practice Guide** to outline what the Commissioner advocates as good approaches for developing a sound privacy management programme. The revised Guide was issued in August 2018.

A **PMP** serves as a strategic framework to assist an organisation in building a **robust privacy infrastructure** supported by an **effective on-going review and monitoring process** to facilitate compliance with the requirements under the Ordinance.

High level summary of key data privacy risks

Apart from meeting the requirements and changes in the Ordinance, below are some common privacy risks that the University may face:



The components of the PMP

Part A: Baseline Fundamentals

1. Organisational commitment

- Buy-in from the top
- Appoint Data Protection Officer / Data Protection Office (Personal Data Privacy Committee (PDPC))
- Reporting - Establish internal reporting mechanisms

2. Programme controls

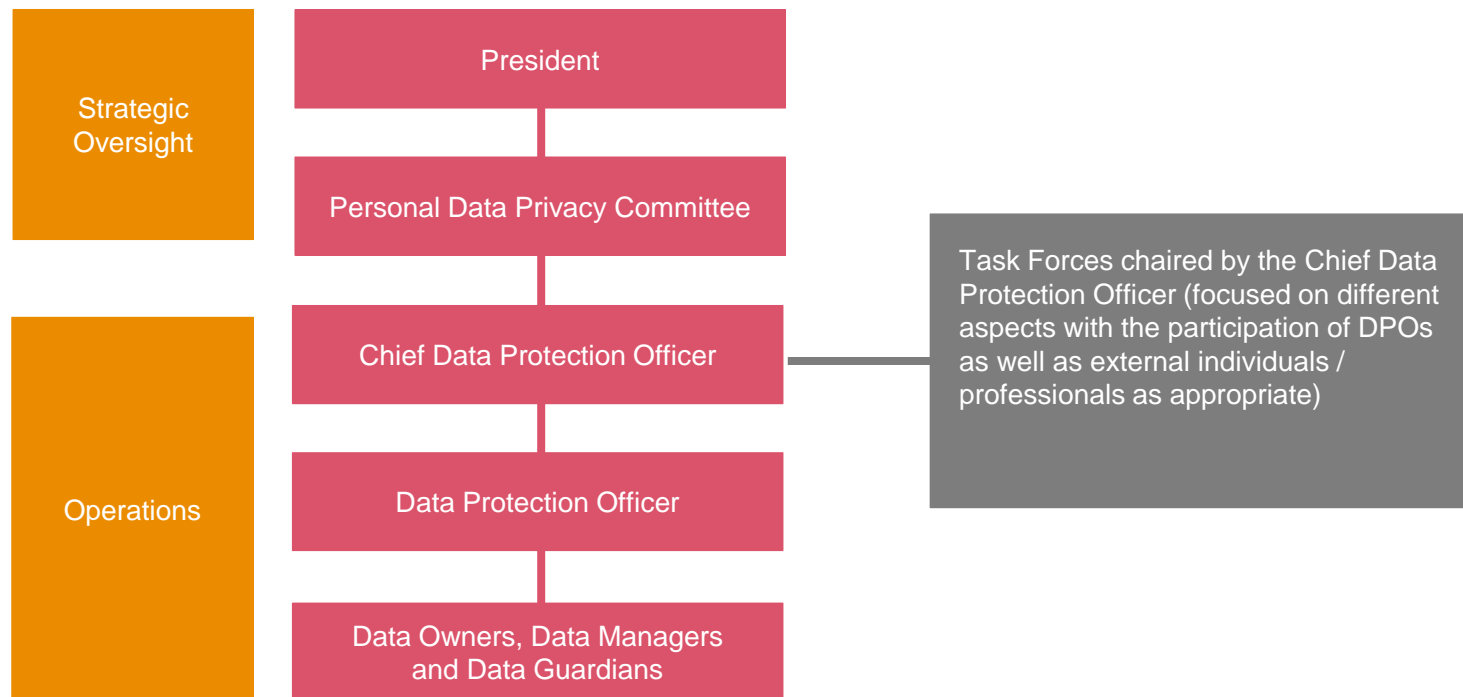
- Personal Data Inventory
- Policies
- Risk Assessments and perform regular review
- Training and Education Requirements
- Breach Handling procedures
- Data Processor Management
- Communication to employees and customers on personal data policies and practices

Part B: Ongoing Assessment and Revision

1. Develop an Oversight and Review Plan (i.e. by the PDPC)

2. Assess and Revise Programme Controls on a regular basis

The University's data privacy governance framework and reporting structure



Key Roles & Responsibilities of the DPO

01

Managing matters relating to data privacy of his/her own department/Faculty/unit, and representing his/her department/ Faculty / unit to communicate with the Chief DPO

02

Carrying out periodic risk assessments within his/her department/Faculty/unit and submitting the review report to the Chief DPO

03

Assisting the Chief DPO in carrying out the ongoing assessment and revision of the Privacy Management Programme

04

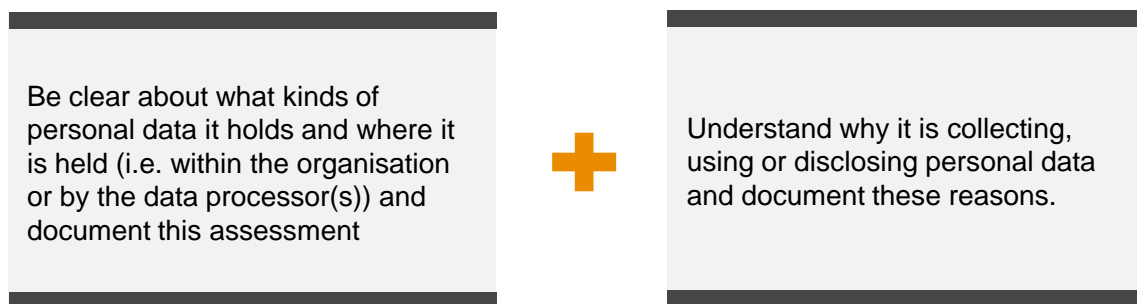
Updating personal data inventory of his/her department/Faculty/unit annually

05

Ensuring PICS prepared by his/her department/Faculty/unit is consistent with the requirements of the Personal Data (Privacy) Ordinance, and submitting the PICS to the Chief DPO for review before adoption for use

Programme Controls - Personal Data Inventory

Purpose of a personal data inventory:

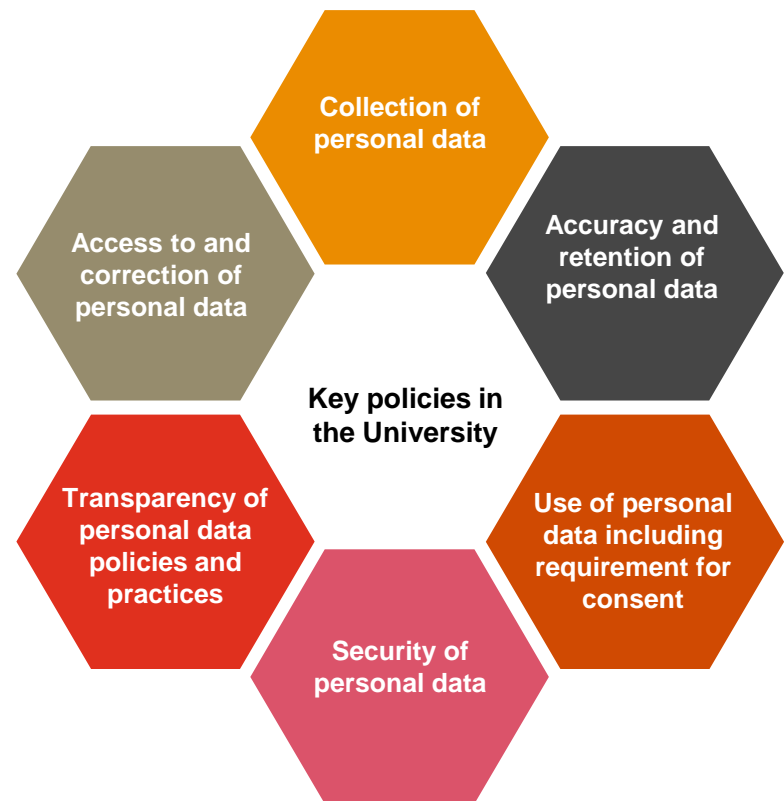
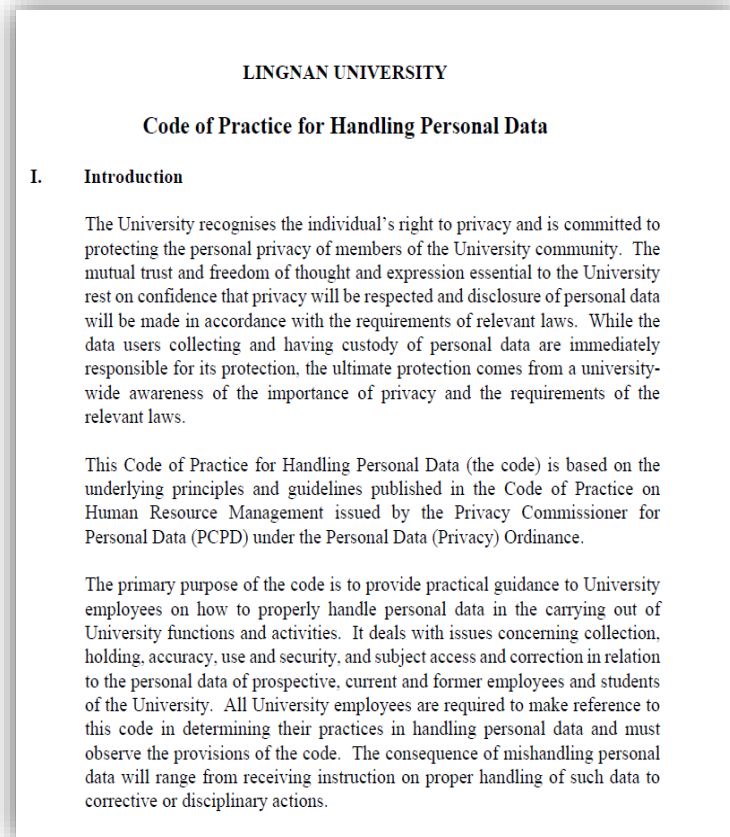


A personal data inventory review exercise, to be coordinated and monitored by the Data Protection Officer, should be conducted annually. There are five steps in performing a personal data inventory review exercise:



Programme Controls - Policies

The University has developed and documented **internal policies** in the Code of Practice for Handling Personal Data. It is made available to employees (i.e. intranet), all employees should be reminded of these policies and any updates periodically.



Programme Controls - Risk Assessments

What is the purpose of a risk assessment and when to perform?

Conducting periodic risk assessments is important to ensure that the policies and practices of the University are and remain compliant with the Ordinance.

Every year, the Chief DPO should **initiate all or select particular Sections/Teams** to participate in the periodic risk assessment. (Note: The decision of having (i) all teams; or (ii) selected teams to participate in the periodic risk assessment is subject to the University's organisational setup and the decision / direction of the Committee)

Examples of key considerations for the periodic risk assessment:

New initiatives/ projects developed	Data breach incidents	Complaints received	Data disposal	New data processor
E.g. Any new personal data handling processes? Any new systems implemented? Any changes to existing activities involving personal data?	E.g. Any data breach incident occurred? Are there any follow-up actions?	E.g. Any complaints about your Team/Section regarding personal data matters?	E.g. Any disposal exercise has been performed for all time-expired records without your Team/Section?	E.g. Any plan to engage or engaged new data processor to handle personal data on behalf of your Team/Section?

What if there are changes on how to handle personal data in your Team/Section/Department?

Definition of Privacy Impact Assessment (“PIA”)

A systematic process that evaluates the personal data privacy impact of the proposed changes on the handling of personal data or the launching of a new project, with the objective of preventing and/or minimising adverse impacts.

When should a PIA be undertaken?

- **Before the implementation** of a new project or a change of policy and practice
- When there is a **material change** to the regulatory requirements relating to personal data that may require corresponding changes in the process of handling personal data in order to comply with the new requirements
- **Before engaging data processors** to handle personal data on its behalf

Before conducting a PIA, the University should consider whether external consultants should be involved and engaged to provide an independent advice / assessment (e.g. complex / cross-border situations)



Factors for consideration:

- The **size** and **scope** of the change/project;
- The **types** and **amount of personal data** which may be involved;
- The **complexity** of the change/project (e.g. whether there is sharing of personal data with other parties/data processors, etc.);
- The involvement of **cross-border data transfer**; and
- The involvement of **third parties**.

Programme Controls – Training and Education

- 01** Introduction of PMP for new staff
- 02** Circulation of new/update data privacy policies and guidelines
- 03** Circulation of case materials (e.g. Risk mitigation measures, complaint cases)
- 04** Re-circulation of the PMP Manual and other data privacy policies and guidelines

Data Breach Handling Procedures



Programme Controls – Data Processor Management

What is a Data Processor?

A person who **processes personal data on behalf of another person** and does not process the data for any of the person's own purposes.

When the University shares personal data it controls with a third party to perform tasks in relation to that data on behalf of the University, this third party is then a “data processor”.

Examples of situations that might engage data processors:

- Carry out survey
- Input personal data into computer systems
- Scan documents which contain personal data
- Transfer/share confidential documents which contain personal data
- Process personal data e.g. a cloud service provider



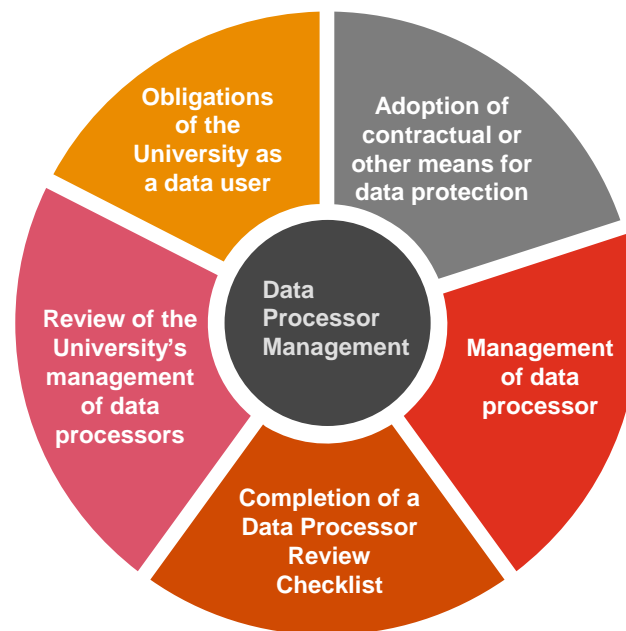
Any data processor engaged by the University?



What types of data have you been sharing with the data processor?



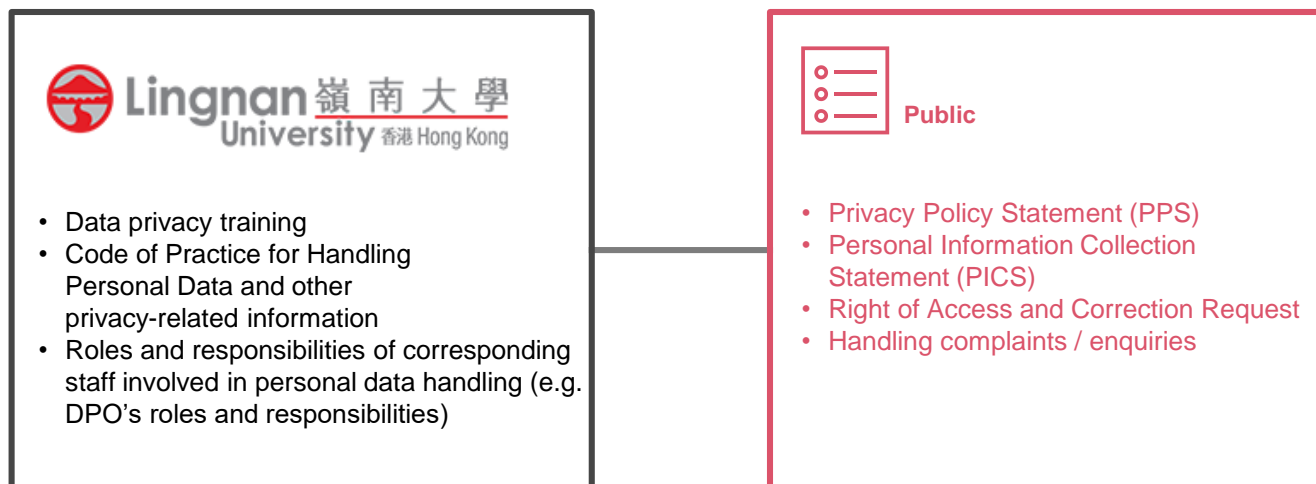
Any data protection clauses included in the agreement?



Programme Controls - Communication

Who and what to communicate?

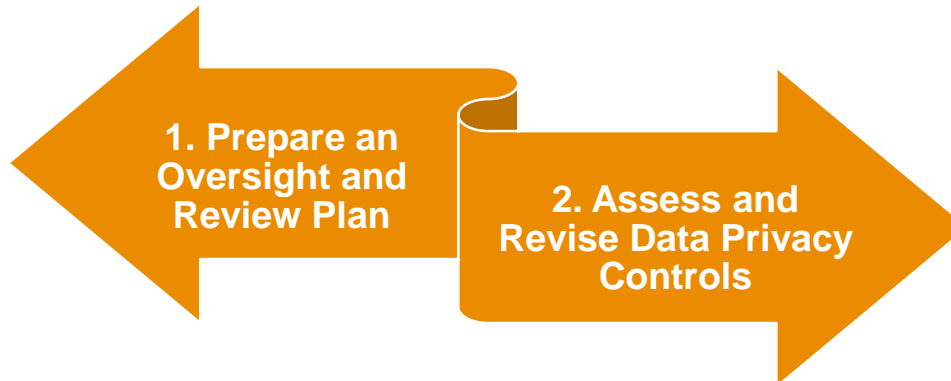
The University is taking all practicable steps to communicate its personal data policies and practices to the general public and its staff.



Oversight and Review Plan and Review of PMP's Effectiveness

How often should the assessment and revision of personal data policies and practices be carried out?

1. The Code will be subject to review annually by PDPC. Any variations and amendments to the document will be announced to members of the University in due course
2. Review coordinated by the secretary of the PDPC in the last quarter of each calendar year



5

Data Protection In Human Resources Management

1. Employer's liability
2. Recruitment
3. Current employee matters
4. Former employee matters

Employer's liability pertaining to the wrongful conduct of its staff or an appointed agent in handling personal data.



The University is liable in civil proceedings for any act or practice relating to personal data that is undertaken by:

- ☐ its employees in the course of their employment that is contrary to the provisions of the Ordinance, even if the employees undertook the act or engaged in the practice without the employer's knowledge or approval.
- ☐ a third party where the third party is engaged as an agent acting with authority (whether express or implied, and whether precedent or subsequent) on behalf of the employer.

Recruitment



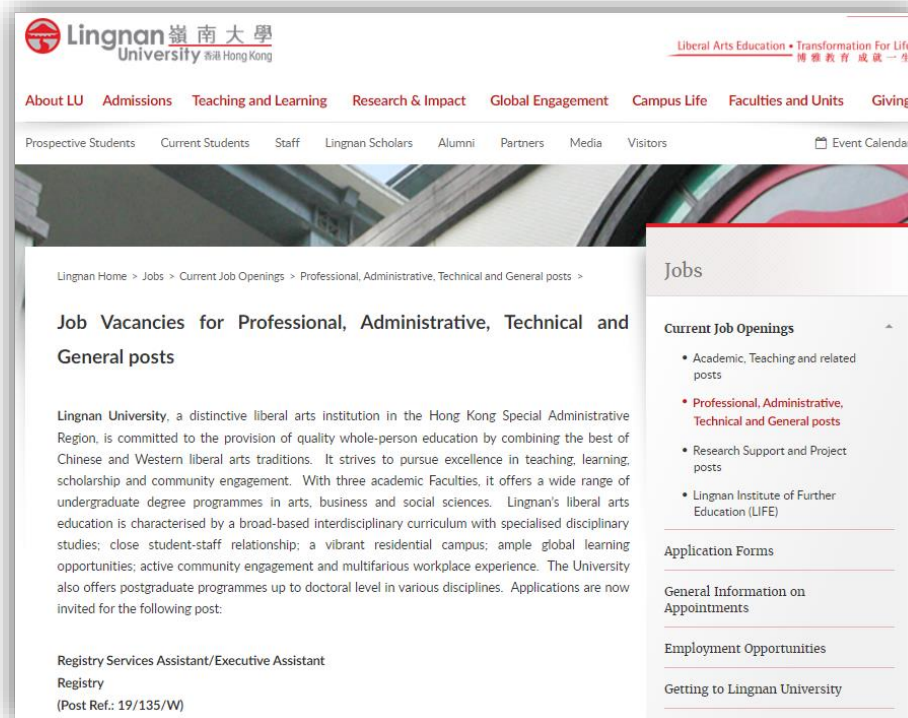
Recruitment – Advertisement

Definition of “blind” recruitment

A “blind” recruitment advertisement is one that **does not identify** either the employer or the recruitment agency acting on its behalf.

Factors for consideration in recruitment advertising

- ❑ The University **should not solicit** personal data from job applicants, e.g. their personal resumes, in a recruitment advertisement that **provides no identification** on of either the University or recruitment agency acting on its behalf.
- ❑ If it necessary to conceal its identity in recruitment advertisements, the University may ask the applicant to obtain an application form in the advertisement.
- ❑ Recruitment advertisements should inform applicants about the purposes for which their personal data is to be used



Recruitment – Collection of Personal Data from Job Applicants

Examples of things that an employer should do....

- Where an employer requires job applicants to fill in a job application form, either in a paper format or online on a web page of the employer's website, it should ensure that the PICS notification requirement is in compliance
- should specifically inform job applicants of the purposes(s) for collecting their personal data and the way(s) these data will be used on or before the collection.

Examples of things that an employer **should not do**...

- collect personal data from job applicants **unless** the purpose for which the data is to be used is **lawful**
- collect personal data from job applicants **unless** the data is adequate but **not excessive in relation to** the purpose of recruitment
- collect **a copy of the Hong Kong Identity Card** of a job applicant during the recruitment process **unless** and until the individual has **accepted an offer** of employment.

Recruitment – Collection of Personal Data When Processing Application

seeking more information for
selection assessment..?



Such supplementary information should be collected for :

- ☐ the purpose of assessing the suitability of potential candidates for the job,
- ☐ and the data collected should be relevant to the nature of the job.

seeking Personal References of
Job Applicants..?



☐ Consent have to be obtained from a potential candidate

Recruitment – Appointment vs Unsuccessful candidate

Upon Appointment/Acceptance by Candidate

- On appointment, the University may collect additional personal data from an employee and his family members (e.g. working for a competitor) for the purpose of employment, or to fulfil the lawful requirements (i.e. Inland Revenue / Immigration Ordinances) that regulate the affairs of the employer. Data collection should not be excessive (i.e. only ask whether or not the relative works in the same or a similar field).
- Personal data concerning the health condition of a selected candidate may be collected by means of a pre employment medical examination if the data directly relates to the inherent requirements of the job, and employment is conditional upon the fulfilment of the medical examination. However, such data should only be collected after the employer has made a conditional offer of employment to the selected candidate. Also to avoid excessive collection of health data, objectionable data such as genetic testing should not be collected.



Data of Unsuccessful Candidate to be destroyed

- Personal data of unsuccessful applicants are normally destroyed in accordance after the successful applicant(s) has/have formally accepted the offer(s) of appointment at the completion of the recruitment exercise.
- If the personal data of unsuccessful applicants are retained for future reference purposes, such data should not be kept for a period in excess of 24 months.

Current Employee – Collection of data

On or before collection of personal data from an employee, University should provide the employee with a Personal Information Collection Statement (“PICS”) pertaining to employment.

Data collected from employees and their family members

- ✓ Purposes are directly related to the employment
 - E.g. Claim of compensation or benefits when its necessary to ascertain the eligibility of the employee’s claim for compensation; Integrity Checking / Declaration of Conflict of Interest in relation to the inherent nature of the job and the University has a policy covering such practices; Medical Checking and Health Data which directly related to the assessment of continuance in employment
- ✓ Fulfilment of lawful requirement that regulate the affairs of the University

Data relating to Disciplinary proceedings, performance appraisal or promotion planning

- ✓ Purpose are directly related to the process concerned
- ✓ Such information should not be disclosed to a third party unless such party has legitimate reasons to have access to that data.

6

Q&A Session

Thank you!

pwc.com

This training has been prepared pursuant to an engagement contract between PricewaterhouseCoopers Limited and Lingnan University dated 15 March 2019 and is intended solely for the use and benefit of Lingnan University and may not be provided to or relied upon by any other person (including your advisors) for any purpose without our prior written consent. We accept no responsibility or liability whether in contract, tort, including negligence or otherwise to any other party, however arising, in connection with this training.

PricewaterhouseCoopers Limited expects to provide oral deliverables in conjunction with this training. PricewaterhouseCoopers Limited shall not be held responsible for oral advice unless PricewaterhouseCoopers Limited confirms such advice in writing. This document serves to summarise the views and opinions provided to you in our oral deliverable. Our oral deliverable may have placed greater emphasis on certain issues that arose during the discussion and this summary may not address or reflect every matter that was discussed. This document should be read in conjunction with our oral deliverable and is not considered complete without it.

The Services do not include the provision of legal advice and PwC makes no representations regarding questions of legal interpretation. The Client should consult with its attorneys with respect to any legal matters or items that require legal interpretation. Changes in the law or in regulations and/or their interpretation may take place after the date that our engagement commences, or may be retroactive in impact; we accept no responsibility for changes in the law, regulations or interpretation which may occur after the commencement of the Services.

© 2019 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.