

Data Privacy and Privacy Management Programme

23 September 2026

Office of Council and Court Secretariat and Legal

Seminar Agenda

Part 1

The Personal Data (Privacy) Ordinance (Cap. 486)

- Introduction and Key Definitions
- The Six Data Protection Principles and Case Study
- Consequences of Contravention

Part 2

Privacy Management Programme

- Overview and Purpose of PMP
- Governance Structure on Management of Personal Data
- Key Policies, Procedures and Programme Controls

Part 3

- Q & A

Part 1

The Personal Data (Privacy) Ordinance (Cap. 486)



Personal Data (Privacy) Ordinance (PDPO) – Overview

- ❖ Passed in 1995 and took effect from December 1996 (except certain provisions)
- ❖ Applicable to both the private and the public (government) sectors
- ❖ 2012 amendments: direct marketing
- ❖ 2021 amendments: doxxing

Personal Data (Privacy) Ordinance – An Introduction (Cont'd)

- ❖ Technology-neutral
- ❖ Principle-based, i.e. the 6 data protection principles
- ❖ Not exhaustive statements of the law
 - ❖ Check the guidance notes issued by the Privacy Commissioner
 - ❖ Check the wording of the Ordinance
- ❖ Seek legal advice if in doubt

Hierarchy of appellate authority



Key Definitions

Data Subject

- the individual who is the subject of the personal data concerned

Data User

- a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data

Data Processor

- a person who processes personal data on behalf of another person (a data user)

Key Definitions – “Personal Data”

- ❖ “Personal data” means any “data” -
 - (a) relating directly or indirectly to a living individual;
 - (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
 - (c) in a form in which access to or processing of the data is practicable.
- ❖ “Data” means: any representation of information (including an expression of opinion) in any document, and includes a personal identifier.

Categories of Personal Data

- ❖ Email address
 - ❖ “lhy-aastock@per.com.hk” → not personal data (**AAB No. 25/2008**)
 - ❖ Abbreviated name “TL Lau” together with an email address containing pseudonym → not personal data (**AAB No. 25/2012**)
- ❖ IP address → not personal data (**AAB No. 16/2007**)
- ❖ **Caveat:** Totality approach –
 - ❖ read together with other information controlled by the data user
 - ❖ whether practicable to ascertain the identity
- ❖ In practice, student’s email address (s20123456@life.hkbu.edu.hk) - treated as personal data

Categories of Personal Data (Cont'd)

❖ Views and opinions –

(a) *Wu Kit Ping* [2007] 4 HKLRD 849:

- Views and opinions may constitute personal data if relate to the data subject
- e.g. Doctor's opinion about a patient's medical condition

(b) AAB No. 28/2010: Views and opinions expressed by the marker on another person → not personal data the marker

Types of Personal Data collected and kept by HKBU

(1) Identification and personal information

name

date of birth

gender

identity card/passport details

visual and audio recordings

photographic images

(2) Contact details

address

telephone number

email address

social media account

emergency contact

(3) Data provided by the data subjects or third parties

bank account number

credit card account number

(4) Evaluative data created by the University

academic results

assessment records

Types of Personal Data collected and kept by HKBU (Cont'd)

(5) Information collected by means of cookies

webpage(s) visited

options chosen

links clicked to access

(6) Other personal data applicable to the data subjects in Section B(III) of the PPS & PICS

(7) Additional personal data set out in any bespoke PICS of the University

The Six Data Protection Principles (DPPs)



The Six Data Protection Principles (DPPs)

DPP 1

Purpose and Manner of Collection

DPP 2

Accuracy and Duration of Retention

DPP 3

Use of Data

DPP 4

Data Security

DPP 5

Openness and Transparency

DPP 6

Access and Correction

The 6 DPPs (Cont'd)

- ❖ Section 4 of PDPO: A data user shall not do an act that contravenes a DPP
- ❖ Contained in Schedule 1 to the PDPO
- ❖ Outline how data users should collect, handle and use personal data
- ❖ Breach of DPP not an offence

DPP 1 – Purpose and Manner of Collection

- ❖ Personal data shall only be collected for a **lawful** purpose **directly related to a function or activity** of the data user
- ❖ The data collected should be **necessary and adequate** but not excessive for such purpose
- ❖ The means of collection should be **lawful** and **fair**

DPP 1 – Purpose and Manner of Collection (Cont'd)

Inform data subjects at the time of data collection of:

1. the purpose(s) for which the data is to be used
2. the classes of person to whom the data may be transferred
3. whether it is obligatory or voluntary to supply the data, and where it is obligatory to supply the data, the consequences of not supplying the data
4. the rights to request access to and correction of the data
5. contact details of the individual who is to handle such data access and correction request

Incorporate the link to the PPS & PICS before collecting personal data
(<https://bupdpo.hkbu.edu.hk/policies-and-procedures/pps-pics/>)

Making audio and/or video recordings of meetings/hearings

- ❖ See CCSL's memo circulated annually
- ❖ Practice to be adopted in making audio/video recordings
- ❖ Applies to the following meetings/hearings:
 - ❖ Any academic or disciplinary matters of student(s)
 - ❖ Any disciplinary matters of staff member(s)
 - ❖ Any complaints or grievances of student(s) or staff member(s)
- ❖ Consider whether it is justifiable to make the recording

Making audio and/or video recordings of meetings/hearings (Cont'd)

❖ The presider shall ensure:

- ❖ data subjects be notified of the recording and its purpose;
- ❖ ensure **the following statement is captured** at the **beginning** of the recording:

“This is a [meeting/hearing] on [date] at [time] with [names of the relevant student(s)/staff member(s) and other participant(s)]. This [meeting/hearing] is being recorded. The purpose of the recording is [state the purpose].”

- ❖ where appropriate, take **additional measures** to further the objectives of the DPPs

DPP 1 – Purpose and Manner of Collection (Cont'd)

Case Study

Is there any “collection” in the first place?



(photograph taken at the sharing session, “*In dialogue with Dr. Andy Lau*” on 10 August 2026, which was attended by over 700 HKBU students and staff)

Eastweek Publisher Ltd vs Privacy Commissioner for Personal Data [2000] 2 HKLRD 83

- ❖ The magazine took photos taken randomly on the street
- ❖ Comment on her fashion sense: “The complainant was referred to as “Japanese Mushroom Head”, apparently because of what the reporter called “her mushroom hairstyle”
- ❖ Complainant remained anonymous

Court’s ruling : “*the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify*”

DPP 1 – Purpose and Manner of Collection (Cont'd)

Case Study

Use of telephoto lens to take photo of private residence

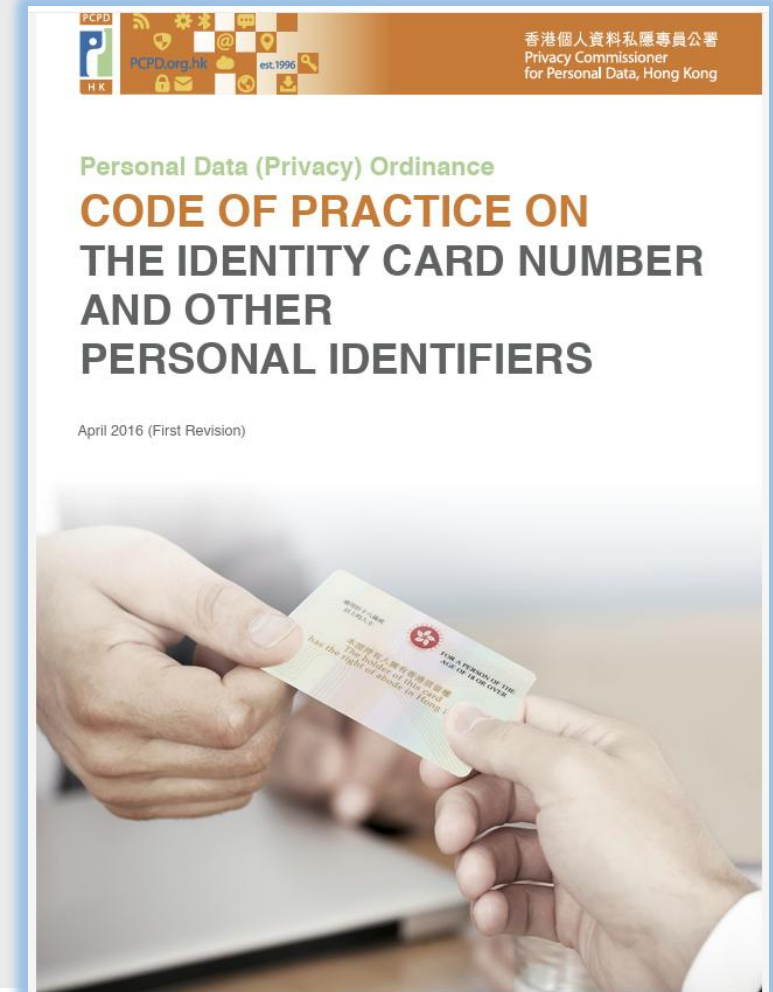
- ❖ Use of 70-200mm lens, 300mm lens and 1.4x magnifier
- ❖ Taking photo of activities inside a private residence from 80m
- ❖ Reasonable expectation of privacy at residence
- ❖ Unfair collection of personal data
- ❖ The magazine ordered to delete the photos and establish privacy guidelines

DPP 1 – Purpose and Manner of Collection (Cont'd)

Case Study

Driving school's collection of enquirer's HKID card

- ❖ Facts of the case :
 - ❖ X enquired on course details and fees;
not applying for course enrollment
 - ❖ staff requested X to provide HKID card
- ❖ PCPD's views : **premature collection** of **sensitive data**
 - ➡ contravened DPP 1
 - ➡ school apologised to X and destroyed HKID card number



DPP1 - PCPD's code of practice on HKID number

- ❖ Paragraph 2.2: *“the data user should consider whether there may be any less privacy-intrusive **alternatives** to the collection of such number, and should wherever practicable give the individual the option to choose any such alternative in lieu of providing his HKID Card number”*
- ❖ Paragraph 2.3: *“should not collect HKID Card number except... correct identification ... is or will be necessary for the advance of interest of the holder or to safeguard against damage or loss ...which is more than trivial”; e.g.:*
 - ❖ To ascertain patient's identity;
 - ❖ To ascertain the identity of the customer in a car-rental business (cf. rental of a bicycle)

DPP 2 – Accuracy and Duration of Retention

- ❖ All practicable steps shall be taken to ensure personal data is:
 - ❖ Accurate; if not, data should not be used or should be erased
 - ❖ not an absolute requirement
 - ❖ i.e. four-eye principle
- ❖ Data not kept longer than necessary
- ❖ For data processor:
 - ❖ adopt contractual or other means to ensure compliance with the retention requirement
 - ❖ select reputable data processor

DPP 2 – Accuracy and Duration of Retention (Cont'd)

- ❖ Personal data shall be deleted in a timely manner after the retention period set out in the University's *Privacy Management Programme* (PMP) :

Personal data of
job applicants

- Not more than 2 years

Personal data of
departed staff

- Not more than 2 years

Personal data of student
applicants (who are
unsuccessful or decline
the offer of admission)

- Not more than 2 years after completion of the relevant admission exercise

Personal data of
student applicants
(who have paid the
admission deposit)

- Not more than 7 years after completion of the relevant admission exercise

Delete,
except with
subsisting
reasons to
retain the
data for a
longer
period

DPP 2 – Accuracy and Duration of Retention (Cont'd)

Case Study

Inland Revenue Department sending tax demand note to a wrong address

- ❖ X, a taxpayer, did not receive the tax demand note
- ❖ IRD has wrongly sent X's tax demand note to another taxpayer
- ❖ PCPD: multiple human error; sensitive data warrants higher degree of care
- ❖ Remedial actions by IRD:
 - ❖ Updating the computer system to enable counter-checking before address update
 - ❖ Conducting random check on at least 10% of address amendments
 - ❖ To trace the tax demand notes delivered to the wrong address

DPP 2 – Accuracy and Duration of Retention (Cont'd)

❖ Examples:

- ❖ Personal data **transferred from another Unit** should be disposed of immediately after use
- ❖ Personal data requested in **invitations** should be disposed of once the event have been held
- ❖ **Audio recordings** of a meeting should be destroyed in accordance with the University's relevant regulation
- ❖ **Survey questionnaires** should be destroyed once the report has been prepared

DPP 3 – Use of Data

- ❖ Personal data shall only be used for :
 - ❖ the purposes **for which the data is collected**; or
 - ❖ **directly related** purposes
- ❖ Other uses – data subject's express and voluntary **consent** is required
 - ❖ Unless an exemption under the PDPO applies, for example :
 - ❖ crime prevention or prosecution
 - ❖ prevention of seriously improper misconduct
 - ❖ Prevention of serious harm to health
 - ❖ Life-threatening situations

DPP 3 – Use of Data (Cont'd)

❖ AAB No. 54/2014

- ❖ “Webb-site.com” – “search people” function
- ❖ X involved in divorce proceedings; her name searchable on the website
- ❖ Comparing the purposes
 - ❖ The website: reporting and publication for general use
 - ❖ Judiciary: reporting judgments and legal principles
- ❖ Data used for a new purpose → contravention of DPP 3

DPP 3 – Use of Data (Cont'd)

❖ AAB No. 41/2006

- ❖ A resident reported smell outside her flat to management company
- ❖ Management company pass her personal data to the Police
- ❖ Issue: whether personal data used for a new purpose?
- ❖ AAB ruling: Provision to the Police is a “directly related purpose” and also justified under section 58 exemption to investigate “deliberate nuisance”

DPP 3 – Use of Data (Cont'd)

- ❖ Direct marketing – a new purpose
- ❖ Definition of “direct marketing”:
 - ❖ the offering, or advertising of the availability, of goods, facilities or services; or
 - ❖ the solicitation of donations or contributionsthough **direct marketing means**
- ❖ Definition of “*direct marketing means*” :
 - ❖ sending information or goods, addressed **to specific persons by name** (向指名特定人士), by mail, fax, electronic mail or other means of communication; or
 - ❖ making telephone calls to specific persons

DPP 3 – Use of Data (Cont'd)

- ❖ Examples of “direct marketing” generally:
 - ❖ Bank sending promotional materials or donation forms through the monthly statement mailed to customers (Note: monthly statements are mailed directly to individual customers **by name**)
 - ❖ Beauty salons contacting **specific individuals by phone** to offer free beauty treatments;
 - ❖ Telecommunications service providers contacting existing customers by phone to promote upgraded services;
 - ❖ Professional organisations attaching promotional offers to newsletters mailed to their members;

DPP 3 – Use of Data (Cont'd)

- ❖ Examples of “direct marketing” in the university:
 - ❖ emails to students, alumni or donations for fundraising purpose; or
 - ❖ emails to promote fee-paying courses or events
 - ❖ emails to promote fee-paying services (even at a below-cost rate);
 - ❖ emails to promote university souvenirs
 - ❖ Examples of promotion activities **not** regarded as “direct marketing”
 - ❖ Banks sending supermarket vouchers to existing customers **as a gesture of appreciation**;
 - ❖ Service providers sending SMS to existing customers informing them of their impending contract expiration and providing their enquiry hotlines, i.e. a form of after-sales services;
 - ❖ Promotional mailings sent to an address or “resident” of an address **without addressing specific persons by name**;
- **Catching promotion of fee-paying goods and services**

DPP 3 – Use of Data (Cont'd)

- ❖ Consent prior to direct marketing
 - ❖ No objection (e.g. not checking the box indicating objection); OR
 - ❖ Express consent (e.g. checking the box indicating agreement to direct marketing)
- ❖ Appendix C to PMP – sample consent form

If you **do not wish** the University to use or provide your permitted kinds of personal data to the permitted classes of transferees for use in direct marketing as described below, **you should put a tick in the box below. Please note that this will result in your ceasing to receive some of the information and materials which the University has in the past been providing to its data subjects, although such information may still be accessed should you voluntarily search for it on the University's website.**

☐ I do not wish the University to use or provide to other persons for use the permitted kind of personal data for direct marketing.
- ❖ Right to opt out anytime

DPP 3 – Use of Data (Cont'd)

(HK01, 17 November 2017;
updated on 11 February 2025)

❖ Penalty

- ❖ Fine up to \$500k and imprisonment of 3 years for some offences
- ❖ Fine up to \$1 million and imprisonment of 5 years for other aggravated offences (e.g. for gain)

香港01 港聞 娛樂 酒店優惠碼 天氣消息 即時 熱榜 國際 中國 科技 生活 更多

港聞 / 社會新聞

理財顧問用政府電話簿搵客 違私隱條例 罰款2萬元

撰文：陳宇軒
出版：2017-11-17 16:56 更新：2025-02-11 23:38

在Google 追蹤《香港01》

一名案發時任職康宏資產管理有限公司的理財顧問疑透過公開的政府電話簿，致電在政府相關機構工作的人員，向其推銷投資產品，該名人員遂向個人資料私隱專員公署投訴，公署其後向理財顧問提出兩項控罪，理財顧問今（17日）承認控罪，被判罰款共2萬元。公署提醒即使個人資料是來自公共領域，如公開的政府電話簿，仍是受條例保障。

公署：公共領域資料亦受條例保障

公署提醒，在條例下的直銷條文規定資料使用者在未取得當事人的同意前，不可以將其個人資料用於直銷用途，資料使用者須告知資料當事人擬使用哪一種類的個人資料、將會進行促銷的貨品或服務類別，並取得有效同意，提供回應途徑，讓該資料當事人表明同意與否。公署又指，即使個人資料是從公共領域，如公開的政府電話簿所取得，仍然受條例保障。

DPP 4 – Data Security

- ❖ The personal data shall be kept securely
- ❖ All practicable steps shall be taken to protect the personal data against unauthorised or accidental access, processing, erasure, loss or use
 - ❖ Kind of data; possible harm
 - ❖ Physical location of data storage
 - ❖ Security measures relating to storage
 - ❖ Secure transmission of data
- ❖ Common security issues
- ❖ If data processor is engaged : adopt contractual or other means to ensure that the data processor comply with the security requirements

DPP 4 – Data Security (Cont'd)

- ❖ Staff members shall strictly follow the relevant University's policies / guidelines:
 - ❖ *Data Governance Policy*
 - ❖ *Data Leakage Prevention Policy*
 - ❖ *Staff Handbook of Information Security*
 - ❖ *Personal Data Breach Protocol* –
 - ❖ Containment measure
 - ❖ Report to CCSL

DPP 5 – Openness and Transparency

- ❖ All practicable steps shall be taken to ensure that a person can:
 - ❖ ascertain a data user's **policies and practices** in relation to personal data;
 - ❖ be informed of the **kind** of personal data held by a data user;
 - ❖ be informed of the main **purposes** for which personal data held by a data user is or is to be used.
- ❖ The University's PPS & PICS
(<https://bupdpo.hkbu.edu.hk/policies-and-procedures/pps-pics/>)

PPS & PICS

PRIVACY POLICY STATEMENT AND PERSONAL INFORMATION COLLECTION STATEMENT (PPS AND PICS)

[Personal Data Protection](#) / [Policies and Procedures](#) / [Privacy Policy Statement and Personal Information Collection Statement \(PPS and PICS\)](#)

[Home](#)

[Foreword](#)

[Policies and
Procedures](#)

[Departmental
Personal Data Privacy
Manager](#)

[Useful Links](#)



香港浸會大學
HONG KONG BAPTIST UNIVERSITY

Privacy Policy Statement
and
Personal Information Collection Statement
(PPS and PICS)

PPS & PICS: Types of personal data

Types of personal data applicable to all data subjects

1. Types of personal data

Your personal data collected or held by us includes:

	Types	Examples (illustrative only)
(1)	identification and personal information	• name • date of birth • gender • identity card/passport details • visual and audio recordings • photographic images
(2)	contact details	• address • telephone number • email address • social media account • emergency contact
(3)	provided by you or third parties (e.g. spouse, employer or parents/guardian) to us	• bank account number • credit card account number
(4)	evaluative data created by us (including our staff members, agents or service providers)	• academic results and qualifications • assessment records
(5)	information collected by means of cookies (when you access our website, online applications or apps)	• webpage(s) visited • options chosen • links clicked to access
(6)	other personal data applicable to you in Section III	
(7)	additional personal data set out in any Bespoke PICS	

PPS & PICS: Types of personal data

3. Applicants for admission to the University and its related bodies

(1) Additional personal data collected or held by us:

(a)	proof of address
(b)	bank account information
(c)	family data
(d)	educational background
(e)	professional body associations, qualifications and work experience
(f)	academic transcripts
(g)	test results and testimonials
(h)	academic and job references
(i)	records of assessment and review
(j)	scholarships, awards and financial aid records
(k)	medical or health-related information
(l)	other information provided by you in the admission process

4. Students and alumni members

(1) Additional personal data collected or held by us:

(a)	information provided by you or collected by us during your admission application and admission process and such updated or additional information during the course or after completion of your studies (e.g. regarding employment following graduation)
(b)	study history (including information on courses, exchange programmes, internships, placements, practicums and other training undertaken)
(c)	study records (including programme details, years of study, academic status, qualifications conferred and other attainments)
(d)	academic work, test results and testimonials
(e)	records of assessment and review (e.g. academic grades and results)
(f)	records of extracurricular activities and other achievements
(g)	scholarships, awards and financial aid records
(h)	medical or health-related information
(i)	other activity records (e.g. membership of student bodies, and disciplinary and counselling records)
(j)	employment and career information
(k)	credit rating data and financial (including bank account) information
(l)	nationality, racial or ethnic origin, religious or similar belief
(m)	information relating to criminal or civil proceedings involving you as a party/witness

PPS & PICS: Purposes for which personal data is used

General purposes applicable to all data subjects

2. Purposes for which your personal data is collected

The purposes for which data relating to a Data Subject may be used vary depending on the nature of the Data Subject's relationship with the University. In general, the personal data you provide to us will be used for the following purposes from time to time:

(1)	our provision of services
(2)	our administration, management and recordkeeping
(3)	communication and delivery of information and invitations to you
(4)	teaching, research (including facilitating open access), quality assurance, surveys, review or statistical analysis
(5)	promotion of the University's academic offerings or institutional events, facilities and services, and related publicity activities
(6)	recognising, documenting and publicising your academic, professional, community or other achievements and contributions, as well as your participation in institutional events and academic activities
(7)	implementation of and monitoring compliance with our policies and procedures
(8)	our management (including use, protection and security) of the University's properties (including accommodation) and facilities
(9)	protection of the personal safety and health of the University community
(10)	direct marketing to which you have consented
(11)	provision of referrals, references or recommendations
(12)	handling your complaints or enquiries
(13)	other purposes applicable to you stated in Section III

PPS & PICS: Purposes for which personal data is used

Applicants for admission to University

(2) Additional purposes for which your personal data may be used:

(a)	serve as a basis for selection for admissions and consideration of the award of scholarships
(b)	obtain references and recommendations relevant to your application for admissions
(c)	manage the application account and process the application
(d)	identify possible multiple applications
(e)	obtain records of existing and previous studies and activities at the University and other institutions
(f)	verify your identity, public examination results, qualifications, academic records and, where applicable, work experience
(g)	facilitate communication for admission-related matters
(h)	conduct statistical analysis, research, surveys, quality assurance and review
(i)	process a student visa application, if applicable

If your application is not accepted, your personal data provided during the admission process will be retained and thereafter erased according to our prevailing policy.

Students and alumni members

(2) Additional purposes for which your personal data may be used:

(a)	provide access to and usage of our facilities (whether physical or electronic, such as online applications and apps) and properties (e.g. student accommodation)
(b)	inform and register you for events or courses organised by the University
(c)	enable academic and administrative communications
(d)	provide study, academic, student welfare and accommodation services
(e)	facilitate enquiry or investigation in academic integrity and general conduct
(f)	assess academic progress and attainment (e.g. completion or graduation requirements)
(g)	recognise your academic and other achievements (e.g. announcements at award or graduation ceremonies and publications in related event programmes)
(h)	consider needs for financial aid and special educational support
(i)	provide academic transcripts, academic references, testimonials or verify qualifications to you or to third parties (such as academic institutions and your prospective employers) to whom you have consented
(j)	report graduate employability
(k)	communicate to you University news, activities, initiatives, publications, information and other important notices
(l)	send membership invitations and deliver information about activities organised and/or promoted by student bodies and organisations and teaching units to you
(m)	process the application or extension of student visa, if applicable
(n)	keep in touch with you as an alumni member
(o)	communicate to you information about alumni activities, University news, activities, initiatives and publications

DPP 6 – Access and Correction

- ❖ A data subject is entitled to:
 - ❖ ascertain whether a data user **holds** his or her data
 - ❖ **access** to their own personal data
(*Data Access Request Form* provided by the PDPO)
 - ❖ **correction** of their own personal data

DPP 6 – Access and Correction (Cont'd)

- ❖ Procedures for handling Data Access Request (DAR) :
 - ❖ Check the identity proof of the requestor (e.g. student/staff ID card, HKID Card, passport)
 - ❖ Existence of personal data of other individuals is not a reason of refusal → should be **redacted** (*Wu Kit Ping [2007] 4 HKLRD 849*)
 - ❖ **Common redactions**: names, job titles, signatures of other persons appearing in the documents – *AAB No. 15/2012*)
 - ❖ Fees to be charged should not be excessive
 - ❖ Process the DAR **no more than 40 calendar days** after receiving it; if payment of fees would extend beyond the deadline → inform the requestor (*AAB No. 14/2024*)

DPP 6 – Access and Correction (Cont'd)

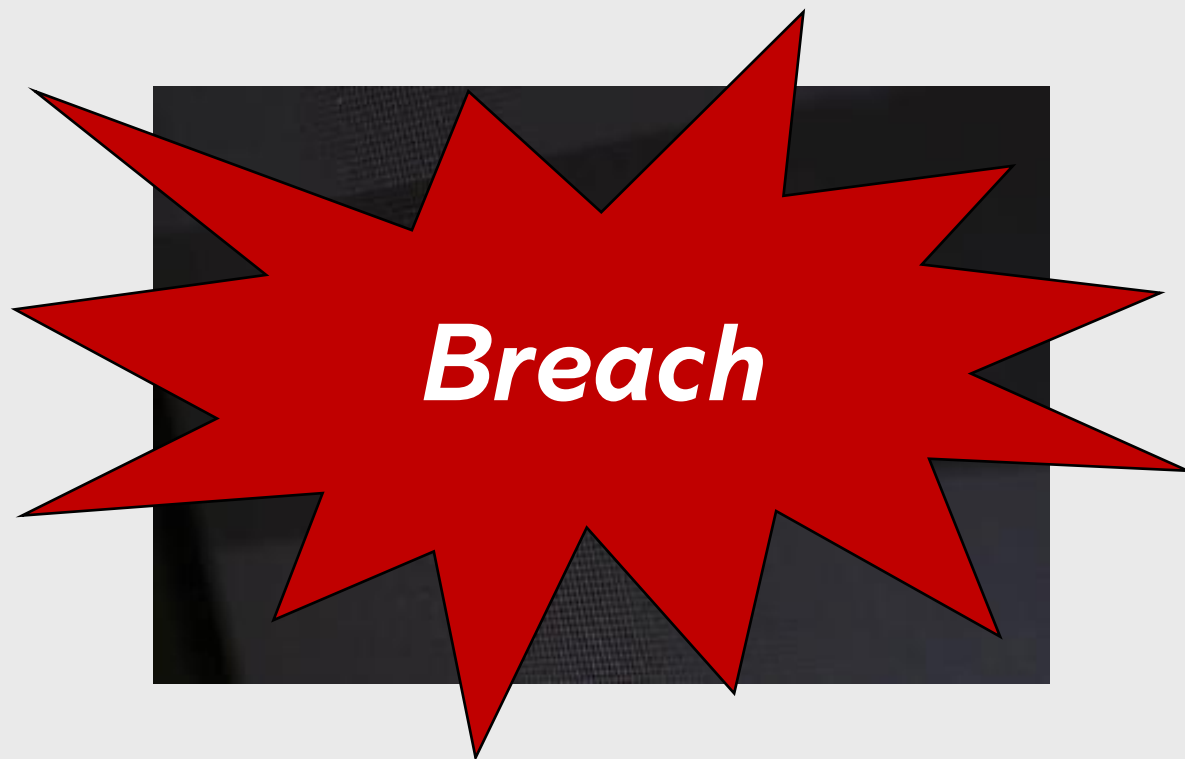
- ❖ Request for “all personal data”
 - ❖ Data user may seek clarification
 - ❖ Requestor shall supply information to enable the data user to locate the relevant data
 - ❖ **Test:** whether it is reasonably practicable for the data user to extract “all personal data” as requested
 - ❖ Data subject has no right to demand an exhaustive list of personal data
- ❖ Only entitled to have a copy of the data, **no right to obtain** a copy of the document which contains the data (*Gotland Enterprises Ltd* [2007] 1 HKLRD 226; *Wu Kit Ping* [2007] 4 HKLRD 849)
- ❖ Documents compiled as part of the “internal workflow” or “complaint handling” → Generally no need to disclose (*AAB No. 20/2013*)
- ❖ **Please see legal advice on individual cases**

DPP 6 – Access and Correction (Cont'd)

❖ Responsible units of data access and correction:

Group of Data Subjects	The relevant Unit(s)
Job applicants, current and former staff members	Human Resources Office
Students (including applicants and current students)	Academic Registry, Graduate School or Office of Student Affairs
Alumni	Alumni Affairs Office
Donors	University Advancement Office
Patients	Clinical Division of the School of Chinese Medicine
Other data subjects	DPDPM of the relevant Unit

Consequences of Contravention



Consequences of Contravention

- ❖ Contravention of a DPP is not an offence *per se*, **but** contravention of certain provisions of the Personal Data (Privacy) Ordinance is an offence
- ❖ The Commissioner may carry out criminal investigation and institute prosecution for relevant offences

Fine



Imprisonment



Consequences of Contravention (Cont'd)

❖ Appendix A of the PMP : list of offences under the PDPO

- ❖ Section 26: failure to take all practicable steps to erase personal data no longer required for the purpose for which the data was used (max fine: \$10,000)
- ❖ Section 35E: using personal data in direct marketing without data subject's consent (max fine: \$500,000; max imprisonment: 3 years)
- ❖ Section 35G: failure to comply with an opt-out request for direct marketing (max fine: \$500,000; max imprisonment: 3 years)
- ❖ **Section 50B: making false statement to the Privacy Commissioner marketing (max fine: \$10,000; max imprisonment sentence: 6 months)**
- ❖ Section 64: doxxing offence (max fine: \$1 million; max imprisonment: 5 years)



Media Statement

Date: 4 December 2014

A Person was sentenced to Imprisonment for Making False Statement to the Privacy Commissioner

(4 December 2014) A former insurance agent (the "Agent") was charged with two counts of making a false statement to the Privacy Commissioner under section 50B(1)(c)(i) of the Personal Data (Privacy) Ordinance (the "Ordinance"), one count of fraud under section 16A of the Theft Ordinance and five counts of using a false instrument under section 73 of Crimes Ordinance on 20 November 2014. The Agent pleaded guilty to the charges. Today, he is sentenced to 4 weeks' imprisonment at the Tuen Mun Magistrates' Court. Since the enforcement of the Ordinance in 1996, this is the first conviction for contravention of the Ordinance by misleading the Privacy Commissioner in discharging his statutory functions.

First Sentencing Case of the New Doxxing Offence



The Shatin Magistrates' Court earlier on 6 October 2022 convicted a 27-year old male, Mr HO Muk-wah, of seven charges of the new doxxing offence upon his guilty plea. After considering the relevant reports, the court sentenced the defendant to 8 months' imprisonment on 15 December 2022. Privacy Commissioner Ms Ada CHUNG Lai-ling welcomed the court's ruling.

The defendant and the victim had a short relationship before breaking up. Between 19 and 26 October 2021, the defendant disclosed on four social media platforms the personal data of the victim without her consent, including her name, photos, residential address, private and office telephone numbers, name of her employer and her position. The defendant also impersonated the victim to open accounts on three of the said platforms. The defendant stated in the relevant messages that the victim welcomed others to visit her at her residential address. Many strangers

瑪麗醫院去年電郵洩130病人病歷 私隱專員公署向醫管局發警告信

撰文：吳祖德

出版：2022-04-28 20:43 更新：2022-04-28 20:44



《香港01》去年4月率先揭發，有瑪麗醫院手術室經理在同年3月發送手術室安排電郵，未有加密處理，洩露130名病人個資、病歷及手術名稱等不必要及敏感資訊予多個部門。

私隱專員公署近日已完成調查，裁定醫管局違反了《個人資料私隱條例》，亦已向醫管局發出警告信，如局方再犯，私隱公署或考慮發出檢控通知，違反便屬刑事罪行。

醫管局表示個案發生後，瑪麗醫院已採取系列措施加強保障病人私隱，稱已接獲調查報告，惟未回覆是否接獲警告信。



(HK01, 28 April 2022)

熱門文章

2021年4月20日 星期二 5:56PM
24°C

主頁 每日明報 即時新聞 明報OL網 明報影片

即時首頁 港聞 娛樂 經濟 地產 兩岸 國際 體育 文摘 熱點 焦點 圖輯 新聞

熱門話題：修改選舉制度·習近平博鰲講話·譚德塞·Tesla致命車禍·許樹昌·麗城花園·歐洲超級聯賽·河
引瘋搶潮

港聞

2019年5月21日 星期二

客戶拒收直銷信息仍接保險推廣 花旗被控違私隱條例罰款1萬 (18:46)

客戶拒收直銷信息仍接保險推廣 花旗被控違私隱條例罰款1萬

Twitter Facebook WhatsApp 讚好 0

A+ A- 圖 鏈 印

(Ming Pao Daily, 21 May 2019)



圖1之1-花旗銀行被控違反《個人資料（私隱）條例》第35G(3)條，今……（資料圖片）



香港個人資料私隱專員公署2016年接獲投訴，投訴人於2016年8月透過互聯網申請花旗銀行信用卡時，選擇拒收直接促銷資訊，惟同年10月卻收到該銀行推廣保險服務的來電。花旗銀行被控違反《個人資料（私隱）條例》第35G(3)條，今日（21日）在九龍城裁判法院承認控罪，被判罰款1萬元。

Media Statements

Date: 12 September 2019

Direct Marketing Offence Admitted: Telecommunications Company Fined HK\$84,000

SmarTone Mobile Communications Limited (SmarTone) faced 23 charges under the Personal Data (Privacy) Ordinance (the Ordinance) today at the Kwun Tong Magistrates' Courts. All charges related to the offence of failing to comply with the requirement from the data subject to cease to use her personal data in direct marketing, contrary to section 35G(3) of the Ordinance. The Company pleaded guilty to 14 charges, and was fined HK\$84,000 in total (HK\$6,000 in respect of each charge). This single case has recorded the highest number of charges and the second highest amount of fine since the added provisions of the Ordinance relating to regulating direct marketing activities came into effect on 1 April 2013.

Case Background

The case stemmed from a complaint received by the office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) in 2017. The complainant received 23 direct marketing text messages or emails from SmarTone between August and December 2017 (in four months' time).

The complainant was a customer of SmarTone which provided mobile telecommunications service to her. In July 2017, she made her opt-out request to SmarTone relating to cessation of using her personal data in direct marketing by phone. However, the complainant still received a direct marketing email from SmarTone in August 2017 and hence complained to PCPD. During the period when PCPD was handling her complaint, the complainant continued receiving direct marketing text messages and emails from SmarTone. The Privacy Commissioner for Personal Data, Hong Kong was of the view that SmarTone failed to comply with the opt-out request of the complainant.

Related Regulation

Pursuant to section 35G(3) of the Ordinance, a company which receives a customer's request for ceasing to use his or her personal data in direct marketing must comply with the request without charge. Failure to comply with the request is a criminal offence which is punishable by a fine of up to HK\$500,000 and imprisonment of up to 3 years.

Topick 24°C 香港時間 2021年4月29日 星期三 17:08

熱門關鍵字：粵人記 校長專欄 藍夢傳奇 德必泰廣告 高登飲食 網木安樂會 新屋廣告 專題 即時傳聞

話語 健康 親子 娛樂 新聞 休閒消費 觀點 TOPick TV Band 1學堂 密傳

無視客戶拒收促銷電話 和記電訊違私隱條例罰款2萬元

關社會 22:30 2018/08/22 讚好 9

關注文章 儲存文章 分享

熱門 粵人記 校長專欄 藍夢傳奇 德必泰廣告 高登飲食 網木安樂會 新屋廣告 免費健康 防欺 開心通區



▲ 無視客戶拒收促銷電話，和記電訊違私隱條例罰款2萬元。(資料圖片)

和記電訊旗下「3」的一名用戶於2016年5月已向提出拒收直銷訊息，惟同年6月及8月仍接獲「3」流動電話服務來電，遂公私隱專員公署作出投訴；和記電訊今日(22日)在於東區裁判法院被控違反兩項《私隱條例》，無依從資料當事人的拒收直銷訊息要求，並繼續使用其個人資料作直接促銷，和記電訊承認控罪，每項控罪分別被判罰款1萬元，即合共被罰款2萬元。

私隱專員黃繼兒表示，為了有效地依從客戶的拒絕直銷服務要求，服務供應商應備存一份拒收直銷訊息的客戶名單，並適時發放予相關同事，停止使用名單內的客戶資料作直銷用途，以及向員工提供適當的訓練等。

(HK Economic Times, 22 August 2018)

Consequences of Contravention (Cont'd)

- ❖ To strictly follow the DPPs and the University's PMP
- ❖ Seek legal advice if in doubt

Part 2

Privacy Management Programme ("PMP")



Background

- ❖ organisations should develop their own **Privacy Management Programme** (Privacy Commissioner for Personal Data, Hong Kong)
- ❖ **corporate governance responsibilities**
- ❖ institutionalise a proper system for responsible use of personal data

Purpose of the PMP

- ❖ the University's commitment to personal data protection
- ❖ uphold personal data protection as part of the University's corporate governance
- ❖ demonstrate responsible collection, holding, processing and use of personal data
- ❖ minimise risks of non-compliance

PMP can be accessed and downloaded via **BUniPort → U-Wide Policies & Info → Policies & Guidelines → Guidelines on Personal Data Protection**

Policies, Guidelines & Standards

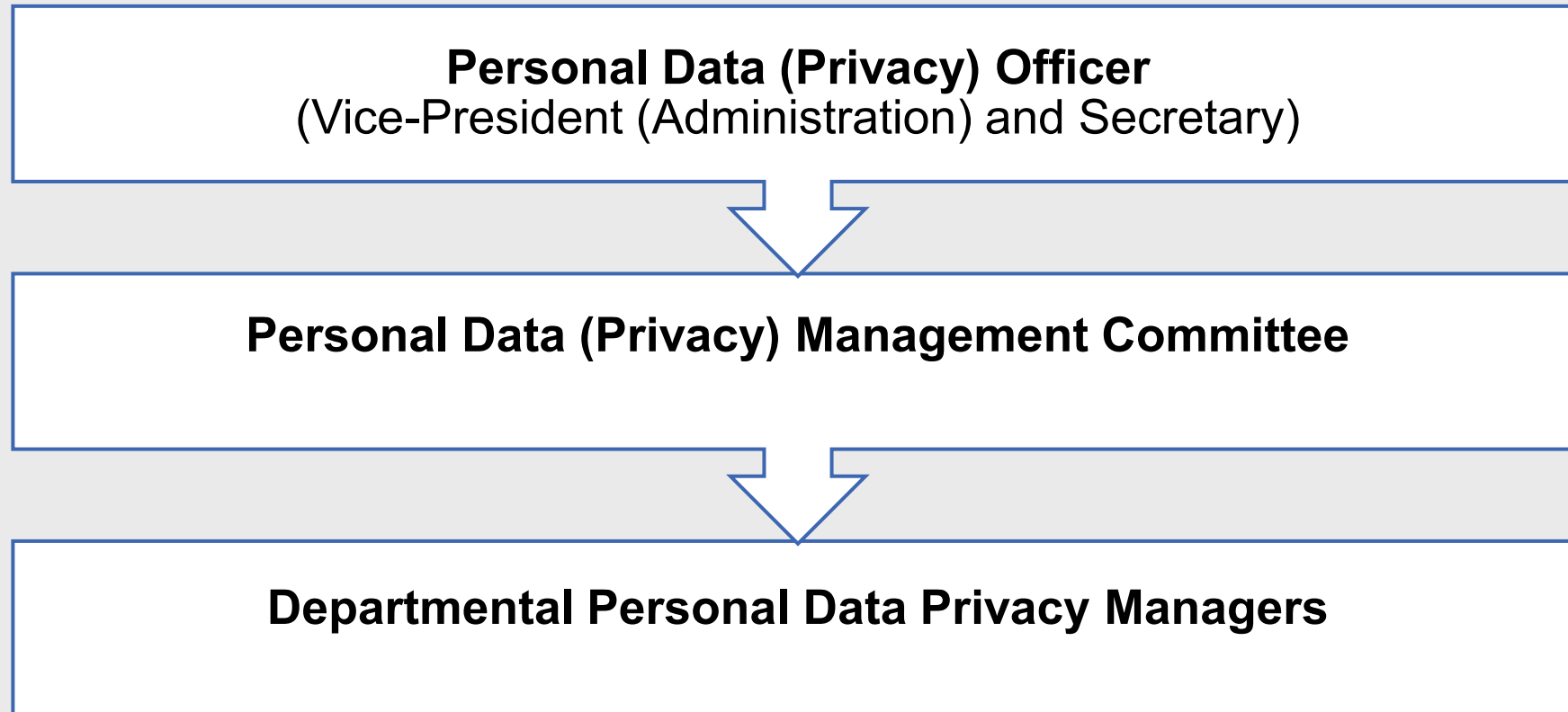
- Personal Privacy
- Guidelines on Personal Data Protection**
 - Privacy Management Programme**
 - Personal Data Breach Protocol (Physical and Electronic Records)
 - Personal Data Breach Incident Form (Microsoft Word format)
 - Personal Data Breach Incident Form (PDF format)
 - External Guidance Notes issued by PCPD (English and Chinese versions)
- Information Security Principles, Guidelines & Standards
- Finance, Human Resources & IT Policies
- Quality Assurance, Teaching & Learning



香港浸會大學
HONG KONG BAPTIST UNIVERSITY

Privacy Management Programme

Governance Structure on Management of Personal Data



Personal Data (Privacy) Management Committee

- ❖ perform periodic review of the PMP
- ❖ keep a record of the University's personal data inventory
- ❖ coordinate and monitor the handling of data breach incidents
- ❖ oversee the discharge of duties by the DPDPMs
- ❖ manage the handling of personal data privacy complaints

Departmental Personal Data Privacy Managers (DPDPMs)

- ❖ represent the department to communicate regularly with the Personal Data (Privacy) Management Committee
- ❖ update the personal data inventory of his/her department periodically
- ❖ carry out periodic risk assessments within his/her department and submit to Personal Data (Privacy) Management Committee via CCSL
- ❖ acting as the primary handler of personal data privacy complaints and enquiries, data access and correction requests in his/her department

Programme Controls



Types of Personal Data Collected by the University

Types	Examples
Identification	name, date of birth, gender, identity card/passport details, photo
Contact details	address, telephone number, email address, emergency contact
Evaluative data	academic results, assessment records

Further details: *Privacy Policy Statement and Personal Information Collection Statement*

Personal Data Inventory

- i. understand the type of consent that the University needs to obtain from data subjects
- ii. determine how the data is protected
- iii. comply with data access and correction requests
- iv. assess the impact of any personal data leakage incidents

Data Processor Management

Definition of “Data Processor”

A **Data Processor** is 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.*

Data Processor Management

Examples of tasks performed by data processors:

- ❖ organising events on behalf of the University
- ❖ carrying out surveys on behalf of the University

Data Processor Management

Data user must adopt contractual or other means to prevent:

- any personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP2(3)); and
- unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2)).

Data Processor Management

if a data processor is proposed to be engaged:

complete the *Data Processor Engagement Checklist* (Appendix J)

sign the *Data Processing Agreement* (Appendix K)

obtain approval from
VPAS via CCSL

Data Processor Management

Cases of Data Processor Engagement:

- ❖ printing graduation certificates
- ❖ document scanning
- ❖ sending invitation emails
- ❖ developing online registration system

Data Processor Management

1. send your draft **Data Processor Engagement Checklist** (Appendix J) and draft **Data Processing Agreement** (Appendix K) to CCSL
2. comments from CCSL
3. Data Processor Engagement Checklist - to be signed by DPDPM
4. Data Processor Engagement Checklist - to be endorsed by Unit Head
5. Send the signed Data Processor Engagement Checklist to CCSL **for approval** by VPAS
6. Arrange signing of the Data Processing Agreement

Data Processor Management

Practical Tips:

- time management
- ongoing discussion with data processor (e.g. security measures to be adopted by the data processor)
- context
- types of personal data

Data Processing Agreement

Updated version in September 2026

Key updates:

- technical and organisational measures required to be adopted by a data processor
- upon the University's request, the data processor shall report to the University on its compliance with the Data Processing Agreement and the data security measures taken

Appendix K

Data Processing / Transfer Agreement

This Data Processing / Transfer Agreement ("Agreement") is dated the date of the last signature of the Parties hereto stated at the end of this Agreement, and is made

BETWEEN

Hong Kong Baptist University ("HKBU" or the "Transferor"), at 224 Waterloo Road, Kowloon Tong, Hong Kong

AND

[] ("Transferee"), at []

(each a "Party" and collectively, the "Parties").

WHEREAS

[]

IT IS AGREED AS FOLLOWS:

1. Obligations of the Transferor

1.1 The Transferor represents and warrants to the Transferee that:

- the personal data (as set out in **Annex** to this Agreement) has been collected in accordance with data protection principle ("DPP") 1 in Schedule 1 to the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("Ordinance");
- all reasonably practicable steps have been taken to ensure the accuracy of the personal data in accordance with DPP2;
- the personal data has not been retained longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is to be used; and
- the transfer of the personal data to the Transferee is permitted by DPP3, as it is in line with the purpose for which the data was to be used at the time of the collection of the data, or in so far as the data is to be used for a new purpose, the prescribed consent of the data subject has been obtained.

Data Transfer other than to a Data Processor

- ❖ transfer of personal data to third party is not allowed, unless such transfer has been approved by VPAS
- ❖ *Application for Transfer of Personal Data to a Third Party (Appendix L)*
 - ❖ Submit to Personal Data (Privacy) Officer (i.e. VPAS) via CCSL

Data Transfer other than to a Data Processor

Blanket approval:

- ❖ **academic partnerships** with educational institutions
- ❖ **financial institutions** in relation to payment of salary, MPF and employment benefits
- ❖ bureau/department of the **Government of the HKSAR** for facilitating or enabling participation by members of the University in the Government's community education or promotional/publicity activities

Data Transfer other than to a Data Processor

Blanket approval:

- ❖ **types of personal data restricted to those strictly necessary for the relevant purpose**
- ❖ **blanket approval for transfer of personal data to the Government of the HKSAR:**
 - (i) name of staff members, students;
 - (ii) staff/student numbers;
 - (iii) university email address; and
 - (iv) university work telephone numbers of staff members (if requested by the bureau/ department)

Data Transfer other than to a Data Processor

- ❖ upon obtaining approval from the Personal Data (Privacy) Officer or if blanket approval applies, sign the *Data Transfer Agreement* (**Appendix K**) with the transferee

Data Transfer

complete the *Application for Transfer of Personal Data to a Third Party* (Appendix L)

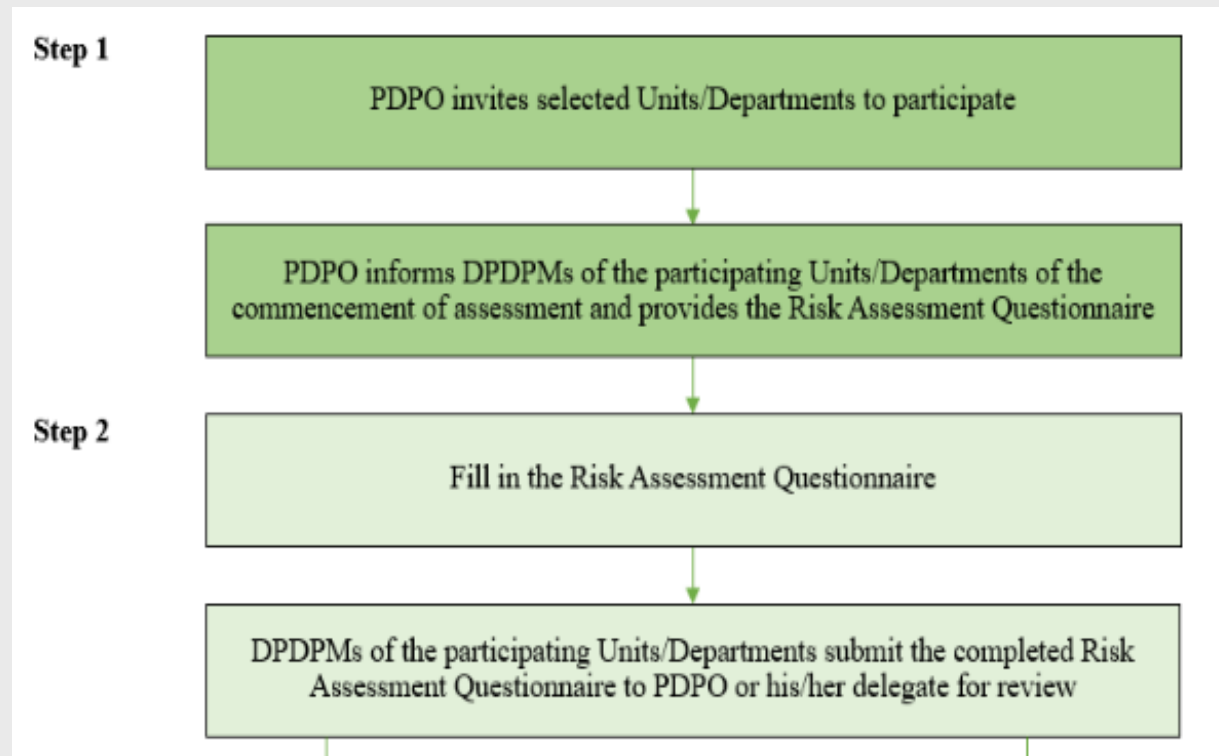
sign the *Data Transfer Agreement* (Appendix K)

**obtain approval from
VPAS via CCSL**

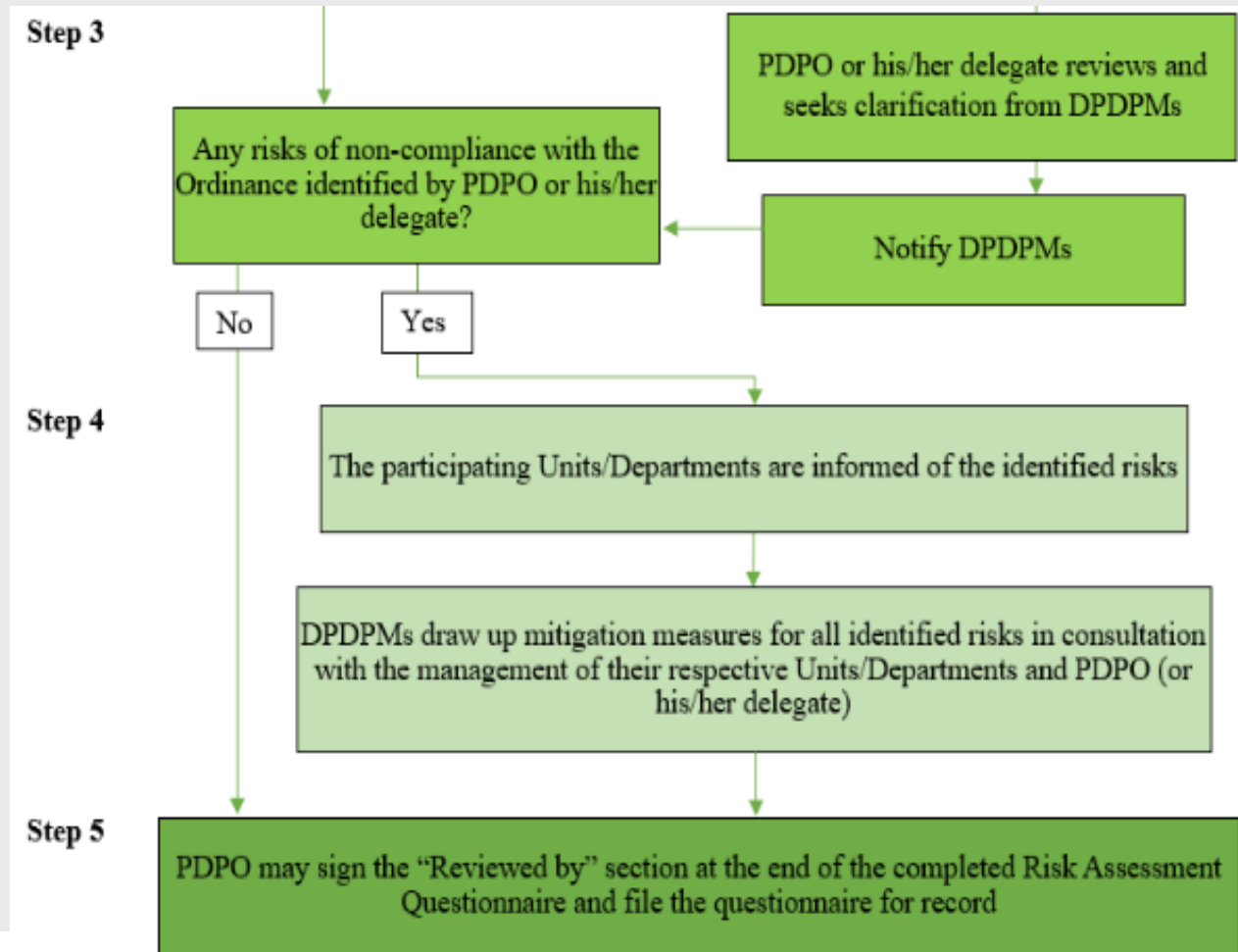
Risk Assessment Tools

- (1) Periodic Risk Assessment
- (2) Privacy Impact Assessment

Periodic Risk Assessment



Periodic Risk Assessment



Risk Assessment Questionnaire

Appendix G Risk Assessment Questionnaire

Faculty/School/Office ("Unit"):	
Date of this Periodic Risk Assessment:	

Note: The following questions apply to all personal data, irrespective of the medium in which it is collected, processed, used or stored. Units must evaluate their handling of personal data in both electronic and physical records. If any of your answers differ depending on the format of the records, please state this clearly.

Questions	Answers
Part A: Compliance with Data Protection Principles ("DPPs")	
1. Does your Unit have the practice of providing the University's Personal Information Collection Statement ("PICS") ²⁸ to data subjects prior to collecting personal data?	☐ Yes ☐ No, but it is our Unit's practice to provide a bespoke PICS whenever we collect personal data. ☐ No, neither the University's PICS nor a bespoke PICS has been provided. (Please provide further details.) ☐ N/A (Our Unit did not collect any personal data.)
2. Please confirm that it has been your Unit's practice to collect necessary and adequate (but not excessive) personal data for a lawful purpose directly related to a function or activity of your Unit, in compliance with DPP1 ²⁹ (Purpose and Manner of Collection).	☐ Yes ☐ No (Please provide further details.) ☐ N/A (Our Unit did not collect any personal data.)
3. Please confirm that your Unit has taken all practicable steps to protect personal data against unauthorised or accidental access, processing, erasure, loss or use ³⁰ .	☐ Yes ☐ No (Please provide further details.)

Privacy Impact Assessment (“PIA”)

- ❖ evaluates the impact of any proposed change in handling of personal data, e.g. launching a new personal data handling procedure
- ❖ PIA Questionnaire (**Appendix H**) shall be completed by subject officer, reviewed by DPDPM (endorsed by Unit Head), vetted by CCSL, and submitted to the Personal Data (Privacy) Officer via CCSL

Breach Handling

In the event of any breach or suspected breach of the security of personal data, all staff are expected to strictly observe the prescribed procedures



Personal Data Breach Protocol (Physical and Electronic Records)

- the incident to be reported expeditiously and within the time frame as set out in the Personal Data Breach Protocol

Ongoing Assessment and Revision

- ❖ reflect the latest developments in personal data privacy law
- ❖ adopt a proactive approach in building a privacy-respectful culture

Updates in September 2026

- ❖ “**four-eyes principle**” as recommended practice
- ❖ personal data may be retained longer than originally necessary for the purpose of **handling disputes** and potential legal claims
- ❖ payment requests about data access requests shall be **handled asap**

Updates in September 2026

- ❖ expanded the **blanket approval** (transfer of personal data to the Government of the HKSAR) for the purposes of its community education or publicity activities
- ❖ revised the ***Data Processing/ Transfer Agreement (Appendix K)***

❖ if in doubt, please contact us at data-privacy@hkbu.edu.hk

End