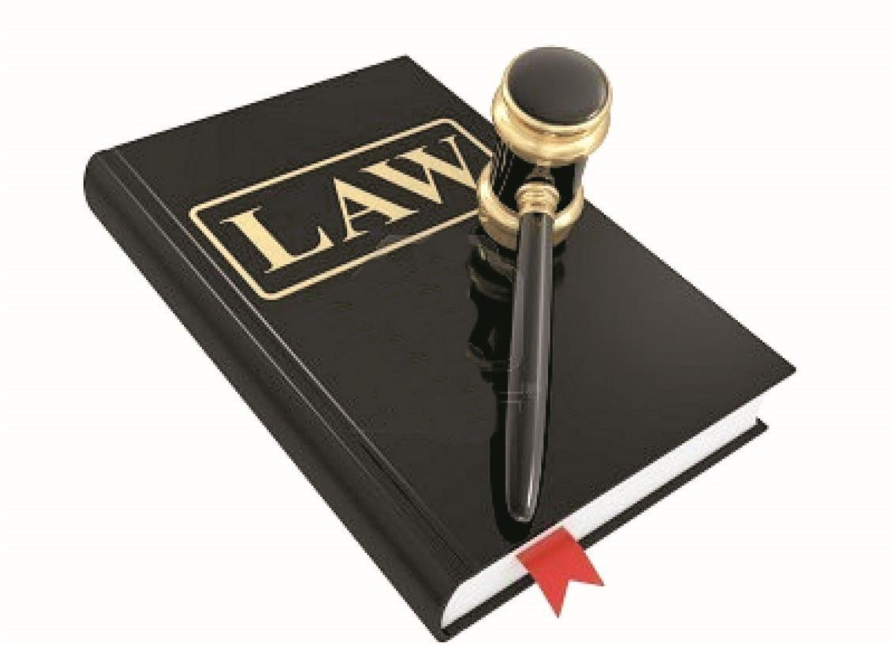

PCPD
HK
20
PCPD.org.hk
est.1996
University
Privacy Campaign
大學保障私隱活動

University Privacy Campaign 2016/17
24.02.2017

Protecting Personal Data Privacy in University Administration

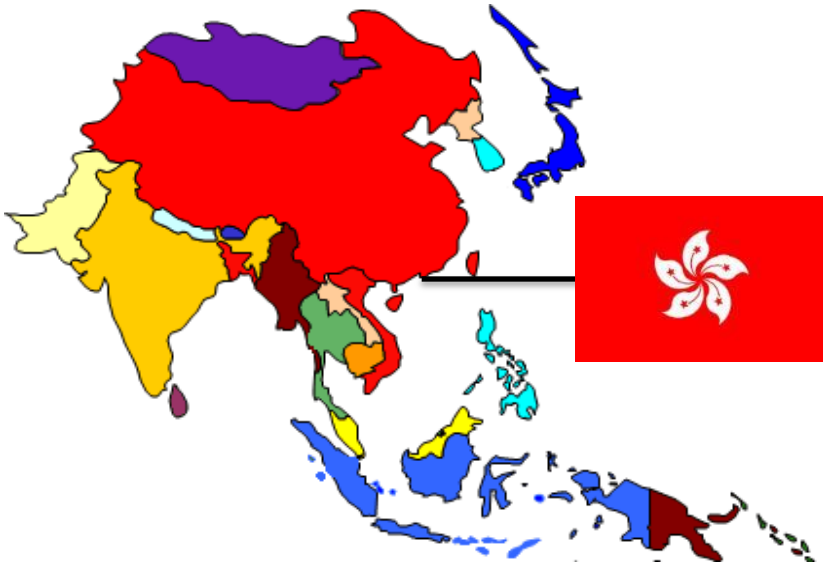
Note: The contents herein are for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data ("the Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The contents herein will not affect the exercise of the functions and power conferred to the Commissioner under the Ordinance.

Personal Data (Privacy) Ordinance



Personal Data (Privacy) Ordinance

- single and comprehensive legislation
- covers the public (government) and private sectors



Personal Data (Privacy) Ordinance

Legislative Background

- Personal Data (Privacy) Ordinance came into effect on 20 December 1996, based on internationally accepted data protection principles.

Amendment of the Ordinance

- Gazette published on 6 July 2012
- All amendments came into force

Objectives of the Ordinance

- Protecting the privacy right of a "data subject" in respect of "personal data", but general privacy issues are not protected.

- "**Data Subject**"

  A data subject refers to the living individual who is the subject of the "personal data" concerned.

Definitions under the Ordinance

"**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.

Are examination answer books personal data of students?

Are examination answer books personal data of students?

Examination answers are not necessarily students' personal data

Examination papers and answers generally do not constitute personal data of the students because they do not refer to their personal information

Personal information of a student which are contained in answers, or comments marked on answer books by examiners are personal data of the students

Reference: i) Report Number - R08-10578 ; ii) AAB No. 7/2007

Who is responsible

Section 4 – ***A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance***

"data user" in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data

Who is responsible

Section 65

*(1) Any act done or practice engaged in by a person **in the course of his employment** shall be treated for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.*

*(2) Any act done or practice engaged in by a person as agent for another person **with the authority** (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.*

Six Data Protection Principles (DPPs)

Cross-office Use of Personal Data

Cross-office Use of Personal Data

Relevant requirements under DPP1(3)

- **Inform the data subject of the purposes of data collection immediately or in advance.**

Relevant requirements under DPP3

- **Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.**
- **New purpose means any purpose other than the purposes for which the data was collected or directly related purposes.**

Cross-office Use of Personal Data

- **Controlling access to personal data and limiting the disclosure of personal data on a need-to-know basis**
- **Reasonable expectation of data subjects**

Case Sharing - Disclosure of warning email by supervisor without consent

The complaint:

- the Complainant was an executive staff of an academic department and the secretary of a specific management committee in a university
- the Complainant needed to report to the head of department and the head also acted as the chairman of the Committee
- the head sent a warning email to the Complainant and, without the Complainant's consent, copied the full contents of the warning email to all members of the Committee

Case Sharing - Disclosure of warning email by supervisor without consent

Explanation by the University:

- one of the purviews of the Committee was to give advice on "deployment of human and other resources"
- disclosure of the warning email enabled the Committee members to ascertain the deficiency found on the Complainant's work performance

Outcome:

- there was insufficient evidence indicating that the Committee members were empowered to review the work performance of the Complainant

Case Sharing - Disclosure of warning email by supervisor without consent

Outcome:

- the Complainant's supervisor mere forwarded the warning email to the Committee members without requesting the recipients to render their advice and views on the Complainant's performance

- the Commissioner considered that the university's disclosure of the warning email to the members of the Committee was not on a "need to know" basis and hence contravened the requirements of DPP3

Cross-office Use of Personal Data

Relevant exemptions

- Section 59: Health
- Section 60B: Legal proceedings etc.
- Section 62: Statistics and research
- Section 63C: Emergency situations

Exemption

The complaint:

- After work injury, the Complainant, a technician of a public transport institution, was referred to psychological treatment during which the Complainant had told the psychologist and counsellor of a service association more than once that he wanted to blow up the public transport facilities of the institution ("the Data").

- After consideration and discussion with the psychologist, the association informed the institution of the Data

Exemption

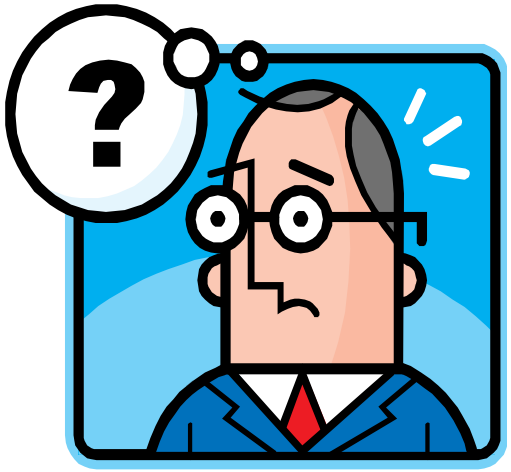
Outcome:

- The PCPD considers that blowing up public transport facilities is unlawful or seriously improper conduct under section 58(1)(d) of the Ordinance. The association informed the institution of the Data for the prevention of the above conduct. Under the circumstances, the Data should be exempt from the requirement

- Moreover, section 59 of the Ordinance also applied . If the association could not disclose the Data without the consent of the technician, it would be likely to cause serious harm to the physical or mental health of the technician. Under the circumstances, the Data should also be exempt from the requirement

Cross-office Use of Personal Data

Providing personal data to the authorities?



Fundraising and Alumni Affairs

Fundraising and Alumni Affairs

New regulatory regime of direct marketing

- **Part VIA of the Ordinance: 35A to 35M**
- **More stringent regulation and higher penalties**
- **「Opt-out Mechanism」unchanged**

Fundraising and Alumni Affairs

"Direct Marketing" is defined to mean:

1) **the offering, or advertising of the availability, of goods, facilities or services; or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through**

2) **sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or making telephone calls to specific persons.**

Fundraising and Alumni Affairs

Direct marketing does not include unsolicited electronic messages sent to:




Unsolicited Electronic Messages Ordinance

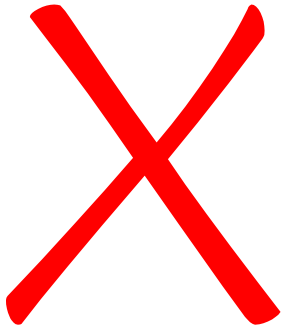
Fundraising and Alumni Affairs

Is it direct marketing?

Introducing a donation programme face-to-face

Fundraising and Alumni Affairs

Is it direct marketing?



Introducing a fundraising programme exclusively for corporations/organisations

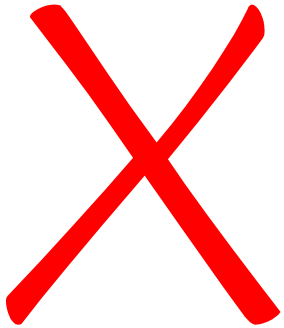
Fundraising and Alumni Affairs

Is it direct marketing?

Notification of membership renewal

Fundraising and Alumni Affairs

Is it direct marketing?



Invitation to a reunion

Fundraising and Alumni Affairs

Is it direct marketing?

Sending a newsletter

Fundraising and Alumni Affairs

Relevant requirements under DPP1(1)

- **Only necessary, adequate but not excessive personal data is to be collected by a data user.**
- **Collection of personal data that is necessary for specific purpose (e.g. name and contact data) generally suffices.**
- **Additional personal data for direct marketing purpose is to be provided on a voluntary basis (e.g. education level, marital status).**

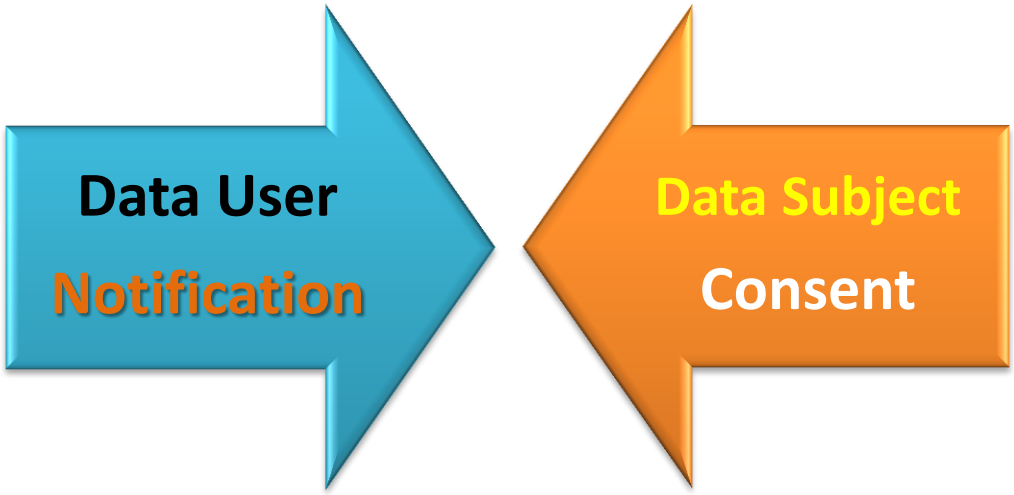
Fundraising and Alumni Affairs

Relevant requirements under DPP1(2)

- **No deceptive or misleading means should be used (e.g. bundled consent in an application form).**

Fundraising and Alumni Affairs

Intends to use personal data or provide personal data to another person for use in direct marketing



Provision of Personal Data

- Provide data subjects with "prescribed information" and response channel through which the data subject may elect to give consent
- Notification should be easily readable and understandable

- Should be given explicitly and voluntarily
- "consent" includes an indication of "no objection"

Fundraising and Alumni Affairs

Prescribed information：

Use of Personal Data in Direct Marketing	Provide Personal Data to another person for Use in Direct Marketing
1. The data user intends to use the personal data of the data subject for direct marketing;	1. The data user intends to provide the personal data of the data subject to another person for use by that person in direct marketing;
2. The data user may not so use the data unless the data user has received the data subject's consent to the intended use;	2. The data user may not so provide the data unless it has received the data subject's **written consent** to the intended provision;
3. The kinds of personal data to be used;	3. The provision of the data is **for gain** (if it is to be so provided);
4. The classes of marketing subjects in relation to which the data is to be used;	4. The kinds of personal data to be provided;
5. The response channel	5. The classes of persons to which the data is to be provided;
	6. The classes of marketing subjects in relation to which the data is to be used; and
	7. The response channel

Fundraising and Alumni Affairs

"Consent" includes an indication of no objection.

Example of indicating no objection *generally*:

We intend to use your name, telephone number and address for direct marketing credit card and insurance products/services but we cannot so use your personal data without your consent.

Please sign at the end of this statement to indicate your agreement to such use. Should you find such use of your personal data not acceptable, please indicate your objection before signing by ticking the box below.

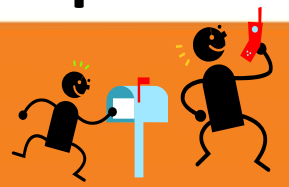
☐ The customer named objects to the proposed use of his/her personal data in direct marketing.

_____

Signature of the customer
Name: xxx
Date: yyyy/mm/dd

Fundraising and Alumni Affairs

- A data user must notify data subject of his opt-out right when using his personal data for the first time in direct marketing, irrespective of whether the personal data is obtained directly from him or from other sources
- A data subject may at any time require a data user to cease to use his/her personal data in direct marketing. A data user must, without charge, cease to use the personal data concerned upon request.
- There is no restriction as to the manner in which the data subject shall exercise his opt-out right.



Fundraising and Alumni Affairs

Grandfathering arrangement

1) The data subject had been explicitly informed of the intended use or use of the data subject's personal data in direct marketing in relation to the class of marketing subjects;

2) the data user had so used any of the data;

3) the data subject had not required the data user to cease to use any of the data; and

4) the data user had not in relation to such use contravened any provision of the Ordinance as in force at the time of the use.

Fundraising and Alumni Affairs

- **It suffices that the organisation had used any of the data.**

  For example, if the organisation had used the data subject's mobile phone number in question, not only the mobile phone number be exempted but the use of the other personal data already held by the organisation.

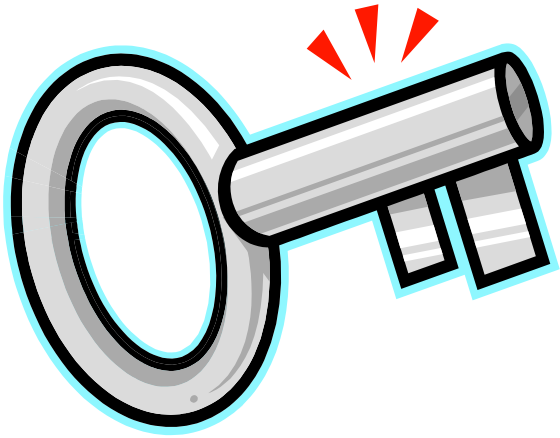
- **The grandfathering arrangement also applies to update of personal data held by a data user before the commencement date, but not apply to new data acquired.**

Use of Social Networks

Use of Social Networks

Key principles

- Appropriateness
- Transparency
- Respect for individual rights
- Protection



Use of Social Networks

Using contact information for direct marketing purposes

- **Must comply with the direct marketing requirements**
- **When make use of the social connection, keep the members informed and allow them to opt out of participating in such process.**

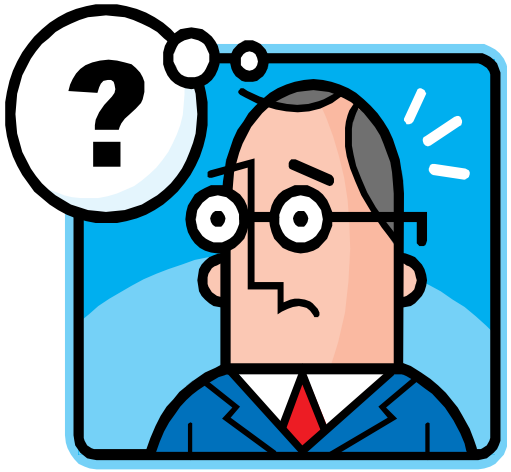
Use of Social Networks

Collection and display of personal data

- **Must supply a corresponding Personal Information Collection Statement (PICS)**
- **Remind members not to disclose in open social networks their personal data.**
- **Make known the practices and policies.**

Use of Social Networks

Showing videos or photos of events?



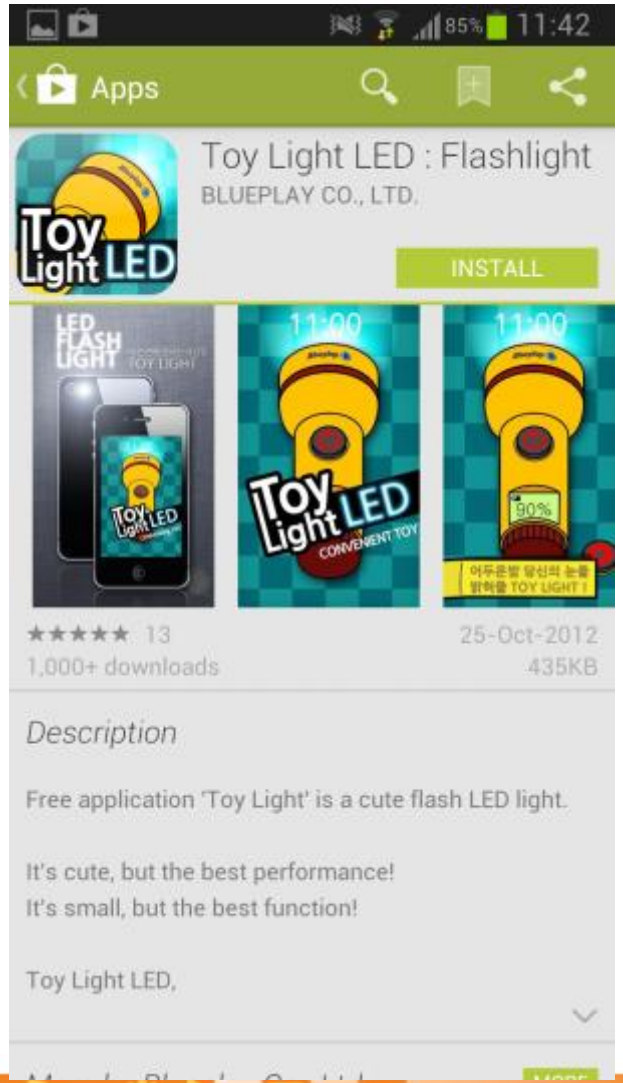
Mobile App

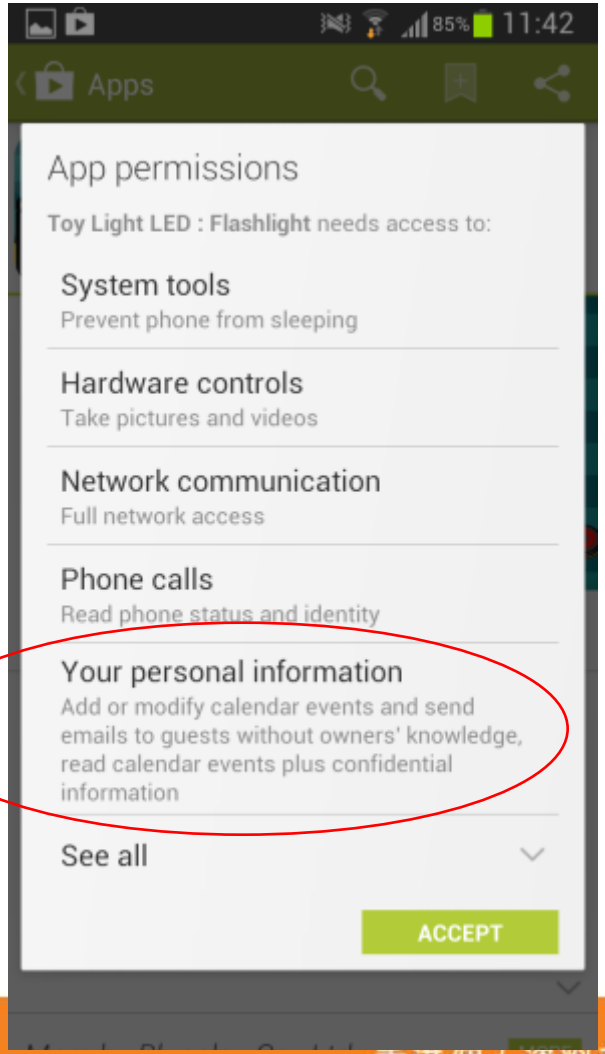
Surveys on the top 60 mobile apps

May 2014

- 55% provided privacy policy
- 15% of the policies that were tailor-made to apps
- 8% app developers had not provided sufficient details to identify themselves

Would you use this app?





Excessive Collection of Personal Data Through Mobile App

Media Statements

Date: 15 December 2014

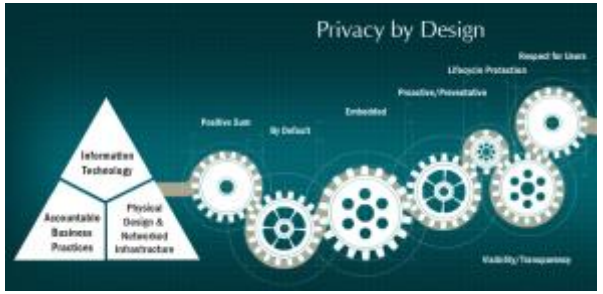
Excessive Collection of Personal Data through Mobile Application by Worldwide Package Travel Service Operating with No Privacy Policy

(15 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") published an investigation report today concerning the excessive collection of personal data by Worldwide Package Travel Service Limited ("Worldwide Travel") from customers when they enrolled for the company's loyalty programme ("Programme") and when making online enquiries about the reward points under the Programme using the mobile application ("App") developed by Package Tours (Hong Kong) Limited ("Package Tours") and operated by Worldwide Travel. Further, both Worldwide Travel and Package Tours did not explain to the App users the purpose of use of the customers' personal data they collected via a privacy policy, app marketplace description or other communication means.

2. The two companies have contravened the Data Protection Principle ("DPP") 1 in Schedule 1 to the Personal Data (Privacy) Ordinance ("Ordinance").

Privacy by Design

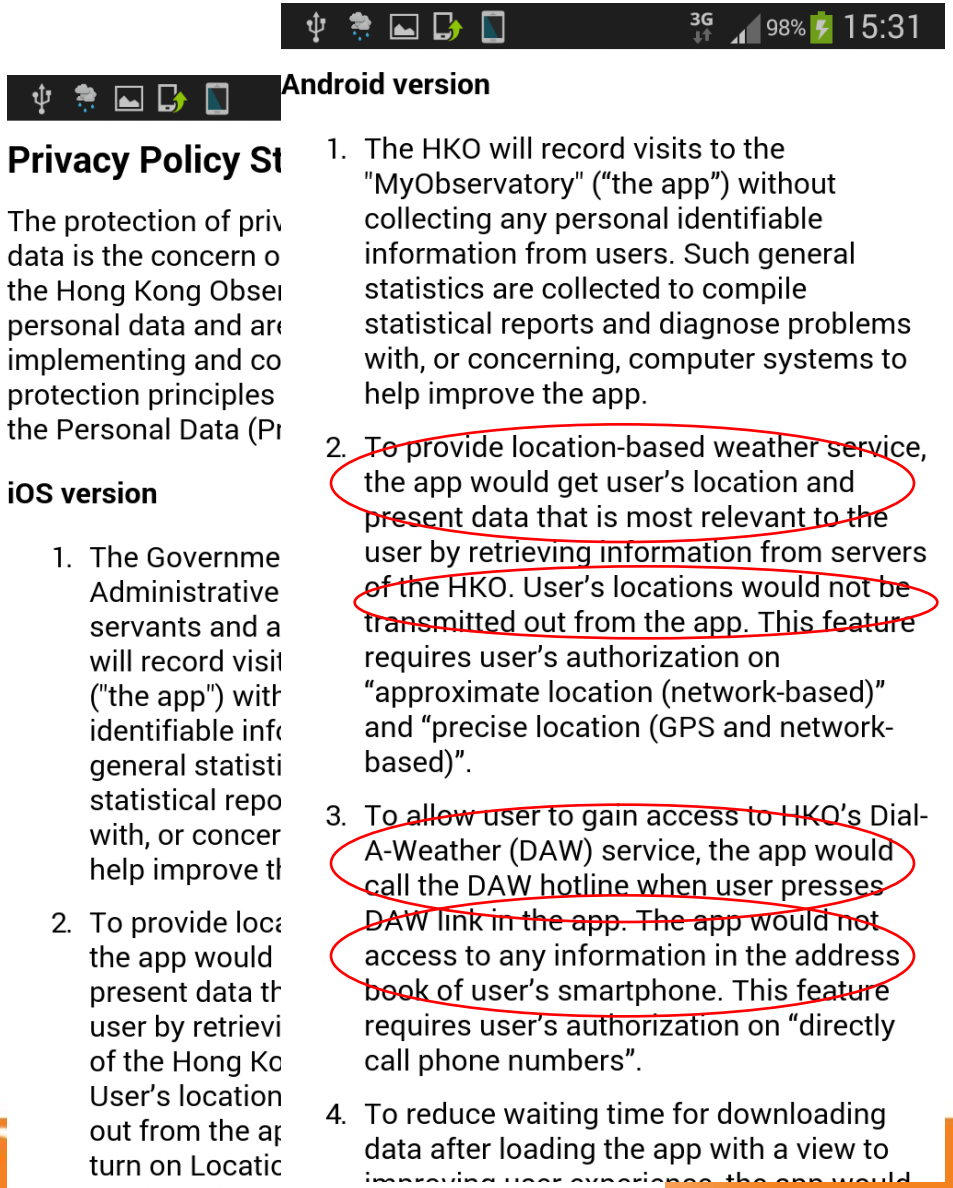
Privacy by Design* is the philosophy of embedding privacy from the outset into the design specifications of accountable business processes, physical spaces, infrastructure and information technologies



*http://privacybydesign.ca/

Privacy by Design – when applying it to app development

- Is the access of the information necessary?
  - If access is necessary, is there a clear/accessible privacy policy/notice?
  - If access is necessary, is the uploading of the information necessary?
    - If uploading is necessary, is the storage necessary?
  - If access is necessary, is the sharing/transferal of the information necessary?
- What other information is being collected/combined/associated? What are the impacts?
- What safeguards (such as encryption and access controls) are in place to the information accessed/transmitted/shared/kept?
- Can mobile user opt-out of any of these and erase accounts?



Privacy Policy St

The protection of priv
data is the concern o
the Hong Kong Obser
personal data and are
implementing and co
protection principles
the Personal Data (Pr

iOS version

1. The Governme
Administrative
servants and a
will record visit
("the app") with
identifiable info
general statisti
statistical repo
with, or concer
help improve th
2. To provide loca
the app would
present data th
user by retrievi
of the Hong Ko
User's location
out from the ap
turn on Locatic
service. Please see paragraph 5 below for
details.)

Android version

1. The HKO will record visits to the "MyObservatory" ("the app") without collecting any personal identifiable information from users. Such general statistics are collected to compile statistical reports and diagnose problems with, or concerning, computer systems to help improve the app.
2. To provide location-based weather service, the app would get user's location and present data that is most relevant to the user by retrieving information from servers of the HKO. User's locations would not be transmitted out from the app. This feature requires user's authorization on "approximate location (network-based)" and "precise location (GPS and network-based)".
3. To allow user to gain access to HKO's Dial-A-Weather (DAW) service, the app would call the DAW hotline when user presses DAW link in the app. The app would not access to any information in the address book of user's smartphone. This feature requires user's authorization on "directly call phone numbers".
4. To reduce waiting time for downloading data after loading the app with a view to

The good example

- Available before installation
- (Nearly) single page and in simple language
- Specific to the types of data accessed
- Assured users what it would not do
- But – don't copy this…

Best Practice Guide for Mobile App Development

Outsourcing & Subcontracting

Outsourcing & Subcontracting

"Data Processor"

a person who processes personal data on behalf of another person and does not process the data for his own purposes, whether within or outside Hong Kong

Outsourcing & Subcontracting

Relevant requirements under DPP2(3)

- The data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary.

Relevant requirements under DPP4(2)

- The data user 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.

Outsourcing & Subcontracting

Contractual means

- Security measures required to be taken
- Timely return, destruction or deletion of the personal data
- Prohibition against unauthorised use or disclosure
- Prohibition against subcontracting or imposing obligations
- Immediate reporting of any sign of abnormalities

Outsourcing & Subcontracting

Contractual means

- **Measures required to be taken to ensure its staff will comply with the obligations**
- **Right to audit**
- **Consequences for violation of contract**

Outsourcing & Subcontracting

Other means

- Selecting reputable data processors
- Robust policies and procedures in place
- Exercising the right to audit and inspect

Six Data Protection Principles (DPPs)

DPP1 - Purpose and manner of collection

- Data shall be collected for purposes related to the functions or activities of the data user.
- Data collected should be adequate but not excessive.
- The means of collection must be lawful and fair.

DPP1 - Purpose and manner of collection

Inform the data subject of the following immediately or in advance:

1)the purposes of data collection;

2)the classes of persons to whom the data may be transferred;

3)whether it is obligatory or voluntary for the data subject to supply the data;

4)where it is obligatory for the data subject to supply the data, the consequences for him if he fails to supply the data; and

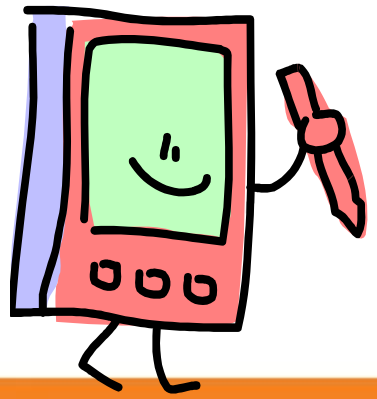
5)the name or job title and address to which access and correction requests of personal data may be made.

DPP2 - Accuracy and duration of retention

- Data users shall take practicable steps to ensure the accuracy of personal data held by them.
- All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose.
- If a data user engages a data processor to process personal data on the data user's behalf, the 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.

DPP3 – Use of personal data

- **Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.**
- **A "relevant person" may give the prescribed consent required for the data subject under specified conditions.**



DPP4 – Security of personal data

- All practicable steps shall be taken to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss and use.
- Security in the storage, processing and transmission of data
- If a data user engages a data processor to process personal data on the data user's behalf, the data user 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.

DPP5 – Information to be generally available

Data users have to provide:

1)policies and practices in relation to personal data;

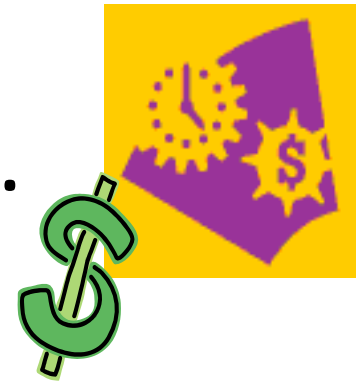
2)the kind of personal data held; and

3)the main purposes for which personal data is used.

DPP6 – Access to personal data

A data subject shall be entitled to:

- **request access to his/her personal data;**
- **request correction of his/her personal data.**



Data user may charge a fee for complying with the data access request.

Resources

- New Guidance on Direct Marketing
- Guidance for Data Users on the Collection and Use of Personal Data through the Internet
- Information Leaflet: Privacy Implications for Organisational Use of Social Networks
- Best Practice Guide for Mobile App Development

Office of the Privacy Commissioner for Personal Data

- **Hotline:** (852) 2827 2827
- **Fax:** (852) 2877 7026
- **Website:** pcpd.org.hk
- **E-mail:** enquiry@pcpd.org.hk
- **Address:** 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai