Hong Kong Computer Society

Security and Privacy Forum

on

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

11 Jan 2012

Forum Agenda

1. Introduction

Mr Peter Yan, Vice President (Policy and Communication) of HKCS and Chairperson of HKCS IPC

Mr Micky Lo, Chairperson of HKCS ISSIG

2. Enterprise Strategy and Policy for Personal Data Protection

Mr Dennis Fullgrabe, Chief Internal Auditor, Hospital Authority

3. Data Protection Principles

Ir Stephen Lau, JP, President, Hong Kong Computer Society and Former Privacy Commissioner for Personal Data, and

Mr Thomas Parenty, Managing Director, Parenty Consulting Limited

4. Outsourcing & Cloud Computing

Mr Peter Yan, Executive Director, Computer And Technologies Holdings Limited

5. Workplace Monitoring

Ms Susanna Shen, Head of Information Technology, The Hong Kong and China Gas Company Limited

6. Direct Marketing

Mr John Chiu, JP, Managing Director, AT Group Limited

7. Biometrics

Professor YB Yeung, Adjunct Professor, Department of Information Systems, City University of Hong Kong

8. Panel Discussion

9. Forum Ends

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Introduction

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Enterprise Strategy and Policy for Personal Data Protection

Dennis Fullgrabe,
Chief Internal Auditor, Hospital Authority

Enterprise wide Responsibility

- legal obligation
- good for business:
  - confidence & trust
  - competitive advantage
- a key to good corporate governance, accountability and transparency

Enterprise Strategy & Policy (Chapter 3)

Strategy to achieve personal data protection

- be proactive, minimise the risks
- 'how' depends on your environment/industry
- usually four key elements:
  - policy
  - embedding
  - privacy culture
  - continuous improvement

Enterprise Strategy & Policy

Policy

- compliance / good governance require clear & enterprise-level personal data protection policy:
  - demonstrates top management commitment
  - provides relevant rules to follow
- communication

Embedding

- prevent privacy risks / reduce impact
- works best in design & architecture
- Integral part, not an add-on

Enterprise Strategy & Policy

Privacy Culture

- not solely a technical or policy issue
- risk treatments supported by privacy culture, where personal data protection is second nature
- requires persistent effort over long term

Continuous Improvement

- monitor for changing risks
- regularly review effectiveness of strategies

Privacy Impact Assessment (Chapter 4)

- Ideally a policy requirement
- practical guidance on:
  - why, who, which, when, how
  - common elements of a PIA report

Data Breaches and Privacy Impact Management (Chapter 5)

- not a case of ‘IF’, but rather ‘WHEN’
- how you respond can have a big impact
- data privacy incident strategy - a policy requirement
- ensure a quick, effective and orderly response

Thank You

HONG KONG COMPUTER SOCIETY

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Data Protection Principles

Stephen Lau, JP
HKCS President

HONG KONG
Personal Data (Privacy) Ordinance

- ***to protect the individual's right to privacy with respect to personal data***

- ***to safeguard the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws***

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 User

- **The term** “data user” **is defined in** section 2(1) **of PD(P)O as follows:**
- ***“ ‘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.”***

Data Subject

- **The term** “data subject” **is defined in** section 2(1) **as follows:**
- ***“Data subject, in relation to personal data, means the individual who is the subject of the data.”***

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 1 - Purpose and manner of collection

- (1) Personal data shall not be collected unless-
  - (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
  - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
  - (c) the data are adequate but not excessive in relation to that purpose.
- (2) Personal data shall be collected by means which are-
  - (a) lawful; and
  - (b) fair in the circumstances of the case.

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 1 - Purpose and manner of collection

- (3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that-
  - (a) he is explicitly or implicitly informed, on or before collecting the data, of-
    - (i)whether it is obligatory or voluntary for him to supply the data; and
    - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
  - (b) he is explicitly informed-
    - (i)on or before collecting the data, of-
      - (A) the purpose (in general or specific terms) for which the data are to be used; and
      - (B) the classes of persons to whom the data may be transferred

Personal Information Collection Statement (PICS)

- It is a common practice for the data user to provide a written statement, generally referred to as a Personal Information Collection Statement (PICS), which should contain the purpose of use of the personal data and the classes of transferees of the data. A sufficiently clear, unambiguous and easy to understand PICS should be given to the data subject to take into account of the characteristics of the targeted data subjects (in terms of age, education level, etc.).

Personal Information Collection Statement (PICS)

- Many disputed cases between a data user and a data subject revolve around transfer of data to third party by the data user, e.g. transfer of data to an outsourced service provider for processing, or to a debt collection agency for debt recovery. A well drafted transfer clause will go a long way to minimise unpleasant surprise or dispute. Defining a class of transferees in vague terms such as “business partners” or “such third parties” should be avoided. A data user should define the class of data transferees by its distinctive features.

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 2 - Accuracy and duration of retention

- this provides that personal data should be accurate, up-to-date and kept no longer than necessary

Section 26(1) of PD(P)O

- *"A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless –*
- *(a) any such erasure is prohibited under any law; or*
- *(b) it is in the public interest (including historical interest) for the data not to be erased."*

Guidance for Data Users for Compliance with DPP2

- In application systems which hold and process personal data, there should be in place a sound sub-system of recording and updating of personal data to highlight data inconsistencies and optimise data accuracy, e.g. to include features of periodic triggering system to seek personal data updates from customers and employees, and where possible cross checking or referencing from different data sources for data validation.

Guidance for Data Users for Compliance with DPP2

- In application systems which hold and process personal data, there should be in place a sound sub-system of monitoring and triggering data deletion when necessary to comply with the requirements under DPP2 taking into account the requirements under statues, codes of practice and guidelines relevant to data retention and deletion.

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 3 - Use of personal data -

- this provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

USE includes transfer and disclosure

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 4 - Security of Personal Data –

All practicable steps shall be taken to ensure that personal data held by a data user are protected against *unauthorized or accidental access, processing, erasure or other use* having particular regard to -

(a) the kind of data and the *harm* that could result if any of those things should occur;

(b) the *physical* location where the data are stored;

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Data Protection Principle 4
Security of Personal Data

Thomas Parenty
Parenty Consulting Ltd.

Topics

- Summary of DPP4 – Security of Personal Data
- Approach taken in developing recommendations
- Overview of recommendations

DPP Requirements

All **practicable steps** shall be taken to ensure that **personal data** (including data in a form in which access to or processing of the data is not practicable) held by a data user are **protected against unauthorised or accidental access**, **processing**, **erasure** or **other use** having particular regard to-

DPP4 Considerations

- Kind of data and harm that could result
- Physical location(s)
- Security measures incorporated into IT equipment
- Integrity, prudence and competence of data users
- Secure transmission

Approach to Recommendations

- Structured as process, not just list of recommendations
- Addresses lifecycle
  - Development
  - Use
  - Decommissioning
- Practical
- Focus on DPP4, not general security

Define Scope

- What types of personal data will be managed?
- Where will they be stored?
  - Physical locations
  - Computing devices
  - Software (provides security functionality)

Reduce Scope

- Minimize number of locations
- Promote working on data “in place”

Control Access

- Controls based on use
- Designated owner or custodian
- Formal process for assigning and revoking access
- Periodic review

Audit

- Proportionate to risk and consequences
- Integrity of audit trail
- Address administrators
- Audit analysis tools

Identification & Authentication

- First, have it
- Passwords
  - Strong
  - Protected
  - On all devices, including phones

Encryption

- Stored data
- Backups
- Network transmission
  - Public network
  - Private network

Security of Computing Devices

- Organizational control
- Patching
- Malware protection
- Authorized applications

Recycling Computing Devices

- Secure delete before reuse
- Broad view of computing devices, to include:
  - Mobile phones
  - Tablets
  - Printers and copiers

Hard Copy

- Minimize
- Control access to
  - Hard copy
  - Printers that generate hard copy
- Properly dispose of

Organizational Issues

- Job-specific training
  - Administrator versus end user
- DPP apply to third parties, as well

Thank You

HONG KONG COMPUTER SOCIETY

Personal Data (Privacy) Ordinance Data Protection Principles

Principle 5 - Information to be generally available -

- this provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

Privacy Policy Statement (PPS)

- A data user should have a written policy statement, commonly referred as a Privacy Policy Statement (PPS) which states the kind of personal data it held, and the various purposes for which personal data are being used or to be used. Other relevant information, such as the data retention periods and the right of data subjects to access and correct their personal data, would be relevant for reasons of transparency and clarity to gain customers' and employee's confidence.

Personal Data (Privacy) Ordinance Data Protection Principles

- Principle 6 - Access to personal data

- **A data subject shall be entitled to-**
- **(a) ascertain whether a data user holds personal data of which he is the data subject;**
- **(b) request access to personal data-**
- **(i) within a reasonable time;**
- **(ii) at a fee, if any, that is not excessive;**
- **(iii) in a reasonable manner and**
- **(iv) in a form that is intelligible;**
- **(c) be given reasons if a request referred to in paragraph (b) is refused;**
- **(d) object to a refusal referred to in paragraph (c);**
- **(e) request the correction of personal data;**
- **(f) be given reasons if a request referred to in paragraph (e) is refused, and**
- **(g) object to a refusal referred to in paragraph (f).**

Guidance for Data Users for Compliance with DPP6

For IT applications which collect and process personal data, there should be a log subsystem to handle data access and correction requests, which should include such features as:

- Log the date when a data access/correction request is received and monitor related actions of compliance or refusal within the subsequent 40 days;
- Trigger the necessary response to the requestor in good time before the expiry of the 40-day period; and
- Create and maintain a log book on refusals to data access and correction requests and reasons for such refusals.

Exemptions

While PD(P)O generally requires the compliance with the six DPPs and other provisions in personal data handling by data users, there are exceptional circumstances when the overall public interests are taken into consideration. These exceptions are commonly referred to as exemptions.

Generally speaking, most exemptions apply to DPP3 which governs the use of personal data, and DPP6 which provides the right of data access

Exemptions Include

- Recreational Purposes
- Detection and Prevention of Crime
- *the assessment or collection of any tax or duty*
- Health Data *likely to cause serious harm to the physical or mental health of –*

(i) the data subject; or

(ii) any other individual.”

Exemptions Include

Statistics and Research

- Section 62 concerns the use of personal data for preparing statistics or carrying out research. It exempts personal data from the application of DPP3 when the following conditions are satisfied:
- *“(a) the data are to be used for preparing statistics or carrying out research;*
- *(b) the data are not to be used for any other purpose; and*
- *(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them.”*

Checklist for Data Users in Ensuring Compliance with PD(P)O

- Is there any function or activity involving the collection of personal data? Is the collection of personal data directly related to the function or activity?
- What are the purposes of use? Is collection of personal data necessary for or directly related to the purposes? Are the means of collection lawful and fair? Are data collected adequate but not excessive in relation to the purpose?
- What information should be provided to the data subject on or before collection?
- What are the practicable steps taken to ensure data accuracy and how long will the collected personal data be retained before erasure?
- Does the use (which includes disclosure and transfer) of personal data fall within the original purpose of collection or its directly related purpose?

Checklist for Data Users in Ensuring Compliance with PD(P)O

- What are the practicable steps taken to ensure that there are in place adequate security measures so that personal data collected are protected from unauthorised or accidental access, erasure or other uses?
- Are there privacy policies and practices in place and made generally available?
- Are the data access requests and data correction requests received being properly handled?
- Are there any applicable exemptions from compliance with the relevant requirements under PD(P)O?

Thank You

HONG KONG COMPUTER SOCIETY

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on Personal Data (Privacy) Ordinance

Outsourcing and Cloud

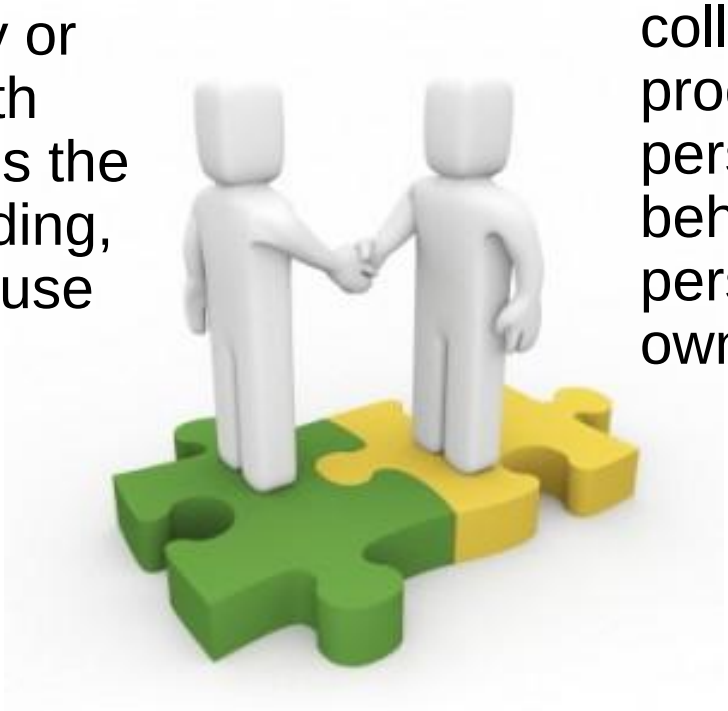
Peter Yan
CEO
Computer And Technologies Solutions

Data Privacy in the Outsourcing / Cloud World

Data User vs Agent

- **Data User**

  alone or jointly or in common with others, controls the collection, holding, processing or use of the data



- **Agent**

  collects, holds, processes or uses personal data solely on behalf of another person, and not for his own purposes

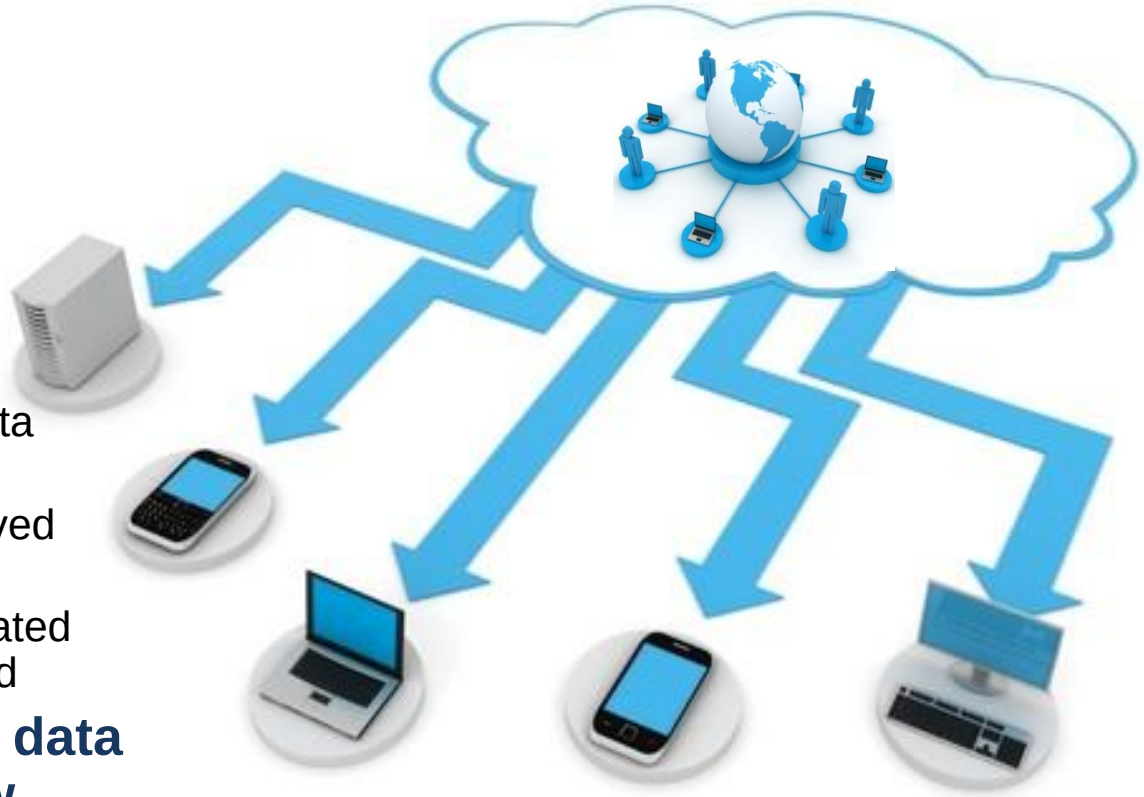
The Right Outsourcing Agent

- **General**
  - √ Company culture
  - √ Privacy by design
- **Contractual**
  - √ Privacy impact assessment
  - √ Operation audits
  - √ Back-to-back employment terms
- **Technical infrastructure**
  - √ System level
  - √ Network level
- **Operation**
  - √ Standard data handling practices specific to outsourcing processes
  - √ Comprehensive end-to-end process

The Right Cloud Service Provider

- **All of the above**

- **Application**
  - √ Sensitivity of the data involved
  - √ Data subjects involved
  - √ How transactional, relationship and related information are used
- **Location of Cloud data and applicable law**
- **Ownership of the Cloud service provider**



Thank You

HONG KONG COMPUTER SOCIETY

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Workplace Monitoring

Susanna Shen
Head of Information Technology
The Hong Kong & China Gas Co. Ltd.

Workplace Monitoring

Workplace monitoring is widely deployed across organizations for a variety of reasons, mainly for protecting organizational interests

Internet Monitoring

CCTV Monitoring

Email Monitoring

Telephone Monitoring

Why do we need Workplace Monitoring?

Manage service quality

Protect a wide range of security requirements

Manage workplace productivity

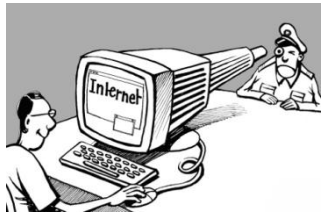
Comply with statutory or regulatory requirements

Common Workplace Monitoring Applications

1. **Email Monitoring**
   employees' use of Email sent and received

2. **Telephone Monitoring**
   telephone calls and voice mails made or received by employees on telecommunications equipment

3. **CCTV Monitoring**
   employees' work activities and behaviors by the use of video recording or CCTV



4. **Internet Monitoring**
   employees' web browsing activities using equipment

General Guidance for Workplace Monitoring

Workplace monitoring applications should be accompanied by the following considerations:

1. Assess appropriateness and necessity of workplace monitoring

2. Assess its impact on the personal data privacy of employees

3. Consider the use of less privacy intrusive alternatives to workplace monitoring where possible

HONG KONG COMPUTER SOCIETY

General Guidance for Workplace Monitoring

4. Overt or Covert monitoring? Determining the parameters for a reasonable expectation of privacy at work

5. Implement a comprehensive Employee Monitoring Policy and Communicate to employees

6. Make known the areas and information being or to be captured by the monitoring applications

General Guidance for Workplace Monitoring

7. Implement appropriate security and access control measures to safeguard security of personal data collected and stored against unauthorized and accidental access or erasure, or wrongful use

8. Specify the retention period of personal data in monitoring records

9. Provide appropriate training to personnel responsible for managing / operating workplace monitoring applications

Specific Guidance for Workplace Applications

1. Email Monitoring, e.g.

- IT administrator should only manage the communications logs for the purpose of proper email system functioning without a need to examine the email content
- Use automatic tools for the purpose of system/security control (E.g. Spam, Virus) for examining the email content digitally without revealing the content

2. Telephone Monitoring, e.g.

- Ensure there is a data access request mechanism in place for customers as well as employees to request access to recording

Specific Guidance for Workplace Applications

3. CCTV Monitoring, e.g.

- A clear notice should be displayed so that people are aware of such monitoring is in operation

4. Internet Monitoring, e.g.

- Aggregate of traffic statistics rather than collecting traffic on individual
- Preventive approach by blocking inappropriate sites is better than detective approach

Do it right…

Clean surfing

Save workplace

Increase productivity

Quality services

Thank You

HONG KONG COMPUTER SOCIETY

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

DIRECT MARKETING (Call Centres & Telemarketing)

John Chiu JP
Chairman – HKCCA
Managing Director – ATG Holding Ltd.

Personal Information in Direct Marketing

- Collection of Personal Information
- Data usage and sharing
- Opt-In and Opt-Out : what is the impact?
- Code of Practice for the DMA and CCA industry

Personal Information in Direct Marketing

Data Collection

- Indicate clearly mandatory and optional elements
- Sensitive data
- State clearly the scope to be used
- Fonts and position of the terms and conditions
- Signatory from the subject for confirmation
- Reconfirm the data content

Personal Information in Direct Marketing
Accuracy and Duration of Retention

- Expiration date for each data fields collected
- Mechanism to automatically obsolete a record after expiry
- Data stored electronically, shred all paper records
- Synchronise updates and amendments between subsets
- Use traceability methodology such as Phantom Clients

Personal Information in Direct Marketing

Usage of Data

- Creating Subsets
- Data recorded to be classified as Personal Data or Common data
- Attributes of each data fields – security levels, users access, usage logs, expiration
- Notify subject when data is to be used
- Maintain Do Not Call List

Personal Information in Direct Marketing
Security

- Data Encryption
- Design sophisticated and drill periodically Data Penetration Tests
- Use Close Network
- Thin Client technology (e.g. M/S Terminal Service; Citrix)
- Avoid usage of PSD
- Only enable essential Data I/O port
- Training for Staff along the work line

Personal Information in Direct Marketing
General Availability & Right of Access

- Facility for subject to obtain copy of the record
- Allow data subject to access and edit information
- Monitor and log data access and correction request
- Inform subject when and which projects and campaign the data is used

Thank You

HONG KONG COMPUTER SOCIETY

Hong Kong Computer Society

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

Personal Data(Privacy) Ordinance

Biometrics

Prof YB Yeung
Adjunct Professor
Department of Information Systems
City University of Hong Kong

Biometrics

Definition

- Measurement of physiological and behavioral characteristics used to identify computer users
- Example: face, fingerprints, iris, DNA, voiceprint, body movement

Applications of biometrics

- For identity authentication
- Capture physical characteristics to create of a digital map ("template")
- Store template in a security system for subsequent authentication during system access
- Example:
  - Access control
  - Identity authentication (eg. HK immigration)
- Fingerprints capture most popular

Personal data privacy guidelines in biometrics applications

DPP1 – only capture biometric data for a lawful purpose; individuals involved should be explicitly informed what data is collected and for what purpose

DPP2 – ensure accuracy of captured biometric data; delete source biometric data after the template is generated; data must not be stored longer than necessary

Personal data privacy guidelines in biometrics applications (2)

DPP3 – use of biometric data must be the same as the stated purpose of collection and use; change of use must have consent of the individual

DPP4 – biometric data must be stored in a secured manner to guard against unauthorised or accidental access, loss, erasure or other use

Personal data privacy guidelines in biometrics applications (3)

DPP5 – the purpose of collecting biometric data must be well documented so that both the individuals and the employees of the data user are fully aware of why the data is collected.

The policy and practice in handling biometric data captured must also be well documented

DPP6 – develop procedures to handle data access requests from individuals for their personal data and correction requests for inaccuracies

Thank You

HONG KONG COMPUTER SOCIETY

A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance

http://www.hkcs.org.hk/en_hk/home/publication/PDPO/