Protection of Personal Data Privacy – Practical Tips for In-house Lawyers

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data, Hong Kong
1. Recent Development in Personal Data Privacy Protection

2. How an Investigations is Carried out

3. How an Inspection is Carried out

4. Disclosure of Customers’ Personal Data For Crime Prevention and Detection

5. How to Improve Transparency on Privacy Policy and Practice
The First Comprehensive Data Protection Law in Asia
The Hong Kong Data Protection Law

The Personal Data (Privacy) Ordinance 1995 (the Ordinance)

- comprehensive and stand-alone
  - covering the public (government) and private sectors
- enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data
The Personal Data Landscape in Asia
The Personal Data (Privacy) Ordinance

6 Data Protection Principles

1. Collection Purpose & Means
   Personal data must be collected in a lawful and fair way for a purpose directly related to a fundamental activity of the data user.
   All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.
   Data collected should be necessary, but not excessive.

2. Accuracy & Retention
   Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3. Use
   Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4. Security
   A data user needs to take practical steps to safeguard personal data from unauthorized or accidental access, processing, damage, loss or use.

5. Openness
   A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

6. Data Access & Correction
   A data subject must be given access to his personal data and to make corrections where the data is inaccurate.
Two Decades of Developments
The First Ten Years – Information Age?

1996 - Code of practice on identity card numbers
1997 - Code of practice on HR management
2000 - Code of practice on consumer credit data
2002 - Code of practice on workplace monitoring
2004 – Guidelines on workplace monitoring

Information age?

Dealing with collection and processing of personal data as information:

• development of awareness
• issued codes of practice on identity card numbers, HR management, consumer credit data, and workplace monitoring
Dealing with collection and processing of personal data by ubiquitous ICT systems:

- capacity building - enforcement framework, outreach programme, etc.
- issued publications on use of Internet, anonymisation, biometric, social networks, cloud computing, online behavioural tracking, mobile app development, data breach handling etc.

Digital age?

2006 - Recommended practice for IT practitioners

2010 - 2016 - 17 publications on ICT matters
How the Octopus Incident Has Changed the Scene
Octopus Card Incident – The Watershed Case

- Information age
- Digital age
- The Octopus incident
- Ordinance amendment

The “Octopus Incident” 2010

• found to have profiteered from the sales of membership data to insurance for direct marketing calls without consent
• management stepped down
• law changed
Amendments in 2012 – Criminalisation of Direct Marketing

Direct Marketing (s.35A - M)
Outsourcing of personal data processing (DPP2(3) & 4(2))

New offence against disclosure of personal data obtained without data user’s consent (s.64)

Legal assistance to affected individuals
Strengthening the Privacy Commissioner’s enforcement power
New exemptions (e.g. legal proceedings etc.)
Direct Marketing (DM) Convictions

1. A telco not honouring opt-out request from a customer
   • named and fined HK$ 30,000 for contravening s.35G(4)

2. A storage company sent a DM message without obtaining prior consent
   • named and fined HK$ 10,000 for contravening s.35C(5)

3. A body-check company not honouring opt-out request from a prior customer
   • named and fined HK$ 10,000 for contravening s.35G(4)

4. An estate agent pass on a social contact to an insurance agent who made DM calls
   • the estate agent was fined HK$ 5,000 for contravening s.35J(5)(b)
   • the insurance agent was acquitted due to uncertainty on whether she could have taken ‘specified actions’ should she be not interrupted in the call

5. An insurance agent obtained client details from his wife and sent a DM letter
   • the insurance agent was ordered 80 hours of community service for contravening s.35C(5) and s.35F(3)

6. A marketing company made DM calls to a customer & not honoured opt-out
   • named and fined HK$ 16,000 for contravening s.35C(5) and s.35G(4)
New Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

1.1 Direct marketing is a common business practice in Hong Kong. It often involves collection and use of personal data by an organization for direct marketing itself and in some cases, the provision of such data by the organization to another person for use in direct marketing. In the process, compliance with the requirements under the Personal Data (Privacy) Ordinance (the “Ordinance”) is essential. This document is issued by the Privacy Commissioner for Personal Data, Hong Kong.

What is “direct marketing”?

1.3 The Ordinance does not regulate all types of direct marketing activities. It defines “direct marketing” as:

(a) the offering, or advertising of the availability of goods, facilities or services; or
Current Outreach Programmes
Building on Solid Foundations – Data Protection Officers’ Club

- provide practising data protection officers with a platform for
  - advancing their knowledge
  - experience sharing
  - training
Workshop topics in 2016

- Data Protection and Data Access Request
- Data Protection in Banking/Financial Services
- Data Protection in Direct Marketing Activities
- Data Protection in Human Resource Management
- Data Protection in Insurance
- Data Protection in Retail Operation
- Legal Workshop on Data Protection
- Practical Workshop on Data Protection Law
- Privacy Management Programme

Building on Solid Foundations – Professional Workshops

- 77 workshops were held with over 2,100 participants in 2015
Building on Solid Foundations – Guidance Notes and Information Leaflets

Guidance Notes

You Are Looking For

Biometric Data

- Guidance on Collection and Use of Biometric Data (July 2015) NEW!

Children Privacy

- Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children (December 2015) NEW!

Corporate Governance

- Privacy Management Programme: A Best Practice Guide (February 2014)

Data Access Request

- Guidance on the Proper Handling of Data Correction Request by Data Users (December 2012)
Building on Solid Foundations – Two Consultative Advisory Committees

Personal Data (Privacy) Advisory Committee:
• to advise the Commissioner on privacy matters

Standing Committee on Technological Developments:
• to advise the Commissioner on matters relevant to the developments in the processing of using technology
Current Challenges
Current Challenges on Technology

Data security incidents:
2015: Contactless credit card leakage recalling 1.25 million cards
2015: VTech data leakage involving 6.3 million kid profiles
2015: SanrioTown (Hello Kitty) exposed of 3.3 million members’ data

Technology developments:
Proliferation of C2B/P2P mobile payment systems, big analytics, Internet of Things
• proportionality – collected data directly related to function?
• transparency – data subjects clearly informed of purposes?
• data security – information protected against eavesdropping/alternation?
Current Insights on Consumer Expectations

Data subject opinion revealed in 2015 survey:

Focus group:
• all participants agreed mandatory breach notification should be in place

Survey:
• 67% serious concern on collection of names-addresses for loyalty cards
• 46% experience misuse of their personal data but 35% of which not filed a complaint because they didn’t want to complain their friends
• 6% will certainly pay HK$20 per month to use ad-free email system (56% will certainly not pay)
• 50% of 40s and under were prepared to provide personal data to exchange convenience
• All those above 41s prepared to provide personal data to exchange benefit/benefit-in-kind
Current Challenges on Legal Developments

Transborder data flow/Free flow of information
2015: Safe Harbor invalidated
2016: Privacy Shield to be implemented
2016: Implications of these to s.33 of the Personal Data (Privacy) Ordinance?

Access to public registers
2015: Study report of 10 public registers published
2016: Company register access formalised
Current Challenges on Legal Developments

GDPR impact to Personal Data (Privacy) Ordinance

Comparative study to be conducted on at least the following areas that are not covered in the Ordinance (first four items):

1. Accountability
   - Commitment to privacy impact assessment, privacy by design etc.

2. Children’s Protection
   - Parental consent is needed for processing children’s personal data

3. Data Breach Notification
   - Mandatory breach notification

4. Data Processor Obligations
   - Processors to implement technical and organisational measures to ensure security
Current Challenges on Legal Developments

GDPR impact to Personal Data (Privacy) Ordinance
Comparative study to be conducted on at least the following areas that are not covered in the Ordinance (last five items):

5. Data Protection Officers
   • Appointment of a DPO in many cases

6. Data Protection Seals
   • Encourage the establishment of data protection seals and marks

7. Fining Power
   • Ability to fine up to 4% of global turnover

8. Right to the Forgotten and Data Portability
   • Individuals have right to request erasure and certain right to port their personal data from one controller to another in a common format

9. Sensitive Personal Data
   • Sensitive personal data is defined and can only be processed upon explicit consent
Future Challenges?
The Third Ten Years – The AI Age?


Information age?
- 1997 - Code of practice on identity card numbers
- 2000 - Code of practice on HR management
- 2002 - Code of practice on consumer credit data
- 2004 – Guidelines on workplace monitoring

Digital age?
- 2006 - Recommended practice for IT practitioners
- 2010 - 2016 - 17 publications on ITC matters

Artificial Intelligence age?

---


Digital age?
The Third Ten Years – Artificial Intelligence Age?

Dealing with collection and processing of personal data for automated decision making?

• can IoT and big data analytics lead to automated decision-making by artificial intelligence that is not easily understandable by human?

• calling for not only compliance, but accountability and algorithmic transparency (how automated decision about individuals are made) to avoid discrimination
Further Surveys

IoT Survey¹:
- 62% of global consumers concerned about privacy
- 54% concerned about security
- 27% concerned about physical safety
- 21% “machines taking over the earth”

Authentic Brands survey²:
- Authentic brands are Reliable, Respectful and Real
  - Respectful brands are “Treat customers well” and “Protect customer data and privacy”
- 71% of consumers would be angry if company sells their personal data
- 67% extremely angry if company fails to protect their personal data

---
¹ www.mobilestrategies360.com/2016/05/05/privacy-iots-highest-hurdle
The Solution?

Liability + Accountability = Asset

Enforcement and compliance + Accountability = Trust

Culture (Protect and Respect)
How to Demonstrate Accountability?

“An accountable organisation must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management programme.”

privacy management programme  ➔  accountability
Privacy Management Programme (PMP)

• from Compliance to Accountability:
  ➢ Hong Kong Government
  ➢ 25 insurance companies
  ➢ 9 telecommunications companies
  ➢ 5 organisations from other sectors

• all pledged to implement PMP
Privacy Management Programme (PMP)

- strategic framework
- good corporate governance
- trust building
- transparency

- 3 organisational commitments, 7 bottom-up controls and 2 review processes
Three top-down management commitments:

1. top-management commitment and buy-in
2. setting up of a dedicated data protection office or officer
3. establishing reporting and oversight mechanism for the privacy management programme
Seven practical programme controls:

1. recording and maintaining personal data inventory
2. establishing and maintaining data protection and privacy policies
3. developing risk assessment tools
4. developing and maintaining training plan for all relevant staff
5. establishing workable breach handling and notification procedures
6. establishing and monitoring data processor engagement mechanism
7. establishing communication so that policies and practices are made known to all stakeholders
PMP Best Practice Guide

Two review processes:

1. the development of an oversight review plan to check for compliance and effectiveness of the privacy management programme

2. the execution of the oversight review plan making sure that any recommendations are followed through
Paradigm Shift

Compliance approach:
- passive
- reactive
- remedial
- problem-based
- handled by legal/compliance
- minimum legal requirement
- bottom-up

Accountability approach:
- active
- proactive
- preventative
- based on customer expectation
- directed by top-management
- reputation building
- top-down

From Compliance to Accountability
How the Privacy Commissioner for Personal Data Carries Out Investigations
How to Deal With an Investigation Carried Out by the Privacy Commissioner

• increased public awareness on personal data privacy

• 2,022 complaint cases received in 2015-16

• types of investigations
  ➢ complaint-driven
  ➢ self-initiated (e.g., data leakage incident affecting a vast amount of individuals)
Complaint Screening Stage

• receipt of complaints
• make preliminary enquiries with the complainant and the party-complained-against
• by written correspondence followed by telephone conversations
• determine whether a prima facie case can be established
• a fact-finding but not fault-finding process
Complaint Handling Chart

- Receipt of Complaints
  - Complaint Screening
    - Screening Out
    - Complain Handling
      - Cases of serious nature
        - Conciliation
          - Conciliation successful
            - Warning/Advisory notice/Resolution
          - Conciliation unsuccessful
            - Formal Investigation
              - Enforcement Notice/Warning
              - Contravention
              - No contravention
Conciliation

- contravention of a data protection principle in the Ordinance is not an offence
- focus on public education as well as enforcement
- assist the data user in complying with the requirements of the Ordinance
- prevent recurrence of a similar breach in future
Conciliation

• examples of follow-up/remedial actions taken by the data user:
  ➢ revise its operational practices and provided proper guidance to its staff
  ➢ delete the personal data unnecessarily collected or disclosed to third parties
  ➢ Provide the PCPD with undertakings to cease the malpractice leading to the alleged contravention
  ➢ provide the complainant with the requested data or reduced the fee for complying with his data access request
Reasons for Cases to Be Closed Under Section 39 of the Ordinance

• remedial actions taken
• the alleged act or practice is trivial
• complaint of vexatious nature
• complaint not made in good faith
• primary subject matter not related to personal data privacy
• no prima facie evidence of any contravention
• no collection of personal data, i.e., the data protection principles are not engaged at all
Complaint Handling Chart

1. Receipt of Complaints
2. Complaint Screening
   - Screening Out
   - Complaint Handling
     - Cases of serious nature
       - Enforcement Notice/Warning
       - Contravention
         - Formal Investigation
         - No contravention
     - Conciliation
       - Conciliation successful
         - Warning/Advisory notice/Resolution
       - Conciliation unsuccessful
Investigation Stage

- **prima facie case of contravention is established but:**
  - the case cannot be resolved through conciliation; or
  - the breach is of a serious nature

- carry out a formal investigation [section 38]

- serve a notice in writing to inform the data user of our intention to carry out the investigation [section 41]
The Commissioner’s Powers of Investigation Under the Ordinance

- to be furnished with any information, document or thing, from such persons, and to make such inquiries, as he may see fit [section 43(1)]

- data user’s response to the allegation

- supporting documents, such as:
  - its correspondence with the complainant or third parties concerning the alleged contravention
  - its internal policy in handling personal data, and procedures or guidelines for its staff to follow at the material time
  - written statement of the staff member concerned (if applicable)
The Commissioner’s Powers of Investigation
Under the Ordinance

• to carry out a public hearing in such manner as he thinks fit [section 43(2)]

• to summon the person in charge before him and to examine that person [section 44(1)]

• to enter premises of the data user to inspect its personal data system [section 42(2)]
Consequence of Obstructing the Commissioner in Exercising His Powers

• anyone who without a lawful excuse obstructs the staff of PCPD in discharging their duties, or make a statement which the person knows to be false, or knowingly misleads the Commissioner commits an offence, is liable on conviction to a maximum fine of $10,000 and imprisonment of 6 months. [section 50B]
Consequence of Obstructing the Commissioner in Exercising His Powers

- a person was charged with an offence of obstructing the Commissioner in exercising his powers to serve the summonses under section 44(1) of the Ordinance
  - the defendant was ordered by the Court to pay a surety of $2,000 and to be bound over for 12 months

- a person was charged with two counts of making a false statement to the Commissioner under section 50B(1)(c)(i) of the Ordinance, and also six counts of various offences under other ordinances
  - the defendant was sentenced to 4 weeks’ imprisonment
Limitation of the Commissioner’s Powers

- no power to conduct search or seize evidence
- no power to carry out a criminal investigation or initiate prosecution
- criminal investigations are conducted by the Police
- prosecutions, where necessary, are initiated by the Department of Justice
Complaint Handling Chart
Completion of an Investigation

• inform the data user and the complainant of the result of investigation [section 47]

• may publish a report setting out the result of investigation and the recommendations and comments arising from the investigation [section 48]

• may serve on the data user an enforcement notice to direct it to take steps to remedy and prevent any recurrence of the contravention [section 50]

• offences relating to enforcement notice (maximum fine of $50,000 and imprisonment for 2 years) [section 50A]

  ➢ non-compliance with an enforcement notice

  ➢ the data user intentionally does the same act or makes the same omission again after its compliance with the enforcement notice
Secrecy Requirement

• section 46

• the Commissioner and other staff of the PCPD are obliged to maintain secrecy in respect of any information obtained in an investigation

• parties will only be informed of the general progress and outcome of their case

• unable to accede to a request for specific information (e.g., for a copy of a letter sent to the PCPD by another party) unless consent is obtained from the relevant party
How the Privacy Commissioner for Personal Data Carries Out Inspections
The Inspection

- section 36 of the Ordinance empowers the Commissioner to carry out an inspection of any personal data system

- an effective tool for the Commissioner to make recommendations to the relevant data user(s) on its / their personal data system for the purposes of promoting compliance with the provisions of the Ordinance, in particular the DPPs
History of Inspections

2008 – Hospital Authority (electronic patient records)
2010 – TransUnion Limited
2011 – The Trial Scheme on School Drug Testing in Tai Po District 2010/11
2012 – MTR Corporation (CCTV system)
2013 – Student Financial Assistance Agency
2014 – Labour Department (employment service)
2015 – Hong Thai Travel Services Limited
History of Inspections

• generally, no material deficiency in the personal data system were found

• examples on rooms for improvement:
  ➢ to document and closely monitor the compliance of their data security procedures
  ➢ effectively disseminate the policies and guidelines in relating to the handling of personal data to their staff
  ➢ to conduct privacy impact assessment to assess the risk and impact on the personal data involved before launch of a program or system
Procedures of an Inspection

Section 41
- Notification to the data user of the Commissioner’s intention to carry out the inspection
- Request for information and documents

Section 47
- Notification to the data user of the result of the inspection

Section 48
- Inspection process – pre-inspection meeting / site inspections / others
- Assessment of the personal data system
- Publication of an inspection report after completion of the inspection, if deemed necessary for the benefit of the industry
Inspection Work by PCPD

• methodology in assessing the relevant personal data system:
  ➢ examination of the relevant operating procedures, policies, manuals and guidelines
  ➢ meeting with the responsible personnel for understanding the flow of the personal data system
  ➢ face-to-face interviews with responsible personnel and relevant staff members
  ➢ site inspection / walk through on the actual operation of the personal data system
Inspection Work by PCPD

• inspection is **NOT** a fraud finding process

• data users are recommended to provide full support to the Commissioner and its designated staff throughout the inspection process

• meetings and discussion during the inspection would facilitate communication on the data user’s personal data system and also help the relevant industry work out an effective and efficient practice and procedures in handling personal data
Disclosure of Customers’ Personal Data For Crime Prevention and Detection
Disclosure of Personal Data to Law Enforcement Agencies

- use of personal data for a new purpose in disclosing personal data to law enforcement agencies – breach of **DPP3** unless exempted or with data subject’s prescribed consent

- section 58 exemption – personal data used for the purpose of (i) prevention or detection of crime; (ii) apprehension, prosecution or detention of offenders; (iii) prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, are exempted from **DPP3** if the application of **DPP3** would be likely to prejudice any of the above matters (data users must be able to show they had reasonable grounds for believing such prejudice)
Disclosure of Personal Data to Law Enforcement Agencies

- exemption provisions are permissive but not mandatory in nature ((section 51))

- s.58(6) provides that “crime” means -
  - an offence under the laws of Hong Kong; or
  - if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place
Cases on Section 58 Exemption

• **AAB No. 5 of 2006**
  - whether or not the specified purposes would likely be prejudiced does not depend on the subjective view of the data user. The standard is an objective one.

• **AAB No. 64 of 2005**
  - mere or general assertion that the personal data is to be used for a purpose under section 58(1) may not be sufficient.
  - AAB criticised the requestor for failing to inform the data user that no consent was obtained from the data subject
  - AAB went further to criticise any collection approach which may lure the data user into the misbelief that it was mandatorily required to provide the information without data subject’s consent
Application of section 58

Prejudice test (section 58(2))

prejudice test: would be likely to prejudice the matters; data user must be able to show that the ground of its belief is reasonable

Given the sensitive nature of most law enforcement operations, the data user may not always be able to obtain clear proof that the “prejudice” test in section 58(2)(b) has been satisfied. Nevertheless, it is still likely that the law enforcement agency may provide some information, or confirmation of a general nature on:

(1) the purpose for which the personal data is to be used;
(2) the reason why the personal data concerned is relevant to or necessary for the purpose;
Application of section 58

By asking for more information listed below, the data user is put in a better position to invoke the defence under section 58(2) in any subsequent proceedings or complaint against it for alleged contravention of DPP3 in the disclosure of the data:

(1) the reason why the data subject’s consent is not obtained by the agency;

(2) whether the personal data can be obtained from other source; and

(3) in particular, how the application of DPP3 would be likely to prejudice the purpose.
How to Improve Transparency on Privacy Policies and Practices
Two Statements

Personal Information Collection Statement

Privacy Policy Statement
Personal Information Collection Statement (PICS)

V. Personal Information Collection Statement:

All personal data submitted will only be used for the purposes which are directly related to this complaint.

You have the right to request access to and correction of your personal data held by us. Request for access should be made in writing to the Data Protection Officer at the address shown in note 7. Please note that you may refuse to comply with a data access request in the circumstances specified in section 20 of the Ordinance, where the requested data relates to information obtained in the course of handling a complaint disclosure of which would constitute a contravention of the requirements under the secrecy provision of the Ordinance.

Sign by complainant:

Date:

[Image of website interface with form fields for data entry and submission]
Privacy Policy Statement (PPS)
Data Protection Principle 1(3)

• data subject be informed of:
  ➢ purposes of data collection
  ➢ classes of persons to whom the data may be transferred
  ➢ whether it is obligatory or voluntary for the data subject to provide the data
  ➢ where it is obligatory for the data subject to provide the data, the consequences for him if he fails to provide the data
  ➢ name or job title and address to which access and correction requests of personal data may be

• notifications in writing?
Data Protection Principle 1(3) (Cont’)

• exceptions
  ➢ repeated collections in same circumstances within 12 months – section 35
  ➢ compliance would be likely to prejudice an exempted purpose specified in Part 8 in relation to DPP6 (e.g., prevention or detection of crime under section 58)
Data Protection Principle 5

• data users to provide:
  ➢ policies and practices in relation to personal data
  ➢ kind of personal data hold
  ➢ main purposes for which personal data is used

• in writing?
Enquiries & Complaints

• in 2015:

<table>
<thead>
<tr>
<th>No. of enquiries</th>
<th>No. of complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPP1(3)</td>
<td>1,800</td>
</tr>
<tr>
<td>DPP5</td>
<td>70</td>
</tr>
</tbody>
</table>

• important to have proper PICS & PPS
Contents of PICS

• statement of purpose
• statement as to whether it is obligatory or voluntary for the individual to supply his personal data
• statement of possible transferees
• statement of rights of access and correction and contact details
• direct marketing, where applicable (sections 35C & 35J)
• tailor-made for each collection
Contents of PPS

• statement of policy: overall commitment in data protection

• statement of practices:
  ➢ kind of personal data held
  ➢ main purposes for which the personal data issued
  ➢ other useful information, e.g. retention policy, disclosure of personal data, protection measures, etc.

• contact details for enquiries
Language & Presentation

• user-friendly
• easily readable and understandable in terms of length, complexity, font size and accessibility
• avoid highly legalistic language
Purpose Statement

• not too vague and too wide in scope:
  ➢ “The personal data that you provide us may be used by us as a source of data for other related purposes according to industry practice.”

• specify specific practice:
  ➢ “The information collected from you will be used for the purpose of processing your purchase orders and managing your account with us.”
Classes of Data Transferees

• avoid using broad and general terms:
  ➢ “any person”,
  ➢ “any business partners”
  ➢ “any other person under a duty of confidentiality to us”

• define class of transferees by its distinctive features:
  ➢ “financial services companies”
  ➢ “telecommunications service provider”
Headings & Layered Approach

• proper headings:
  ➢ “What personal data we collect”
  ➢ “How we use your personal data”

• layered approach:
  ➢ first layer: a key statement
  ➢ second layer: more in-depth explanation

• use of icons, graphics or animations to simply the communications
Regular Review & Update

• reflect current privacy policies and practices
• state last review date
Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement
Sweat & Glory Seminar on Data Privacy