Asia Privacy Bridge Forum
11 May 2016

Hong Kong’s
Personal Data (Privacy) Ordinance

Fanny Wong
Deputy Privacy Commissioner for Personal Data
Hong Kong, China
The Personal Data Landscape in Asia

The Personal Data (Privacy) Ordinance 1995

• stand-alone legislation
• Regulating **both** the public (government) and private sectors
• enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data (PCPD)
Six Data Protection Principles (DPPs)

1. **收集目的及方式 Collection Purpose & Means**
   - Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.
   - All reasonable steps shall be taken to verify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.
   - Personal data should be necessary but not excessive.

2. **准确性储存及保留 Accuracy & Retention**
   - Personal data is accurate and not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3. **使用 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. **保安措施 Security**
   - A data user must take practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

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

6. **查阅及更正 Data Access & Correction**
   - A data subject must be given access to his personal data and be made corrections where the data is inaccurate.
The Amendment Ordinance 2013

The Personal Data (Privacy) Ordinance in 1995 and effective in 1996

Overhauling of the Ordinance initiated in 2007

New provisions (including outsourcing of data processing) unrelated to direct marketing and legal assistance took effect on 1 October 2012

New provisions relating to direct marketing and legal assistance took effect on 1 April 2013

IT advances + rising trend of outsourcing of data processing (IPCC case in 2006)

Rapid advancement in IT and widespread use of Internet (online distribution of nude photographs of artistes in 2008)

Commonplace of misuse of personal data in business sector (Octopus case in 2010)
New Provisions on Direct Marketing Activities

Prior to 1 April 2013 : “opt-out” mechanism (s.34)
After 1 April 2013 : “opt-in” mechanism, respect data subject’s right of self-determination (new provision s.35A-M)

Catalyst cause: inappropriate handling of personal data by “Octopus” and various large-sized organisations such as banks, telecommunications and insurance companies for direct marketing purposes
Octopus Card

- Stored-value payment card
- Payment for public transport (underground/train/bus/ferry)
- Corner shops, supermarkets, fast-food stores
- On and off street parking
- Access to residential and commercial building
“Octopus Incident” 2010

Personal Data collected for the management of Octopus Card

Sold

Insurance Companies for making Direct Marketing calls without informing their members of such sales
“Octopus Incident” 2010

Octopus sold personal data of customers for HK$44m

Octopus CEO Resigns Over Data Sale

Octopus chairman to step down in Dec
# Problems Revealed in Octopus Incident & the Remedies in New Direct Marketing Provisions

<table>
<thead>
<tr>
<th>Problems revealed</th>
<th>New measures against data users</th>
</tr>
</thead>
<tbody>
<tr>
<td>No requirement for “opt-in” at the collection stage <em>(Not even an opt-out option in the Octopus Incident)</em></td>
<td>• Must take specified actions and obtain data subject’s express consent before using personal data for direct marketing</td>
</tr>
<tr>
<td>Personal data was shared with business partners for monetary gains without obtaining data subject’s prescribed consent</td>
<td>• Must take specified actions and obtain data subject’s consent before such transfer to third party for direct marketing</td>
</tr>
</tbody>
</table>
| Insignificant fine for breach of opt-out request (repealed) : maximum fine of HK$10,000 | • Maximum penalty for breach:  
  • fine of HK$1,000,000 and 5 years’ imprisonment (transfer personal data for direct marketing for gain);  
  • HK$500,000 and 3 years (for others) |
# New Provisions on Outsourcing of Personal Data Processing (DPPs 2 & 4)

<table>
<thead>
<tr>
<th>Issues to be dealt with</th>
<th>New requirements</th>
</tr>
</thead>
</table>
| Data processor’s unnecessary retention of personal data obtained from data user         | If a data processor is engaged, whether within or outside HK, data user must adopt contractual or other means to prevent:  
- unnecessary retention by the data processor (DPP 2)  
- unauthorised or accidental access, processing, erasure, loss or use of data transferred for processing purposes (DPP 4) |
| Commonplace of unauthorised or accidental access, processing, erasure, loss or use of personal data transferred to data processor |                                                                                                                                                                                                                 |
Impact on Business

Public awareness (direct marketing and data processing):

• before - 1 seminar / month for 60 people
• after - demand on talks rocketed
  • average 8-10 seminars / month
  • targeting more specialised audience (finance, HR, IT, insurance, and direct marketing industries)

Public’s increased awareness of their rights to personal data privacy → more complaints to the business and to PCPD(HK)
Impact on Business

Increased use of Privacy Impact Assessments (PIAs) by organisations:

- government – PIAs included in government projects that involve personal data (Transport Department - new speed camera; Immigration Department - smart ID card)

- private sector – sizable companies

Public’s increased awareness:

- of their rights to personal data privacy resulting in more complaints to the business and to PCPD(HK)
Relevant Enforcement and Survey Activities of the PCPD (HK)

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints received</td>
<td>1,179</td>
<td>1,486</td>
<td>1,213</td>
<td>1,792</td>
<td>1,702</td>
<td>1,971</td>
</tr>
<tr>
<td>Enquiries received</td>
<td>18,000</td>
<td>18,680</td>
<td>19,053</td>
<td>24,161</td>
<td>17,328</td>
<td>18,456</td>
</tr>
</tbody>
</table>

Regular opinion surveys on individuals and organisations:
Stakeholders’ Engagement on Topical Issues

- 2002 Employee Monitoring and Personal Data Privacy at Work
- 2006 Property Management Practice
- 2006 Hotel Management Practice
- 2006 Youth Attitude
- 2007 Use of the Internet by Youths
- 2008 Estate Agency Practice
- 2009/2010 Ordinance Review
- 2011 Property Management Practice
- 2012 Insurance Industry Practice
- 2013 Retail Industry Practice
- 2014 Banking Industry Practice
- 2015 Protection of Personal Data in Public Registers
- 2016 Electronic Health Record Sharing System
Publications issued by the PCPD (HK)

Code of Practice & Guidelines

• Code of Practice on Consumer Credit Data
• Code of Practice on Human Resource Management
• Code of Practice on the Identity Card Number and Other Personal Identifiers
• Privacy Guidelines: Monitoring and Personal Data Privacy at Work
Publications issued by the PCPD (HK)

Guidance Notes
• Best Practice Guide for Mobile App Development
• Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children
• Guidance for Data Users on the Collection and Use of Personal Data through the Internet
• Guidance on CCTV Surveillance and Use of Drones
• Guidance on Collection and Use of Biometric Data
• Guidance on Data Breach Handling and the Giving of Breach Notifications
• Guidance on Electioneering Activities
• Guidance on Personal Data Erasure and Anonymisation
• Guidance on Personal Data Protection in Cross-border Data Transfer
• Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement
• Guidance on Property Management Practices
• Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry
• Guidance on the Proper Handling of Customers' Personal Data for the Insurance Industry
• Guidance on the Proper Handling of Data Correction Request by Data Users
• Guidance on the Use of Portable Storage Devices
• Guidance on Use of Personal Data Obtained from the Public Domain
• New Guidance on Direct Marketing
• Personal Data Privacy : Guidance for Mobile Service Operators
• Privacy Management Programme: A Best Practice Guide
• Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users
Publications issued by the PCPD (HK)

Information Leaflets

- A Guide for Data Users - Compliance with Data Access and Correction Requests
- About the Office of the Privacy Commissioner for Personal Data, Hong Kong
- An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012
- Care for Patients - Protect Their Personal Data
- Cloud Computing
- Compliance Guide for Employers and Human Resource Management Practitioners
- Human Resource Management: Some Common Questions
- Matching Procedure: Some Common Questions
- Offence for disclosing personal data obtained without consent from the data user
- Online Behavioural Tracking
- Outsourcing the Processing of Personal Data to Data Processors
- Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)
- Personal Data Privacy Protection: What Mobile Apps Developers and their Clients should know
- Privacy Impact Assessments
- Privacy Implications for Organisational Use of Social Networks
Industry-specific Privacy Campaign

- launched in January 2015
- theme = “Developing Mobile Apps: Privacy Matters”
- co-organised by 10 leading trade associations; supported by 10 ICT professional/academic institutions
Data Protection Officers’ Club

• provide practising data protection officers with a platform for
  – advancing their knowledge
  – experience sharing
  – training
Data Protection Officers’ Club

Number of DPOC members since establishment

267

Professional Compliance Workshops

- 77 workshops were held with over 2100 participants in 2015

<table>
<thead>
<tr>
<th>Workshop topics in 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Protection and Data Access Request</td>
</tr>
<tr>
<td>• Data Protection in Banking/Financial Services</td>
</tr>
<tr>
<td>• Data Protection in Direct Marketing Activities</td>
</tr>
<tr>
<td>• Data Protection in Human Resource Management</td>
</tr>
<tr>
<td>• Data Protection in Insurance</td>
</tr>
<tr>
<td>• Data Protection in Retail Operation</td>
</tr>
<tr>
<td>• Legal Workshop on Data Protection</td>
</tr>
<tr>
<td>• Practical Workshop on Data Protection Law</td>
</tr>
<tr>
<td>• Privacy Management Programme</td>
</tr>
</tbody>
</table>
Support for Small-Medium Enterprises

- self-training module on protection of personal data for SMEs
Online Resources

- online training platform
- Code of Practices / Guidelines, Guidance Notes, Information Leaflets
Privacy Management Programme (PMP)

encourage organisations to
• embrace personal data privacy protection as part of their corporate governance responsibilities and
• apply it as a top-down business imperative throughout the organisation
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
Consultation on Implementing PMP in the Public Sector

November 2015 - to facilitate three HK Government bureaux/departments to implement PMP

Deliverables (toolkits and training) will be beneficial to organisations (public or private) implementing PMP
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
Effect of Paradigm Shift

Enforcement and compliance + Accountability = Trust

Culture (Protect and Respect)

Liability Asset
Change of Business Attitude

A research and consultation study on “Hong Kong Accountability Benchmarking Micro-Study” conducted in early 2015

Purpose: to understand the current status of how privacy is being managed in Hong Kong
Change of Business Attitude

Participating organisations (PMP-pledged organisations and members of the PCPD’s Data Protection Officers’ Club) have:

**implemented** activities that focus on legal compliance requirements and a specific Code of Practice (HR Management) issued by PCPD(HK)

**invested** heavily in privacy and data protection measures related to technical and security measures, records retention, data privacy notices and policies, requirements for processors, and managing and responding to access requests
Change of Business Attitude

• further developing the privacy management programme in training and awareness; managing third-party risk; access requests, inquiries and complaints; expanding privacy impact assessments programmes and implementing privacy by design procedures; and testing incident and breach protocols

• a higher percentage of organisations in Hong Kong implementing personal data inventory and data classification