University Privacy Campaign

Introduction to the

Personal Data (Privacy) Ordinance
Personal Data (Privacy) Ordinance

Legislative Background

• Personal Data (Privacy) Ordinance came into effect on 20 December 1996
• Based on internationally accepted data protection principles
• Legal privacy right in the handling of personal data
• Legal cross-border transmission of personal data to facilitate the development of e-commerce
Personal Data (Privacy) Ordinance

Amendment of the Ordinance

• Gazette published on 6 July 2012
• Reasons for amendment:
  – came into effect more than 15 years
  – rapid advancement in information technology and widespread use of the Internet
  – commercial value of personal and the growing popularity of e-commerce
  – misuse of personal data and frequent occurrence of data leakage
  – enhancing personal data protection by keeping in line with the international standard
Personal Data (Privacy) Ordinance

Amendment of the Ordinance

• Effective dates of the Amendment Ordinance:

  1) provisions unrelated to direct marketing or the legal assistance scheme took effect on 1 October 2012;

  2) provisions relating to direct marketing and the legal assistance scheme came into effect on 1 April 2013;
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.
Definitions under the Ordinance

“Data”: any representation of information in any document, including expression of opinion or personal identifier (e.g. ID Card Number).
“Document”: In addition to written document, “document” includes visual or non-visual device, e.g. photo, audio tape, video tape, optical disc.
Definitions under the Ordinance

Other examples of “Document”:
Examples of Personal Data

**Student:**
- Name, age, address, past and current academic record, interview record, teachers’ comments, etc.

**Staff members:**
- Resume, tax return, medical record, interview record, performance appraisal report
The Ordinance Governs All Data Users

“Data User”

- Any person (including private and public sector organizations and government departments) that controls the collection, holding, processing or use of “personal data”.

[Images of different organizations and a cartoon character]
Data Protection Principles under the Ordinance

• The six data protection principles form the base of the Ordinance.

• Data users must comply with the six data protection principles in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data.
Six Data Protection Principles (DPPs)

- DPP 1 — Purpose and manner of collection
- DPP 2 — Accuracy and duration of retention
- DPP 3 — Use of personal data
- DPP 4 — Security of personal data
- DPP 5 — Information to be generally available
- DPP 6 — Access to personal data
Principle 1 – Purpose and manner of collection

- shall be collected for purposes related to the functions or activities of the data user
- the data collected should be adequate but not excessive
- the means of collection must be lawful and fair
Example of unfair collection – blind advertisement

**Company Assistant**
- Form 5 or above
- Knowledge of company secretarial duties

Please send resume to PO Box 100

**Company Assistant**
- Form 5 or above
- Knowledge of company secretarial duties

Interested parties please contact Miss Chan on 2808-xxxx

• Submission of personal data by job applicants
• No identity of the employer provided
• No notification of purpose of use of the data
• Job applicants are denied of data access rights

• No submission of personal data by job applicants
• Contact person provided from whom applicants:
  - may seek to identify the employer
  - may seek information about purpose statement
inform the data subject of the following immediately or in advance:

a) the purposes of data collection;

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

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

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

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

Personal Information Collection Statement pertaining to Recruitment

The personal data collected in this application form will be used by the Alpha Corporation to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Personal Data Access Form" and forward it to our Data Protection Officer in the Human Resources.
Principle 2 – 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 fulfillment 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.

“Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors”
Principle 3 – Use of personal data

• Personal data shall not, without the prescribed consent of the data subject, be used for **a new purpose**.

• Allow a “relevant person” to give prescribed consent for the data subject under specified conditions.

*New purpose means any purpose other than the purposes for which they were collected or directly related purposes.*
Principle 4 – Security of personal data

• All practicable steps shall be taken to ensure that personal data are protected against unauthorized 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 unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

"Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors"
Principle 5 – Information to be generally available

Data users have to provide

(a) policies and practices in relation to personal data;

(b) the kind of personal data held;

(c) the main purposes for which personal data are used.
Principle 6 – Access to personal data

• A data subject shall be entitled to
  (a) request access to his/her personal data;
  (b) request correction of his/her personal data.

• Data user may charge a fee for complying with the data access request
PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM

Important Notice to Requester:

1. Please read this Form and the footnotes carefully before completing this Form. Where this Form contains a summary of the relevant requirements under the Personal Data (Privacy) Ordinance (the “PDPO”), the summary is provided for reference purpose only. For a complete and definitive statement of the law, please refer to the PDPO itself.

2. This Form is specified by the Privacy Commissioner for Personal Data (“the Commissioner”) under section 5(7) of the PDPO with effect from 1 October 2012. The data user may refuse to comply with your data access request (“your request”) if it is not made in this Form (see section 20(3)(b) of the PDPO).

3. Please complete this Form in Chinese or English. The data user may refuse to comply with your request if your request is not made in either language (see section 10(3)(c) of the PDPO).

4. To make a data access request, you must either be the data subject or a “relevant person” as defined in section 1 or 1A of the PDPO (please refer to Part II of this Form).

5. You are entitled to access data which are personal data or personal data not belonging to you (see section 18(1) of the PDPO). The data user is only required to provide you with a copy of your personal data rather than a copy of the document containing your personal data. In most situations, the data user may elect to provide a copy of the document concerned. If the personal data you request is recorded in an audio form, the data user may provide a transcript of that part of the audio record which contains your personal data.

6. It is important that you specify in this Form clearly and in detail the personal data that you request. The data user may refuse to comply with your request if you have not supplied them with such information as he may reasonably require to locate the requested data (see section 20(3)(b) of the PDPO). If you supply any false or misleading information in this Form for the purpose of having the data user comply with your request, you may commit an offence (see section 18(5) of the PDPO).

7. Do not send this Form to the Commissioner. The completed Form should be sent directly to the data user to whom you make your request.

8. The data user may require you to provide identity proof such as your Hong Kong Identity Card and may charge a fee for complying with your request (see sections 20(3)(a) and 22(2) of the PDPO).

9. The data user may refuse to comply with your request in the circumstances specified in section 20 of the PDPO.

10. You are required by section 19(1) of the PDPO to comply with a data access request within 40 days after receiving the same. To comply with a data access request means: (a) if you hold the requested data, to inform the requestor in writing that you hold the data and supply a copy of the data; or (b) if you do not hold the requested data, to inform the requestor in writing that you do not hold the data (except that the Hong Kong Police may inform the requestor orally if the request is whether it holds any record of criminal conviction of an individual). A mere notification given to the requestor to collect the requested data or a note sent to the requestor for payment of a fee is insufficient. In complying with the request, you should omit or otherwise not disclose the names or other identifying particulars of individuals other than the data subject.

11. If you are unable to comply with the data access request within the 40-day period, you must inform the requestor in writing that you are unable and the reasons, and comply with the request to the extent, if any, that you are able to within the same 40-day period, and thereafter comply or fully comply, as the case may be, with the request as soon as practicable (see section 19(2) of the PDPO).

12. If you have a lawful reason for refusing to comply with the request pursuant to section 20 of the PDPO, you must give the requestor written notification of your refusal and your supporting reasons within the same 40-day period (see section 21(1) of the PDPO).

13. It is an offence not to comply with a data access request in accordance with the requirements under the PDPO. Any data user convicted of such an offence is liable to a fine at level 3 (currently set at HK$10,000) (see section 64A(1) of the PDPO).

14. You may charge a fee for complying with a data access request, but section 23(3) of the PDPO provides that “no fee imposed for complying with a data access request shall be excessive”. The PDPO does not define the meaning of “excessive” with regard to imposing a data access request fee. According to the principle laid down in the decision of Administrative Appeal No. 17/2009, a data user is only allowed to charge the requestor for the costs which are “directly related to and necessary for” complying with a data access request.

15. You shall refuse to comply with a data access request—
(a) if you are not supplied with such information as you may reasonably require—
(i) in order to satisfy you as to the identity of the requestor;
(ii) where the requestor purports to be a relevant person, in order to satisfy you—
(A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and
(B) that the requestor is such a person in relation to that individual;
(b) subject to section 20(2) of the PDPO, if you cannot comply with the request without disclosing personal data of which any other individual is the data subject unless you are satisfied that the other individual has consented to the disclosure of the data to the requestor, or
New Regulatory Regime of Direct Marketing

• Part VIA of the Ordinance: 35A to 35M

• More stringent regulation and higher penalties

• 「Opt-out Mechanism」 unchanged
Use of Personal Data in Direct Marketing

• What is Direct Marketing?

“Direct Marketing” is defined to mean

a. the offering, or advertising of the availability, of goods, facilities or services; or

b. the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

through *direct marketing means*
Use of Personal Data in Direct Marketing

• “Direct marketing means” is further defined to mean
  a. sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or
  b. making telephone calls to specific persons.
New Regulatory Regime of Direct Marketing
(effective from 1 April 2013)

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

Data User Notification

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

Data Subject Consent

- Should be given explicitly and voluntarily
- “consent” includes an indication of “no objection”
**New Regulatory Regime of Direct Marketing**  
*(effective from 1 April 2013)*

**Prescribed information**:

<table>
<thead>
<tr>
<th>Use of Personal Data in Direct Marketing</th>
<th>Provide Personal Data to another person for Use in Direct Marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The data user intends to use the personal data of the data subject for direct marketing;</td>
<td>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;</td>
</tr>
<tr>
<td>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;</td>
<td>2. The data user may not so provide the data unless it has received the data subject’s <strong>written consent</strong> to the intended provision;</td>
</tr>
<tr>
<td>3. The kinds of personal data to be used;</td>
<td>3. The provision of the data is <strong>for gain</strong> (if it is to be so provided);</td>
</tr>
<tr>
<td>4. The classes of marketing subjects in relation to which the data is to be used;</td>
<td>4. The kinds of personal data to be provided;</td>
</tr>
<tr>
<td>5. The response channel</td>
<td>5. The classes of persons to which the data is to be provided;</td>
</tr>
<tr>
<td></td>
<td>6. The classes of marketing subjects in relation to which the data is to be used; and</td>
</tr>
<tr>
<td></td>
<td>7. The response channel</td>
</tr>
</tbody>
</table>
“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

Return the signed form but did not check the box indicating objection = consent
## New Regulatory Regime of Direct Marketing
### Higher Penalties for Non-Compliance

<table>
<thead>
<tr>
<th>Non-Compliance</th>
<th>Maximum Fine (HK$)</th>
<th>Maximum Imprisonment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliance</td>
<td>500,000</td>
<td>3 years</td>
</tr>
<tr>
<td>Non-Compliance if the personal data is provided to third party for its use in direct marketing in exchange for gain</td>
<td>1,000,000</td>
<td>5 years</td>
</tr>
</tbody>
</table>
Guidance to help data user

- "New Guidance on Direct Marketing" (Jan 2013 edition), explaining the requirements under the new regime and providing practical guidance to data users.
- Professional Workshop, to familiarise organisations with the new provisions and compliance measures.
Offences

• Contravention of DPP is not an offence. The Commissioner may serve an enforcement notice on the relevant data user directing the data user to remedy the contravention.

• Non-compliance with an enforcement notice commits an offence and carries a penalty of a fine at $50,000 and imprisonment of 2 years.

• Same infringement of the second time commits an offence and carries a penalty of a fine at $50,000 and imprisonment of 2 years.

• Repeated non-compliance with enforcement notice carries a penalty of a fine at $100,000 and imprisonment of 2 years, in case of a continuing offence, a daily fine of $2,000.
Offences

• Section 64 provides that “A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user’s consent –
  a) With an intent –
    1) to obtain gain in money or other property, whether for the benefit of the person or another person; or
    2) to cause loss in money or other property to the data subject; or
  b) the disclosure causes psychological harm to the data subject.

• Maximum penalty: a fine of $1,000,000 and 5 years’ imprisonment
Compensation

• New section 66B: Privacy Commissioner can grant assistance to data subject in respect of these legal proceedings
Code of Practice

- Identity Card Number and other Personal Identifiers
- Human Resource Management
- Consumer Credit Data
Guidelines and leaflets

• Information Leaflet: An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012

• Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors

• Information Leaflet: Offence for disclosing personal data obtained without consent from the data user
Guidelines and leaflets

- New Guidance on Direct Marketing
- Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement
- Monitoring and Personal Data Privacy at Work
- Guidance on Collection of Fingerprint Data
- Guidance on CCTV Surveillance Practices
- Guidance on Data Breach Handling and the Giving of Breach Notification
Guidelines and leaflets

- Guidance on the Use of Portable Storage Devices
- Guidance for Data User on the Collection and Use of Personal Data through the Internet
- Guidance on Personal Data Erasure and Anonymisation
- Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users
Contact Us

- Hotline  - 2827 2827
- Fax      - 2877 7026
- Website  - www.pcpd.org.hk
- E-mail   - enquiry@pcpd.org.hk

Address  - 12/F, 248 Queen’s Road East, Wanchai, HK

© Office of the Privacy Commissioner for Personal Data, 2013

The above PowerPoint may not be reproduced without the written consent of the Office of the Privacy Commissioner for Personal Data.