



保障資料主任聯會

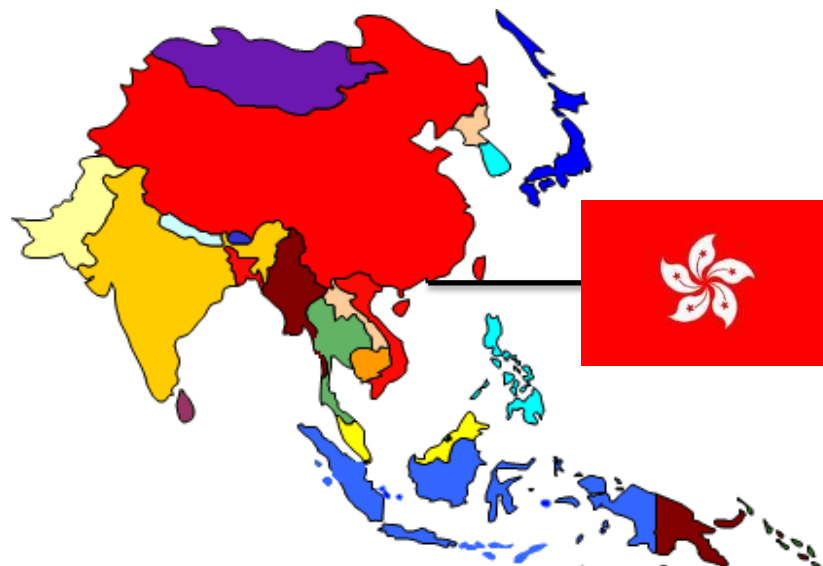
DATA
PROTECTION
OFFICERS'
CLUB

Introduction to the Personal Data (Privacy) Ordinance

Ms Carol CHAN
Manager (Communications and Education)
22 December 2016

Personal Data (Privacy) Ordinance

- single and comprehensive legislation
- covers the public (government) and private sectors
- enforced by an independent statutory regulatory body,
Privacy Commissioner for Personal Data
- no extra-territorial jurisdiction
- came into effect on 20 December 1996



What is “Personal Data”?

“**Personal data**” must fulfill the following three criteria:

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

Eastweek Publisher Limited and Another v Privacy Commissioner for Personal Data



Eastweek Publisher Limited and Another v Privacy Commissioner for Personal Data

Collection of personal data

- Eastweek Publisher Limited and Another v Privacy Commissioner for Personal Data [2000] 2HKLRD83
 - A magazine took pictures of the complainant while walking in the street, and published her picture with unflattering comments on her style of dress

Eastweek Publisher Limited and Another v Privacy Commissioner for Personal Data

- “It is... of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify. The data collected must be an item of personal information attaching to the identified subject, ...”
- If no collection of personal data, the data protection principles would not be engaged at all

Data Protection Principles ("DPPs")

- all persons who use personal data (data users) must comply with the six DPPs at the core of the PDPO
- the six DPPs cover every item of personal data in the **whole data cycle** from collection, retention, use to destruction

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1

收集目的及方式 Collection Purpose & Means



資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

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.

收集的資料是有實際需要的，而不超乎適度。

Data collected should be necessary but not excessive.

2

準確性儲存及保留 Accuracy & Retention



資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達成原來目的的實際所需。

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

使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

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



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5

透明度 Openness



資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

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

查閱及更正 Data Access & Correction



資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

DPP 1 – Purpose and manner of collection

DPP1(1)

- **No collection unless**
 - (a) lawful purpose directly related to a function or activity of the data user
 - (b) necessary for or directly related to that purpose
 - (c) data adequate but not excessive

DPP 1 – Purpose and manner of collection

Case sharing 1: Collection of offenders' date of birth

- complainant committed an alleged fixed penalty offence
- complained that the government officer had collected his date of birth (DOB)
- DOB was used for calculating the age of the offender
- collection of age would be sufficient
- contravention of DPP1(1)
- ceased the practice and deleted DOB previously collected

DPP 1 – Purpose and manner of collection

Case sharing 2: Collection of identification document number from non-account holder

- complainant (a non-account holder) went to a bank to change his HK\$500 note into five HK\$100 notes
- counter officer recorded his name and HKID card number according to bank policy
- no prima facie evidence of money laundering or terrorist financing , and the transaction value is low
- contravention of **PI Code & DPP1(1)**

DPP 1 – Purpose and manner of collection

DPP1(2)


- Means of collection must be
 - (a) lawful; and
 - (b) fair in the circumstances of the case
- × deceptive or misleading means (e.g. in a cold call, misrepresenting to be calling from another company)
- × bundled consent

DPP 1 – Purpose and manner of collection

Case sharing 3: unfair collection of employees' fingerprint data

- a company collected and recorded of employees' fingerprint data for attendance purpose
- did not offer a free choice
- did not inform employees' of the purpose of collection and whether there were any other options
- contravention of **DPP1(2)**

Example of unfair collection – blind advertisement




Company Assistant

- Form 5 or above
- Knowledge of company secretarial duties

Please send resume to PO Box 100

- 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

Company Assistant

- 
- Form 5 or above
 - Knowledge of company secretarial duties

**Interested parties please contact
Miss Chan on 2808-xxxx**

- 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

DPP 1 – Purpose and manner of collection

DPP1(3)

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.

Personal Information Collection Statement

Practical Tips :



design the layout of PICS (including font size, spacing and use of appropriate highlights) in an easily readable manner



present PICS in a conspicuous manner, e.g. in a stand-alone notice or section



use reader friendly language, e.g. simple words



provide further assistance to customers such as help desk or enquiry service



should not state the purpose of use and class of transferees in general and vague terms

- “Guidance Note on Preparing Personal Information Collection Statement and Privacy Policy Statement”

Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement

Introduction

This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement (“PICS”) and Privacy Policy Statement (“PPS”). Both PICS and PPS are important tools used respectively for complying with the requirements of Data Protection Principle (“DPP”) 1(3) and DPP5 under the Personal Data (Privacy) Ordinance (the “Ordinance”).

DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can ascertain its policies and practices in relation to personal data and is informed of the kind of personal data held by the data user and the main purposes for which personal data held by a data user is or is to be used.

The legal requirements

DPP1(3) specifies the collection...

What is personal data?

“Personal data” means information...

指引資料

擬備收集個人資料聲明及私隱政策聲明指引

引言

本指引旨在為資料使用者在擬備《收集個人資料聲明》及《私隱政策聲明》方面提供參考。《收集個人資料聲明》及《私隱政策聲明》分別是資料使用者依從《個人資料(私隱)條例》(「條例」)保障資料第1(3)原則(「第1(3)原則」)及第5原則(「第5原則」)規定的重要工具。

法律規定

第1(3)原則規定，資料使用者在直接向資料當事人收集個人資料時，須採取所有合理地切實可行的步驟，以確保：

- 在收集資料當事人的個人資料之時或之前，以明確或暗喻方式告知資料當事人，他是可以自願或有責任提供該個人資料(如屬有責任，他不提供該個人資料的後果)；及

甚麼是個人資料？

根據條例，「個人資料」指符合以下說明的任何資料：

- 直接或間接與一名在世的個人有關的；
- 從該資料直接或間接地確定有關的個人的身份是切實可行的；及
- 該資料的存在形式令予以查閱及處理均是切實可行的。

資料使用者經常會特意地收集或查閱各類人士的個人資料，並有意或試圖確定這些人士的身份。在某些情況下，其收集的資料總結起來，可能已經足以識別出個別人士的身份。例如，一間公司追蹤記錄顧客對其產品或服務的消費行為，以便鎖定某類顧客為目標以進行推廣。

甚麼是《收集個人資料聲明》及《私隱政策聲明》？兩者有何分別？

DPP 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

DPP 2 – Accuracy and duration of retention

Case sharing 4: Inland Revenue Department failed to take all reasonably practicable steps to ensure the accuracy of a taxpayer's address

- complainant received Tax Return from IRD at home address, completed and returned it
- failing to receive Tax Demand, sent 4 emails to IRD; no reply, called IRD's hotline and visited IRD's office to meet an IRD officer

DPP 2 – Accuracy and duration of retention

- Officer A wrongly attached the Appendix of another taxpayer to the Main Return of the Complainant
- Officer B updated IRD database without checking the file numbers on the Appendix and Main Return; Tax Demand sent to wrong address and returned undelivered;
- Officer C attempted to rectify by checking the tax return of Complainant's employer but wrongly input "Flat A" instead of "Flat F"; Tax Demand sent to another wrong address but never returned

DPP 2 – Accuracy and duration of retention

- After receipt of Complainant's enquiry emails, Officer D simply instructed subordinate to resend copies of Tax Demand according to database, as many as three times
- Remedial actions – revise Tax Return to incorporate address change into the Main Return; daily supervisory checking on at least 10% of address amendments

Accuracy of Medical Opinions

- The Complainant was diagnosed as having “serious psychosis” by a psychiatry clinic of the Hospital Authority (“HA”), and he later sought consultation at a private clinic and was diagnosed as having “anxiety disorder”. He then lodged a complaint with the PCPD against the HA for holding inaccurate medical records about him.
- No contravention of DPP2
- According to the AAB, medical opinions about judgment of the mental condition of a data subject were the professional judgment of the doctor, and its accuracy was not within the jurisdiction of the Ordinance or the PCPD

DPP 2 – Accuracy and duration of retention

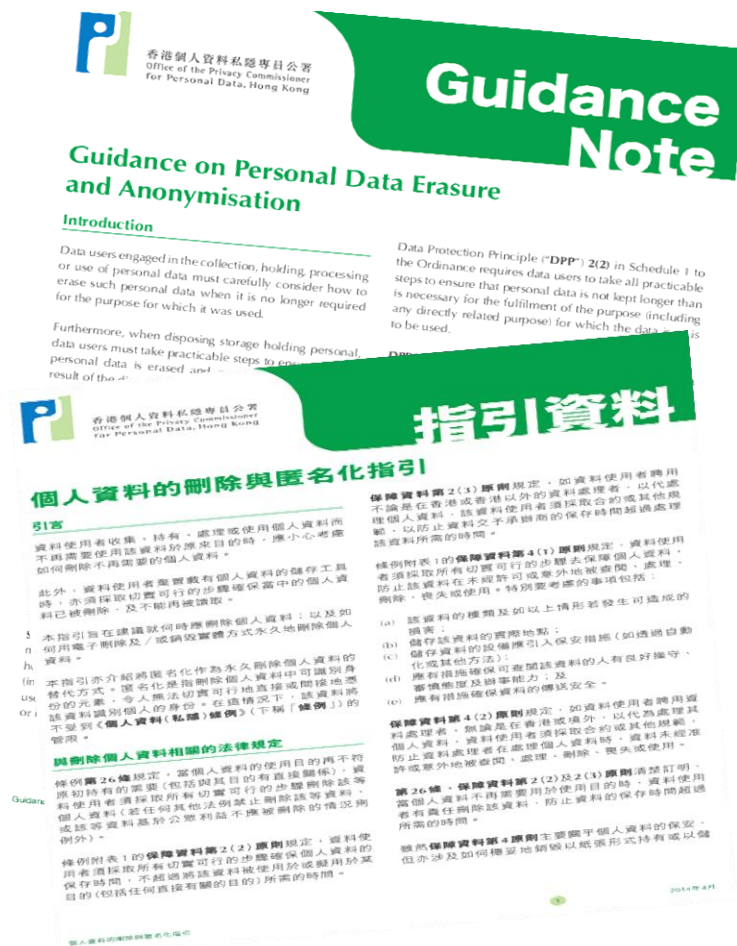
Case Sharing 5: An insurance company retained personal data of unsuccessful insurance applicants for indefinite period of time

- reasons given by insurer
 - ~ legal requirements for keeping books of accounts
 - ~ guidelines and circulars of regulatory authorities
 - ~ potential litigations, enquiries and complaints
 - ~ checking against future applications
- Privacy Commissioner's decision:
 - monetary transaction – retain 7 years
 - ~ non-monetary transaction – retain 2 years
 - ~ unless special circumstances existed
- insurer complied with the enforcement notice issued by the Commissioner, and erased more than 7,000 records



DPP 2 – Accuracy and duration of retention

- “Guidance Note on Personal Data Erasure and Anonymisation”



DPP 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

DPP 3 – Use of personal data

Case sharing 6: Use of Group Instant Messaging App

- MPF intermediary adding a customer to his WhatsApp group for circulating MPF related information
- thereby disclosing the customer's name and mobile number to members of the group
- no consent from customer
- contravention of DPP3

Exemption

- 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
- 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

Exemption (Con't)

- Moreover, the Data was also the personal data relating to the physical or mental health of the technician under section 59 of the Ordinance. 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

DPP 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

DPP 4 – Security of personal data

Case sharing 7: Failed to safeguard employee's personal data

- a chef complained that his employer had photocopied a menu on the back of a copy of his Identity Card and used the menu to record customers' orders
- photocopied two copies of the complainant's ID Card due to a copier malfunction
- the extra one was put into the tray of the copier
- formulated policy on the handling of employees' personal data

DPP 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.



DPP 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

DPP 6 – Access to personal data

Case sharing 8: Non-compliance with data access request

- the complainant under the arrangement of his company attended a doctor's clinic for a medical examination
- made a data access request to the doctor
- the doctor sought suggestions of complainant's company
- the company asked the doctor not to disclose the data on the ground of legal privilege
- entitled to rely on s20(3)(d) to refuse to comply with the DAR
- failed to inform the complainant about the refusal
- contravention of **s21(1)**

**PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM**

Important Notice to Requestor

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 67(1) 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)(e) 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 20(3)(a) 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 2 or 17A of the PDPO (please refer to Part III of this Form).
5. You are not entitled to access data which is not 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 him 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(1)(a) and 28(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.

Important Notice to Data User

1. 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.
2. If you are unable to comply with the data access request within the 40-day period, you must inform the requestor by notice **in writing** that you are so 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).
3. 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).
4. 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).
5. You may charge a fee for complying with a data access request, but section 28(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. 37/2009, 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.
6. 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

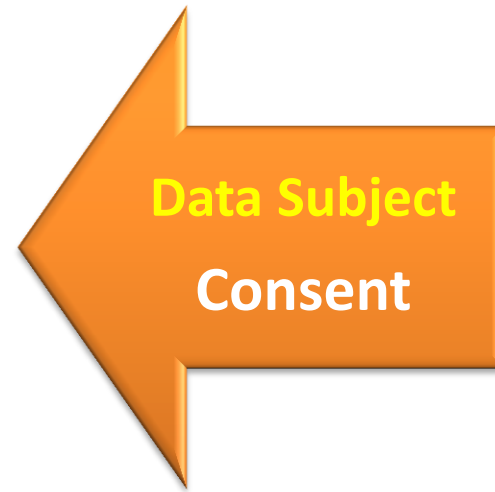
Direct Marketing Requirements



- The new provisions on regulation of direct marketing activities came into force on 1 April 2013
- Direct marketing activities under the Ordinance include such activities made to specific persons by mail, fax, email and phone
- If a data subject submits an opt-out request, the data user must comply with the request without charge
- Data user must notify a data subject of his opt-out right when using his personal data in direct marketing for the first time

Direct Marketing Requirements

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 understandable
- Should be given explicitly and voluntarily
- “consent” includes an indication of “no objection”

Direct Marketing Requirements

	Maximum Fine (HK\$)	Maximum Imprisonment
Non-Compliance	500,000	3 years
Non-Compliance if the personal data is provided to third party for its use in direct marketing in exchange for gain	1,000,000	5 years

Direct Marketing Conviction Cases

Date	Case	Penalty
Sep 2015 <i>(Note: Pending appeal trial)</i>	A telecommunication company ignored customer's opt-out requests	Fined \$30,000
Sep 2015	A storage service provider failed to take specified actions and obtain the data subject's consent before direct marketing	Fined \$10,000
Nov 2015	A healthcare services company ignored customer's opt-out requests	Fined \$10,000
Dec 2015 <i>(Note: Appeal trial in progress)</i>	An individual provided personal data to a third party for direct marketing without taking specified actions and obtaining the data subject's consent	Fined \$5,000

Direct Marketing Conviction Cases

Date	Case	Penalty
Apr 2016	<ul style="list-style-type: none"> an insurance agent used personal data for direct marketing without taking specified actions and obtain the data subject's consent; and failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time 	Community Service Order of 80 hours for each charge
May 2016	<ul style="list-style-type: none"> a telemarketing company used a customer's personal data in direct marketing without taking specified actions and obtaining his consent; and ignored opt-out requests 	Fined \$8,000 for each charge
Dec 2016	<ul style="list-style-type: none"> a watch company used personal data for direct marketing without taking specified actions and obtain the data subject's consent; and failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time 	Fined \$8,000 for each charge

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.
- Max penalty: a fine of \$1,000,000 and 5 years’ imprisonment

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

- Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry
- New Guidance on Direct Marketing
- 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



A Quick Guide



Hot Search



Advanced Search

Keywords

Publications

Multimedia

Industry-specific Resources

Resources by Topics

Frequently Asked Questions

Publications for Sale



Personal Data is Essential
Protect Your Privacy

Job Seeking

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



A Guide for Job Seekers

Cautious in providing personal data to prospective employers...

>>click here to view

What's New

Privacy Sweep Spots Concerns over Personal Websites and Apps Targeting Youngsters

The Collection and Use of Personal Data of Voters in Electioneering Activities Must Comply with the Privacy Ordinance

Mr Stephen Kai-yi WONG takes office today as the Privacy Commissioner for Personal Data, Hong Kong

Privacy Commissioner Provides Advice to Address Smartphone Users' Privacy Concerns

Privacy Commissioner Advises Cloud Users on Privacy Concerns

Government Urged to Tighten Control of Public Registers in Era of Big Data

For Individuals

Tips on Protecting Your Personal Privacy

Using Computers and the Internet Wisely

Have My Say on Personal Data Privacy

Cyber-bullying – What you need to know

Topic Guides

Legal Assistance

For Organisations

Data Protection Principles

Introduction to the PD(P)O Seminar

Professional Workshops

Case Notes

Industry-specific Resources

Topic Guides

Data Breach Notification

PCPD Newsletter

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



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

39th International Conference of Data Protection and Privacy Commissioners

中西薈萃 East Meets West



Stay tuned for updates on
www.privacyconference2017.org

Thank You!