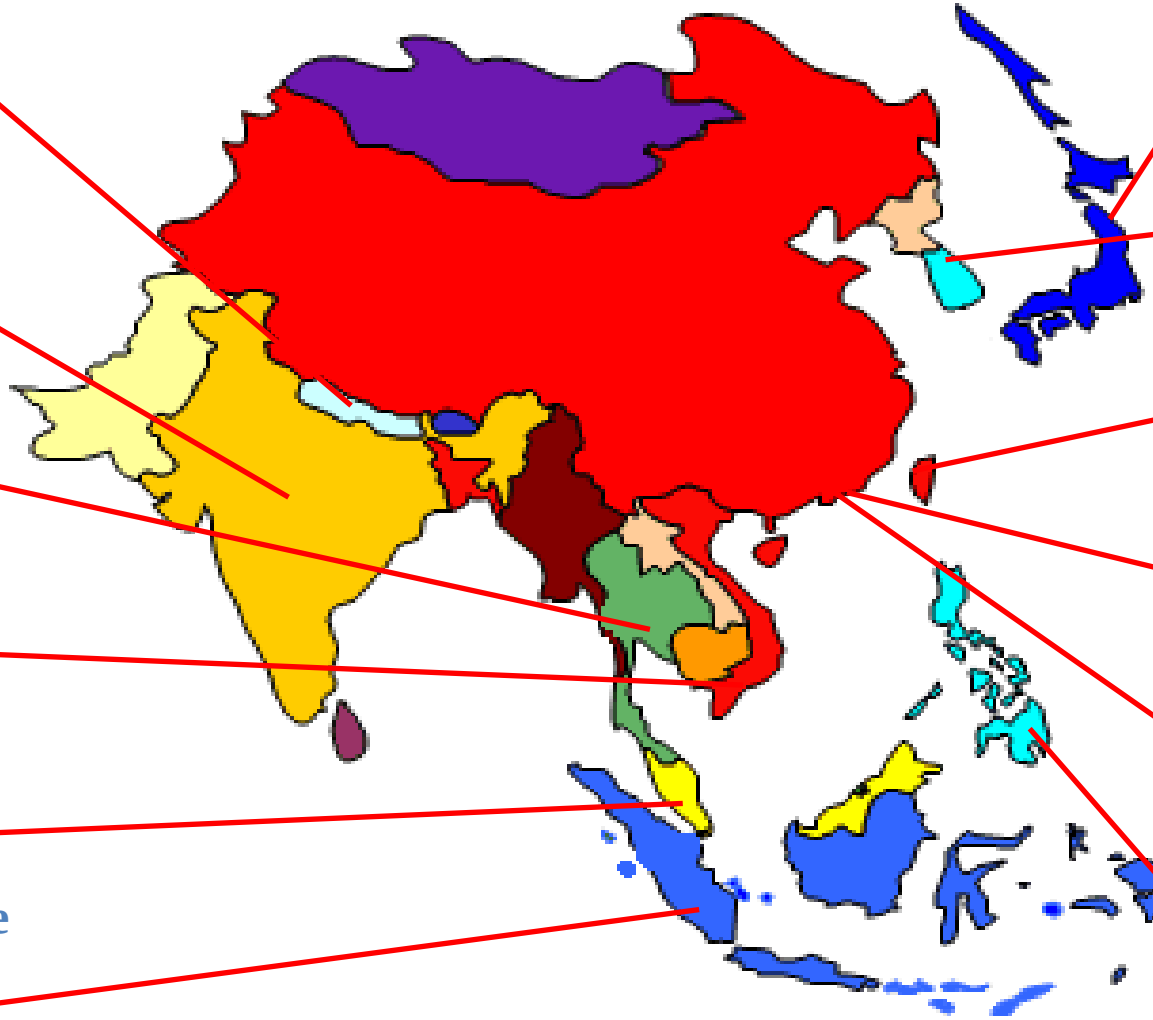
Hong Kong Society of Certified Insurance Practitioners
HKCIP Forum: New Opportunities and New Challenges
2 November 2016

Protect, Respect Personal Data in Insurance Industry

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data, Hong Kong

The Personal Data Landscape in Asia



2007 Nepal

2011 India

1997 Thailand

2010 Vietnam

2010 Malaysia

2012 Singapore

2003 Japan

2011 Korea

2010 Taiwan

1995 HKSAR

2005 Macao SAR

2012 Philippines

Personal Data (Privacy) Ordinance ("PDPO")

1. Introduction
   - Enacted in 1995
   - Core provisions came into effect on 20 December 1996
   - Personal Data (Privacy) (Amendment) Ordinance 2012 effective from 1 October 2012 except for "direct marketing" and "legal assistance" which took effect on 1 April 2013

What is personal data

"**personal data**" (個人資料) means *any **data*** -

*(a) **relating** directly or indirectly to a living individual;*

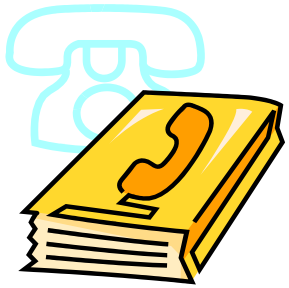
*(b) from which it is practicable for the **identity** of the individual to be directly or indirectly ascertained; and*

*(c) in a **form** in which access to or processing of the data is practicable;*

"**data**" (資料) means *any representation of information (including an expression of opinion) **in any document***

Examples of Personal Data used in everyday life

A person's name, telephone number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical record, etc



The Six Data Protection Principles (DPPs)

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。

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。

收集的資料是有實際需要的，而不超乎適度。

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 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 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致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.

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

The Six Data Protection Principles (DPPs)

www.youtube.com/watch?v=j6fO6JVGGHg

Personal Information Collection Statement (PICS)

- **Commissioner's Report No.R10-9866 (Octopus case)**
  - terms and conditions printed on the registration form in much smaller fonts than the other parts of the leaflet
    - ~ *"used by us for … (b) providing you with carefully selected offers, promotions and benefits* ***by us, our subsidiaries, our affiliates and/or Our Partners …"***
    - ~ *"may transfer or disclose such information to …* ***any other person under a duty of confidentiality to us …"***
  - In view of the small print and the failure to define with any reasonable degree of certainty the classes of transferees – **contravention of DPP1(3)**

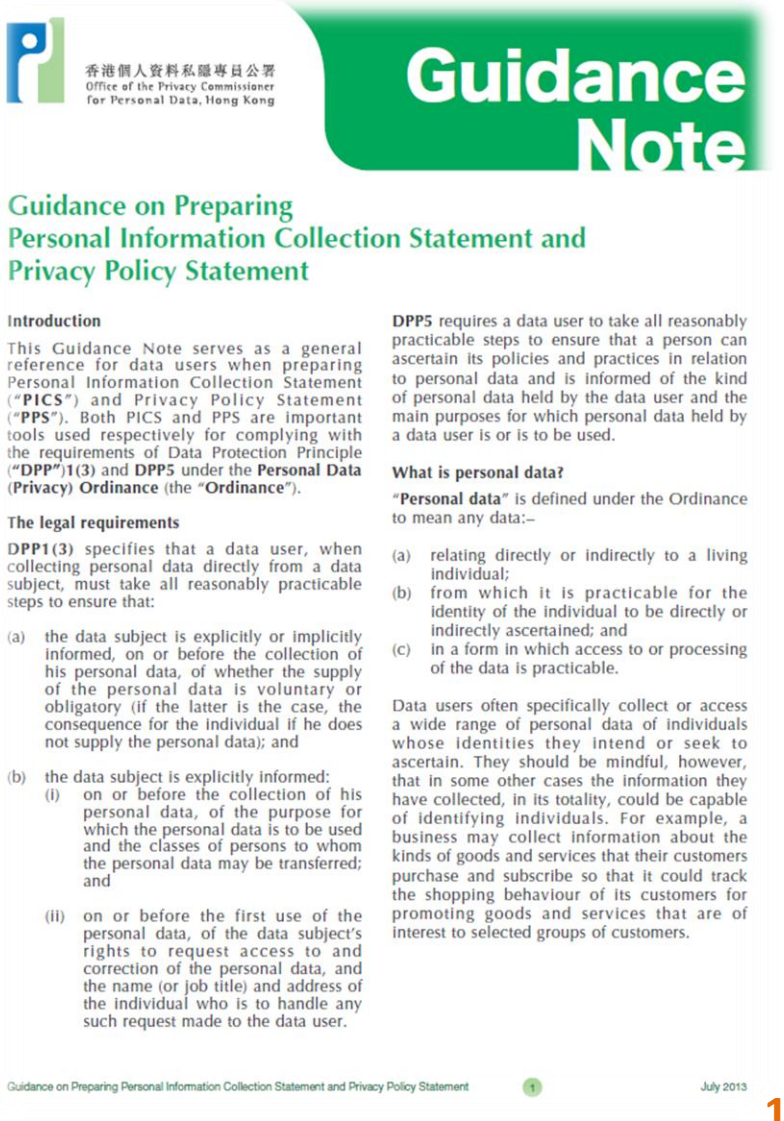
Personal Information Collection Statement

Practical Tips

- properly design the layout of PICS (including font size, spacing and use of appropriate highlights), easily readable
- present PICS in a conspicuous manner, e.g. in a stand-alone notice or section
- use languages which are reader friendly, e.g. use 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 such liberal and vague terms

GUIDANCE

This Guidance Note helps organisations prepare clear and information privacy notices (i.e. PICS and Privacy Policy Statement (PPS))



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

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**").

The legal requirements

DPP1(3) specifies that a data user, when collecting personal data directly from a data subject, must take all reasonably practicable steps to ensure that:

(a) the data subject is explicitly or implicitly informed, on or before the collection of his personal data, of whether the supply of the personal data is voluntary or obligatory (if the latter is the case, the consequence for the individual if he does not supply the personal data); and

(b) the data subject is explicitly informed:
  (i) on or before the collection of his personal data, of the purpose for which the personal data is to be used and the classes of persons to whom the personal data may be transferred; and
  (ii) on or before the first use of the personal data, of the data subject's rights to request access to and correction of the personal data, and the name (or job title) and address of the individual who is to handle any such request made to the data user.

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.

What is personal data?

"**Personal data**" is defined under the Ordinance to mean any data:–

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.

Data users often specifically collect or access a wide range of personal data of individuals whose identities they intend or seek to ascertain. They should be mindful, however, that in some other cases the information they have collected, in its totality, could be capable of identifying individuals. For example, a business may collect information about the kinds of goods and services that their customers purchase and subscribe so that it could track the shopping behaviour of its customers for promoting goods and services that are of interest to selected groups of customers.

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement 1 July 2013

Download: www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

Accuracy and Security of Customers' Data

- **Case Note No.1997C16**
  - husband (H), wife (W) and friend (F) take out travel insurance at the same insurance agency at the same time
  - H and W fail to fill in address in their application forms, staff simply enter F's address in the forms
  - staff later put the 3 policy documents in one envelope and mail to F
  - contravention of **DPP2(1)** and **DPP4**

Retention of customer's data

- **Case Note No.2004C21**
  - insurer retaining 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
    - ~ check against future applications

Retention of customer's data

- the Commissioner's views
  - ~ money transaction – 7 years
  - ~ no money transaction – 2 years
  - ~ unless special circumstances existed
- in compliance with enforcement notice issued by the Commissioner, insurer erased more than 7,000 records

Use of customers' data for internal training

- **AAB No.40/2009**

  - Regional Director of an insurer in a training session of 55 insurance agents held in Mainland China used insurance policy information of a former Regional Manager, her children and ex-husband to illustrate inappropriate practice of issuing policies to connected individuals
  - insurer argued that it was necessary to identify the parties concerned being someone the trainees knew so as to raise vigilance and deterrence

Use of customers' data for internal training

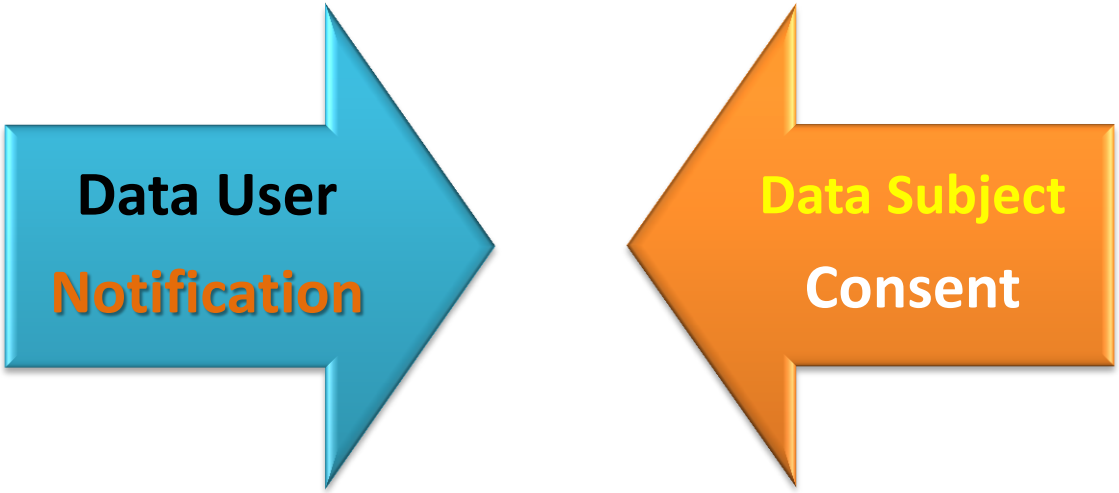
- the Commissioner's views
  - ~ not within a customer's reasonable expectation to use his data for training or share with agents unrelated to his policy
  - ~ not necessary to disclose identities to raise awareness
  - ~ mere mentioning of capacity or roles of the individuals involved would suffice
  - ~ contravention of DPP3 by insurer (vicarious liability through the Regional Director being its agent)

Direct Marketing

- **Part VIA – sections 35A to 35M**
- **"Direct marketing（直接促銷）" ("DM") means**
  - **offering or advertising of goods, facilities or services**
  - **solicitation of donations, etc**
  - **through "direct marketing means", i.e. *(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***

Direct Marketing

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"

Use of Personal Data in Direct Marketing

- Notwithstanding the source of the personal data, the following **specified actions** must be taken before using the personal data for **own** direct marketing activities (S.35C) ：-

  1) To **inform** the data subjects that it intends to so use the personal data and that the data may not be so used unless it receives the data subject's **consent**

  2) To inform the data subjects either orally (easily understandable) or in writing (easily readable and understandable) :

     - the **kinds of personal data** to be used;
     - the **classes of marketing subjects** in relation to which the data is to be used ；
     - the **response channel** through which the data subject may communicate his **consent** to the intended use.

Providing Personal Data to another person for Use in Direct Marketing

- The following specified actions must be taken before providing personal data to a third person for use in direct marketing (S.35J)

  1) To inform the data subject in writing that his/her personal data is intended to be provided for direct marketing and that the data may not be so provided unless it obtains written consent (oral consent is not acceptable)

  2) To provide the data subject with the following written information (easily readable and understandable)

     - where the data is to be provided for gain, that the data is to be so provided
     - the kinds of personal data to be provided
     - the classes of persons to which the data is to be provided
     - the classes of marketing subjects in relation to which the data is to be used

Offence

Failing to take the specified actions is an offence punishable by a fine up to HK$500,000 and imprisonment up to 3 years；if the data is to be provided for gain, the maximum penalty of a fine of HK$1,000,000 and 5 years' imprisonment

Other Offences

- A data user must notify data subject of his opt-out right when using his personal data for the first time (S.35F) (e.g. insert "opt-out" box in promotion materials)
- A data subject may at any time (irrespective of prior consent) require a data user to cease to use his/her personal data in direct marketing (S.35G)
- A data subject may at any time require a data user to cease to provide his/her personal data to any other person for use in direct marketing ; and to notify any person to whom the data has been so provided to cease to use his/her personal data (S.35L)
- A data user is required to notify such other person in writing to cease to use a data subject's personal data (S.35L)
- Must not impose any charge on the data subject who makes such request (S.35G and S.35L)

Other Offences

- **Contravention:**

  -a fine up to HK$500,000 and imprisonment for up to 3 years;

  -if the data is to be provided for gain, the maximum penalty of a fine of HK$1,000,000 and 5 years' imprisonment

Direct Marketing Conviction Cases

2015

Date of Conviction	Case	Penalty
9 Sep	A telecommunication company ignored opt-out requests	Fined $30,000
14 Sep	A company providing moving & storage services charged with the offence of using the personal data of a customer in direct marketing without taking specified actions and obtaining consent	Fined $10,000
3 Nov	A company providing healthcare services ignored opt-out requests	Fined $10,000
30 Dec	An individual provided personal data to a third party for DM without taking specified actions and obtaining his consent	Fined $5,000

Direct Marketing Conviction Cases

2016

Conviction Date	Case	Penalty
25 Apr	An insurance agent was charged with the offence of using the personal data of a customer in direct marketing without taking specified actions, obtaining consent and failing to inform the data subject, when using his personal data in direct marketing for the first time	A Community Service Order of 80 hours for each charge
16 May	A telemarketing company charged with the offence of using the personal data of a customer in direct marketing without taking specified actions, obtaining consent and ignoring opt-out requests	Fined $8,000 for each charge

Conviction DM cases in relation to insurance industry

Case 1:

Case background

- A real estate agent ("1st Defendant") obtained the complainant's Christian name and mobile phone number ("the Data") in a social function
- the 1st Defendant did not inform the complainant or seek his consent for providing the Data to another party for direct marketing
- About two months later, an insurance agent ("2nd Defendant") called the complainant twice on his mobile phone
- During the first phone call, the 2nd Defendant identified herself as a financial planner of an insurance company, claiming that the 1st Defendant provided the Data to her

Conviction DM cases in relation to insurance industry

- Case background (con't)
  - 2nd Defendant called the complainant again. Once the complainant realised that the 2nd Defendant intended to provide him with information about financial planning and insurance products, he immediately indicated that he had no interest in such products and hung up the phone

- Charge
  - 1st defendant: failing to take specified actions and obtain consent before providing personal data to a third party for use in direct marketing (S. 35J)

Conviction DM cases in relation to insurance industry

- Charge (con't)
  - 2nd defendant: failing to take specified actions and obtain consent before using the personal data of a data subject in direct marketing (S.35C)

- Outcome
  - 1st defendant was fined HK$5,000 (first conviction of new offence under S.35J)
  - 2nd defendant was acquitted on the facts of the case, mainly because the Court could not rule out the possibility of her attempting to take those specified actions but was interrupted as the data subject hung up the phone after she mentioned about insurance matters

Conviction DM cases in relation to insurance industry

Case 2:

Case background

- The complainant had purchased an insurance policy at an insurance company ("Insurance Company A")
- Subsequently, the complainant received at his home address a letter from the Defendant who was working as an insurance agent of another insurance company
- the Defendant promoted financial services to the complainant after knowing the suspension of service of Insurance Company A in the letter

Conviction DM cases in relation to insurance industry

- **Charge**
  1. Failing to take specified actions and obtain consent before using the personal data of a data subject in direct marketing (S.35C)
  2. Failing to inform the data subject when using his personal data in direct marketing for the first time, of his right to request not to use his personal data in direct marketing without charge (S.35F)

- **Outcome**

  A Community Service Order of 80 hours was imposed by the Court on the defendant in respect of each charge, to be served concurrently

Practical Tips

Must take specified actions and obtain consent

Must notify data subject of his opt-out right

Update the Opt-Out List regularly

Ensure that organisations' standing procedures for their staff to follow are followed

Guidance to help data users

- Guidance on Direct Marketing issued by the PCPD to assist data users to understand their obligations and promote good practice

- A leaflet on Exercising Your Right of Consent to and Opt-out from Direct Marketing Activities was also issued by PCPD to assist data subjects to understand their rights

Guidance Note

Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

Exercising Your Right of Consent to and Opt-out from Direct Marketing Activities under the Personal Data (Privacy) Ordinance

Q1 What is "direct marketing"?

Privacy as a Competitive Advantage

privacy and personal data protection can be an asset and a business edge