How Insurance Practitioners Can Protect Their Customers' Personal Data

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

HKFI
The Hong Kong Federation of Insurers
香港保險業聯會

In Hong Kong, the privacy of individuals in relation to their personal data is protected by the Personal Data (Privacy) Ordinance ("the Ordinance").

Insurance practitioners handle a large amount of customers' personal data in their daily work: e.g. name, telephone number, address, identity card number, information contained in insurance application forms and insurance policies, etc. With regard to the collection, holding, accuracy, retention period, security, access and correction of personal data, they should ensure that their practices comply with the requirements under the Ordinance.

Respecting your customers' privacy you will earn their trust, which helps build a good reputation and goodwill, broaden your client base and boost your business in the long run.

What are Personal Data?

Personal data are any data relating to a living individual, from which his/her identity can be directly or indirectly ascertained, including an expression of opinion about the individual, which is recorded in a form that can be processed or accessed.

The Six Data Protection Principles ("DPPs"), along with the requirements in relation to **the use of personal data in direct marketing** under the Ordinance, are of direct relevance to the work of insurance practitioners.

The Six Data Protection Principles

Principle 1–

Purpose and manner of collection of personal data

The collection of personal data must be related to a specific function or activity of the data user, and must be necessary for the purpose of the collection; the data collected must not be excessive; the means of collection must be lawful and fair; the data subjects must be informed of the purpose of collection and the classes of persons to whom the data may be transferred.

Example:

When you collect your customers' personal data, you should provide them with a Personal Information Collection Statement (PICS) stating clearly the purpose of collecting the data, the classes of persons to whom the data may be transferred, the consequences of failing to supply the data, and the right of access to the data. The PICS should be attached to documents such as insurance application forms.

Principle 2–

Accuracy and duration of the retention of personal data

All practicable steps must be taken to ensure the accuracy of the personal data, and the data must be erased after the fulfillment of the purposes for which it is used.

Example:

- *If letters sent to a customer are always returned, it could be because of an inaccurate mailing address. You should stop using that mailing address and update it.*
- *Company policy should be formulated to specify the period of retention of customers' personal data.*

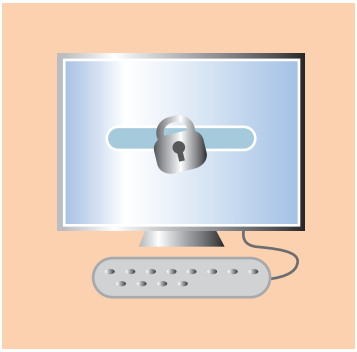
Principle 3–

Use of personal data

Unless the data subject gives "prescribed consent", personal data should not be used for any purpose other than that for which it was collected or a directly related purpose. "Prescribed consent" means express consent given voluntarily by the data subject and which has not been withdrawn in writing.

Example:

Under general circumstances, insurance practitioners are not allowed to disclose their customers' personal data to other companies for promotion of their products, unless prior prescribed consent has been obtained from the customer.



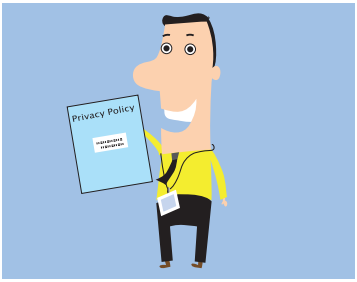
Principle 4–

Security of personal data

All practicable steps must be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure.

Example:

When using window envelopes to mail documents containing customers' personal data, you must ensure that your customers' sensitive data (e.g. identity card number) does not show through the envelope window. If the letter is intended for the recipient only, you should consider marking "Private and Confidential" on the envelope and seal it.



Principle 5–

Information to be generally available

Data users' policies and practices in relation to personal data must be made available to the public.

Example:

Formulate and maintain a Privacy Policy Statement, stating the kinds of personal data held, purpose for using the personal data and its personal data policies and practices, which can be displayed on your company's website.

Principle 6–

Access to personal data

Data subjects have the right of access to, and correction of, their personal data, and data users must comply with a data access request not later than 40 days after receiving the request.

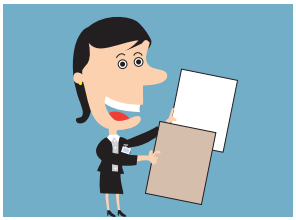
Example:

A customer has the right to ask an insurance company to supply a copy of the personal data contained in his insurance policy.

Section 34 of the Ordinance – Direct Marketing

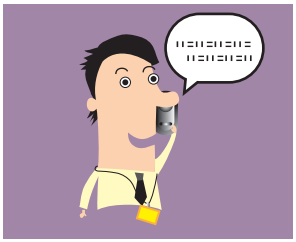
When an insurance company uses a customer's personal data for the first time for the purpose of direct marketing, it must inform the customer that he/she can make an "opt-out" choice, i.e. ask the company to cease to use his/her personal data for the purpose of direct marketing.

Steps for making marketing calls by practitioners:



Before the call

Check the opt-out list to ensure that the telephone number is not on the list.



During the call

- Give the name of both the company and the practitioner.
- Inform the receiver of the opt-out choice by saying, "If you do not wish to have further marketing calls from us, please tell me and we will not call again."

After the call

If the receiver does not wish to receive further marketing calls, you should note down the request and update the opt-out list accordingly. The insurance company is not allowed to charge the receiver for such an arrangement.

Notes:

-Insuracnce companies should maintain a list of all individuals who have said that they do not wish to receive further marketing calls.

-The list should be uplated in a regular and timely manner (once a week is recommended) to ensure compliance with the opt-out requests.

Practical Tips

(I) Collection and Use of Customers' Personal Data for Direct Marketing

(1) Can an insurance company ("Company A") market its products in the name of another company ("Company B")?

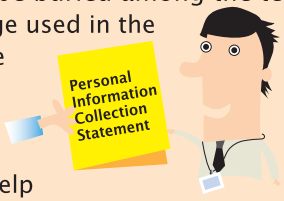
A: If, under such circumstances, a customer was led to believe that it was Company B which was promoting its product/service through direct marketing, and based on such reliance, the customer purchased the relevant product/service and provided his/her personal data, Company A might have contravened Data Protection Principle 1(2) of the Ordinance, which requires that personal data be collected by means which are lawful and fair.

(2) Would it be appropriate for a data user to combine both (i) terms and conditions of service, and (ii) a statement that the personal data would be used for marketing products or services that are not directly related to the service that was originally sought in the service application form, and provide its customers with only one column to sign on the form?

A: If the data user did so, the customer would have to choose between (i) giving up the application for the service and (ii) giving his "bundled consent", thus agreeing to the terms and conditions of the service originally sought, as well as the use of his data as prescribed by the data user, which he may find objectionable. In such circumstances, the data user is advised to design its service application form in a way that separates the customer's agreement to the terms and conditions of service from the consent to the use of his personal data for marketing any products of services not relating directly to the service(s) he seeks. One way to achieve this goal is to ask the customer to "tick" a box or to sign sepatately, indicating whether he/she agrees to the prescribed use of his personal data.

(3) What areas need special attention when designing a Personal information Collection Statement ("PICS")?

A: Firstly, the layout and presentation of the PICS should be easily readable for customers with normal eyesight. Secondly, the PICS should be a standalone section; its contents should not be buried among the terms and conditions of service. Thirdly, the language used in the PICS should be easily understandable; the use of legal terms or convoluted phrases should be avoided. Fourthly, further assistance from the insurance company, such as a help desk or enquiry service, may be provided to help its customers understand the contents of the PICS. Data users should strive to enhance the effectiveness of communicating the PICS to customers by taking into account the actual circumstances in which personal data are collected such as the characteristics of the targeted customers (in terms of age, educational level, etc).



(4) Can an insurance company use personal data obtained from records in the public domain (e.g. public registers) for direct marketing?

A: If there is a specific prohibition in the public register against the use of such personal data for direct marketing, then the insurance company should not use personal data in the public register for direct marketing; otherwise, it may not only contravene DPP3, but also breach the provisions of the relevant ordinances related to the public register. Where the public register does not specify the purpose for which the personal data may be used, the insurance company, when deciding whether to use the personal data for direct marketing purposes, needs to consider the background leading to the creation of the public register, and the reasonable expectation of the data subjects.

(5) Can an insurance company transfer customers' personal data to third parties for monetary gain?

A: The sale of personal data by a data user is normally not regarded as the original purpose for data collection or a directly related purpose. In the circumstances, explicit and voluntary consent from the customer has to be sought for the sale of the data; otherwise, the data user runs the risk of contravening DPP3. The consent may be indicated by a signature to that effect or by ticking a box.

The PCPD published the "Guidance on the Collection and Use of Personal Data in Direct Marketing" in October 2010 to provide data users with practical guidance on the collection and use of personal data in direct marketing.

(II) Duration of Retention of Customers' Personal Data

How long can customers' personal data be kept by an insurance company?

A: 1. As the cases of collection and use of personal data differ in every organization, no fixed duration of retention is specified in the Ordinance.

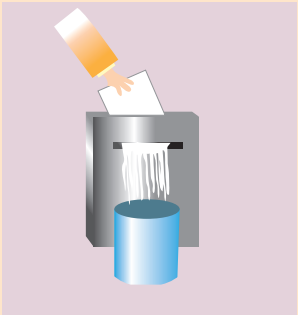
2. Insurance companies should determine the duration of retention of personal data by considering when the purpose for collection of the personal data has been fulfilled.

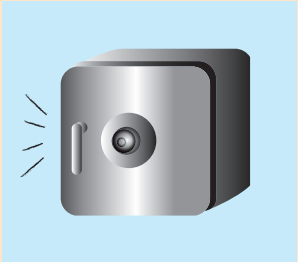
3. If the personal data are no longer required for the original purpose, the data should be erased.

4. The Privacy Commissioner carried out an investigation of one insurance company and found that the company had retained the personal data of unsuccessful insurance applicants for an indefinite period of time. The Privacy Commissioner takes the view that for unsuccessful insurance applications where a monetary transaction is involved (e.g. where the premium is paid together with the application), the optimal period of retention of the personal data concerned should generally not exceed 7 years. For cases where no monetary transaction is involved, the Privacy Commissioner finds that an optimal retention period of two years is generally sufficient for fulfilling the various purposes required by insurance companies. *(For details of this case, please refer to the section "Case Notes" on the PCPD website.)*

(III) Security of Personal Data

What security measures should insurance practitioners take to safeguard their customers' personal data?





A: 1. If practitioners need to take documents containing their customers' personal data away from office, they should handle them with great care to prevent them from being lost or to prevent unauthorized access by third parties

2. If a mobile electronic storage device (e.g. laptop computer, USB flash drive) is used, practitioners must ensure that only necessary data are stored, that the data are encrypted and that they are deleted after use.

3. Practitioners must ensure that no file-sharing software (e.g. Foxy) is installed on their computers. Personal data stored on their computers should be thoroughly erased if it will no longer be used.

4. Practitioners must not dispose of documents containing personal data recklessly. Paper shredders should be used to destroy such documents.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wan Chai, Hong Kong

Website: www.pcpd.org.hk
E-mail: enquiry@pcpd.org.hk

The Hong Kong Federation of Insurers

Enquiry Hotline: (852) 2520 1868
Fax: (852) 2520 1967
Address: 29/F, Sunshine Plaza, 353 Lockhart Road, Wan Chai, Hong Kong

Website: www.hkfi.org.hk
E-mail: hkfi@hkfi.org.hk