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 the Proper Handling of Customers' Personal Data for the Insurance Industry

Contents

1. INTRODUCTION

In the course of providing insurance services to the public, insurance institutions and insurance practitioners handle a lot of customers' personal data. It is essential that they understand and comply with the requirements under the Personal Data (Privacy) Ordinance ("**the Ordinance**") which apply to them in their capacities as data users in the handling of personal data.

This guidance note aims to assist the insurance industry when undertaking insurance activities to comply with the relevant requirements under the Ordinance in handling the collection, storage, use, security of and data access requests for customers' personal data.

2. AN OVERVIEW OF THE RELEVANT REQUIREMENTS UNDER THE ORDINANCE

2.1 What is Personal Data?

Personal data is any recorded information (including an expression of opinion) relating to a living individual from which his identity can be directly or indirectly ascertained. Common examples of customers' personal data are their names, addresses, telephone numbers, identity card numbers, dates of birth, occupations, medical records, financial information, policy information, claims information, etc.

2.2 The Six Data Protection Principles

The six data protection principles ("**DPPs**") provided in Schedule 1 to the Ordinance set out the basic requirements with which data users must comply in the handling of personal data. They regulate the collection, holding, processing and use of personal data as follows:

2.2.1 Principle 1 – Purpose and Manner of Collection of Personal Data

The purpose of collection of personal data must relate to a function or activity of the data user; collection of the data is necessary for or directly related to that purpose; and the data collected is adequate but not excessive (DPP1(1)). The means of collection must be lawful and fair (DPP1(2)). On or before collecting personal data directly

from the data subject, the data user must inform the data subject: (a) whether it is obligatory or voluntary for him to supply the data and if obligatory, the consequences of failing to supply the data; (b) the purpose of collection of the data; (c) the classes of persons to whom the data may be transferred; and (d) the rights of the data subject to request access to and the correction of the data, and the name or job title, and address of the individual who is to handle data access and correction requests (DPP1(3)).

Practical application:
*When collecting customers' personal data, insurance institutions should carefully consider the necessity of collecting each item of information to be collected. If customers are required to supply their personal data, they should be provided with a Personal Information Collection Statement ("**PICS**") stating clearly the purposes 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 and correction of the data. The PICS may be attached to documents which collect personal data such as an insurance application form or a claim form.*

2.2.2 Principle 2 – Accuracy and Duration of Retention of Personal Data

Data users must take all practicable steps to ensure the accuracy of personal data held by them (DPP2(1)), and to erase the data after fulfillment of the purposes for which the data is used (DPP2(2)). Data users must adopt contractual or other means to prevent any personal data transferred to a data processor[1] (e.g. an agent engaged by an insurance institution to send out direct marketing materials on its behalf,) from being kept longer than is necessary (DPP2(3)).

In addition, section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data no longer required for the purpose for which the data was used unless prohibited under any law or public interest requires otherwise.

Practical application:
(1) Before sending documents containing personal data to a customer, it is important to ensure that the address of the customer is accurate and up-to-date, otherwise the data is put to the risk of accidental disclosure to unrelated third parties.

[1] A data processor, means a person who processes personal data on behalf of another person and does not process the data for any of the person's own purposes.

(2) Insurance institutions should formulate their policies and practices to specify the period of retention of customers' personal data.

2.2.3 Principle 3 – Use of Personal Data

Unless prior "prescribed consent" has been obtained from the data subject, personal data shall not be used for a new purpose. A new purpose is any purpose other than the purpose for which the data was to be used at the time of the collection of the data, or a directly related purpose. In this context, "**use**" includes the disclosure or transfer of personal data. Under section 2(3) of the Ordinance, "**prescribed consent**" means the express consent of the data subject given voluntarily. Such consent may be withdrawn by the data subject in writing.

Practical application:
In normal circumstances, an insurance agent or representative should not disclose customers' personal data to other companies for marketing their products. Nor should he use customers' data for purposes unrelated to the handling of the customers' accounts with the insurance institution. Prescribed consent must be obtained from the relevant customer before any change of use of his data. In this regard, insurance institutions should give proper guidance and training to their staff, representatives and agents, and enforce the rules with appropriate sanctions.

2.2.4 Principle 4 – Security of Personal Data

Data users must take all practicable steps to ensure that personal data held by them is protected against unauthorized or accidental access, processing, erasure or other use (DPP4(1)). Where a data user engages a data processor (e.g. an insurance institution engages an agent to destroy obsolete customer records), the data users 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 (DPP4(2)).

Practical application:
Documents containing personal data such as insurance application form or policy should be securely kept against access by unauthorized parties. Personal data stored electronically in computers or portable storage devices should be protected with adequate IT security measures and access control.

2.2.5 Principle 5 – Information to be Generally Available

Data users must take all practicable steps to ensure openness and transparency about their policies and practices in relation to personal data, the kind of personal data they hold and the main purposes for which the data is used.

Practical application:
*Insurance institutions should formulate and make available to customers their Privacy Policy Statements ("**PPS**") stating in detail the kind of personal data held, the main purposes of use of each type of personal data and their privacy policies and practices in place. The PPS may be displayed on the company's website and prominently at their reception counters.*

2.2.6 Principle 6 – Access to Personal Data

Data subjects have the rights of access to and correction of their personal data held by data users. Data users are required to comply with such request within 40 days after receiving the request. Detailed provisions on data access and data correction requests are contained in sections 18 to 25 and 27 to 29 of the Ordinance.

Practical application:
A customer may make a request to an insurance institution to be informed whether it holds his personal data contained in, for example, an insurance application form, medical report, risk assessment questionnaire or claim form, and be supplied with a copy of such data within 40 days.

2.3 Section 34 of the Ordinance – Direct Marketing

When a data user uses personal data for direct marketing purposes for the first time, it must inform the data subject of his right to opt out of such use by the data user. If the data subject opts out, the data user must cease to so use the data.

Practical application:
When making cold calls to customers or potential customers, insurance institutions and insurance practitioners must ensure that the use of customers' personal data for such purpose is the same as or directly related to the original collection purposes of the data. They must also check that the names of customers from previous cold calling activities who have opted out are not retained in their call lists.

During marketing calls, customers must be informed of their opt-out rights. The names and telephone numbers of those customers who exercise their opt-out rights, their names and telephone numbers should be placed on an opt-out list for counter-checking in future cold calling activities.

Attention should also be paid to the amendments to the relevant provisions of the Personal Data (Privacy) Ordinance (due to take effect in early 2013). Under Part VIA of the Ordinance, after the relevant amendments become effective, insurance institutions and insurance practitioners before making direct marketing approaches must inform customers or potential customers, either orally or in writing, that their personal data will be used for direct marketing and the kind of insurance products that they are going to market. Insurance institutions and insurance practitioners must not use the personal data of customers or potential customers to make direct marketing approaches, or provide such personal data to their agents for use in direct marketing without the customers' consent (which includes an indication of no objection). Non-compliance with the said requirements is an offence (for details please refer to Part VIA of the Ordinance). Insurance institutions and insurance practitioners are advised to refer to guidance on carrying out direct marketing activities issued by the Privacy Commissioner from time to time.

2.4 Liabilities of Insurance Institutions and Insurance Practitioners

Under section 65(1) and (2) of the Ordinance, any act done or practice engaged in by an employee or agent shall be treated as done or engaged in by him as well as by his employer or principal. Accordingly, an insurance institution is accountable for the acts done or practices engaged in by its staff, insurance agents and representatives in the course of providing insurance services on its behalf. An insurance institution is also answerable for the acts or practices of its contractors or other agents, e.g. IT contractors, marketing agents or loss adjusters, done or engaged in within the scope of authorities given to them.

In addition, insurance practitioners are liable for their acts or practices in the handling of customers' personal data in their own capacity as data users, unless they do not hold, process or use such data for any of their own purposes.

3. SOME PRACTICAL TIPS

The following notes aim to assist insurance practitioners to better understand the application of the Ordinance to specific situations which they may encounter. They promote the adoption of good practices in the handling of personal data and compliance with the provisions of the Ordinance by insurance institutions and insurance practitioners.

3.1 Personal Information Collection Statement (PICS)

Insurance institutions are advised to formulate and provide customers with PICS containing the information prescribed in DPP1(3).

3.1.1 Contents of a Collection Statement

A PICS should contain the following information:

(1) ***Purpose Statement:*** This is a statement of the purposes of use to which the personal data will be put after collection. Though the statement may be made in general or specific terms, the purposes must be explicitly stated; customers should be able to ascertain with reasonable certainty how their personal data may be used.

Example:
"The information collected from you will be used for the purposes of processing your insurance application, arranging a contract of insurance with you and managing your account with us."

(2) ***Transferee Statement:*** This shall explicitly state the classes of third parties to whom the personal data may be transferred. The categories of transferees should be defined with a reasonable degree of certainty.

Example:
"The data that you have supplied in this insurance application may be transferred to:
(1) providers of risk intelligence for the purpose of customer due diligence or anti-money laundering screening;
(2) reinsurers for the purpose of underwriting your application or administering your policy;

(3) loss adjusters for the purpose of processing any claims on your policy."

(3) ***Optional or Obligatory Provision of Data:*** Unless it is obvious from the circumstances, insurance institutions should explicitly inform customers whether it is obligatory or voluntary to supply personal data, and if obligatory, the consequences of failure to supply data. Even if voluntary, it is advisable to also state the consequences of failure to supply.

Examples:

(1) "It is voluntary for you to provide the information in this insurance application form. However, if you fail to do so, we may not be able to assess your application due to lack of information."

(2) "The completion of all items in Part A of this claim form is compulsory for the processing of your insurance claim. If you fail to provide the information, your claim will not be accepted."

(4) ***Data Access and Correction Rights:*** Insurance institutions must explicitly provide information on the customers' rights of access to, and correction of, their personal data and the name or job title, and address of the person to whom any such request may be directed.

Example:

"You have a right under the Personal Data (Privacy) Ordinance to make a data access or correction request concerning your personal data held by us. You may make such request by writing to our Privacy Compliance Officer at the following address: …"

3.1.2 What Practicable Steps to Take to Inform Customers

DPP1(3) requires insurers to take all practicable steps to provide the above prescribed information to customers. The information may be given verbally or in writing, but it is advisable to provide a written PICS where practicable. This may be done by attaching the PICS to the form for collecting the personal data or giving the customer a notice of the PICS before collection of the data from him. Where personal data is collected from the customer over the phone, the PICS must be given before collecting the data. This may be provided verbally, e.g. in a recorded message, and as a matter of good practice, followed up by sending a written version of the PICS.

Insurance institutions may collect personal data from customers in different situations for different purposes, e.g. when processing an insurance application or an insurance claim. Insurance institutions should therefore ensure that the PICS used for each situation fits the particular circumstances in which personal data is collected.

To ensure that a PICS is effectively communicated to customers, insurance institutions are advised to:

(1) pay attention to the layout of the PICS (including the font size, spacing and use of appropriate highlights) to ensure readability to customers of normal eyesight;
(2) present the PICS in a conspicuous manner, e.g. in a stand-alone notice or section of the form, and its contents should not be buried among other terms and conditions;
(3) use reader-friendly language, e.g. use simple words and avoid jargon or convoluted expressions;
(4) provide help desk or enquiry service to customers to assist understanding.

In the event of repeated collections of personal data from a customer for the same purposes, in accordance with section 35 of the Ordinance it is not necessary to repeatedly provide him with the same PICS if it has already been given to him in an earlier collection in the immediate past 12 months.

3.1.3 Case Study - small print and vague classes of transferees

The Complaint

A service provider was accused of selling customers' personal data to an insurer for direct marketing purposes. The service provider's notice relating to the collection and use of customers' personal data stated that it may transfer or disclose the personal data to *"any other person under a duty of confidentiality to [it]"*. The notice was printed in a much smaller font than other terms and conditions.

Outcome

In view of the small print used in the service provider's notice and the failure to define with reasonable certainty the classes of transferees of personal data, the service provider was found to have contravened DPP1(3).

In consequence of an investigation of the complaint, the service provider undertook to remedy the contravention. Its revised notice was easily readable to individuals of normal eyesight, and to specify the classes of transferees of the personal data with a reasonable degree of certainty as to whom the personal data may be transferred.

3.2 Collection of Customers' Medical Data

Insurers often collect customers' medical data on an application for insurance policy or in processing an insurance claim. The data may be collected from customers directly or from third parties.

3.2.1 No Collection of Excessive Data

Before collecting the medical data, insurers should first consider, in respect of each item of the data to be collected, whether it is indeed necessary to collect the data. Collection of excessive data is contrary to DPP1(1). For example, in an insurance claim for medical expenses incurred in relation to an operation to remove the claimant's tonsils, it may not be necessary to collect medical data about a surgery on his knee ten years ago, unless the insurer can show the relevancy of the data to the claim.

3.2.2 Lawful and Fair Means of Collection

In addition, as required by DPP1(2), the means of collection must be fair and not prohibited under any law. Fairness is a broad principle and will be assessed based on the particular circumstances of a case. In general, obtaining information by deception or misrepresentation would not be considered fair means of collection of data.

3.3 Collection of Hong Kong Identity Card Number and Copy

The collection of Hong Kong Identity Card ("**HKIC**") number (and other personal identifiers such as a passport number) and HKIC copy is regulated by DPP1 and the ***Code of Practice on the Identity Card Number and other Personal Identifiers*** ("**PI Code**") issued by the Privacy Commissioner for Personal Data ("**Privacy Commissioner**").

3.3.1 Identity Card Number

A data user must not collect HKIC number (or other personal identifier) of an individual unless authorized by law or permitted in the situations set out in paragraph 2.3 of the PI Code. The situations which are of practical relevance to insurance transactions are those provided in paragraph 2.3.3 of the PI Code. It provides that a

data user may collect HKIC number (or other personal identifier) to enable the correct identification of the individual for the advancement of the interest of the individual, or for the prevention of detriment to any person other than the data user, or to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances. For example, an insurer may require the HKIC number of a customer or beneficiary to ensure that a payout from an insurance claim is made to the right person.

3.3.2 Identity Card Copy

Insurance institutions must comply with paragraph 3.2 of the PI Code in collecting HKIC copy. Generally speaking, they may not collect HKIC copy except where the collection is authorized by law or for the purpose of providing proof of compliance with any statutory requirement. For example, an insurance institution may collect a copy of the identity card of an individual, who is the customer of a life insurance policy, as proof of compliance with section 3 of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("**AMLO**"), which requires an insurance institution to verify the customer's identity when conducting customer due diligence before establishing a business relationship with the individual or as soon as reasonably practicable thereafter.

3.4 Engagement of Private Investigators in Insurance Claims

3.4.1 Liability for the Acts of Private Investigators

Insurers may employ the services of private investigators to investigate suspicious claims. In the course of carrying out such investigations, private investigators may use various types of surveillance or search to gather as much information as possible about individuals. Private investigators must comply with the requirements of DPP1 in the collection of personal data, namely, the means of collection must be lawful and fair, and the data collected must not be excessive. An insurer may be held liable for the acts of the private investigator appointed by it pursuant to section 65(2) of the Ordinance.

3.4.2 Lawful and Fair Means of Collection

Private investigators must not use means which are contrary to the laws of Hong

Kong to collect personal data. For example, hacking into computers to obtain information about the claimant or theft of documents containing personal data may constitute unlawful means of collection of personal data, or even criminal offences.

The means of collection must also be fair. Whether the means is fair or not will depend on all the circumstances of the case. Generally speaking, obtaining information covertly would not be considered fair means of collection of data. However, each case turns on its own facts and there may be special circumstances which justify particular means of collection. For example, the collection of information about a claimant's activities by physical surveillance may be justified if there is reasonable suspicion of a fraudulent insurance claim of personal injury and there are no realistic alternatives to obtaining evidence of the fraud other than by way of such means of collection. In the event of a complaint made to the Privacy Commissioner, the insurer would be asked to explain and show that the special features of the case justify using the means of collection in question.

3.4.3 Data is Adequate but Not Excessive

Insurers should ensure that the data collected by private investigators on their behalf is adequate but not excessive. For example, in the course of investigating a suspected false claim of personal injury, data in relation to the claimant's private life which is unrelated to the claim should not be collected.

3.4.4 Control of the Private Investigators

Insurers are advised that when they engage private investigators to investigate suspicious claims, they should take measures to prevent the investigators from contravening the requirements under the Ordinance in the course of investigation. Reliance on simple agreement from the private investigator to abide by the laws of Hong Kong including the Ordinance will not suffice. Insurers should put in place practical guidelines in respect of the collection and handling of personal data by the private investigators. They should ensure that the personal data collected on their behalf is by lawful and fair means, and that the data collected is not excessive.

3.5 Collection and Use of Personal Data in Direct Marketing

Insurance institutions and insurance practitioners are advised to refer to the ***Guidance Note on the Collection and Use of Personal Data in Direct Marketing*** issued by the

Privacy Commissioner ("**DM Guidance Note**"), and the ***Code of Practice on Person-To-Person Marketing Calls*** issued by the Hong Kong Federation of Insurers for detailed guidelines on direct marketing activities. Furthermore, insurance institutions and insurance practitioners should be aware of the new requirements under Part VIA of the Ordinance in relation to collection and use of personal data in direct marketing. The current DM Guidance Note will be revised to take into account the new provisions before they come into effect. The following examples and case studies highlight some of the areas which they should pay attention to.

3.5.1 Lawful and Fair Means of Collection

Insurance institutions and insurance practitioners may collect the personal data of potential customers, e.g. names and contact information, for marketing purposes. They must not use unfair means to collect the data. For example,

(1) When an insurance practitioner changes job to work for another insurance institution, he should not make copies of the insurance policies or other information of his former customers from the records of his former employer.

(2) Some organizations or government authorities maintain registers or directories containing certain information of individuals. The registers or directories may be open for public inspection, but enquirers are required to give reasons for making the searches. If an insurance institution or insurance practitioner obtains personal data from such registers or directories for direct marketing by misrepresenting the reason for the search, the means of collection will be considered unfair.

3.5.2 No Change in Purpose of Use of the Data

In addition, insurance institutions and insurance practitioners should ensure that the use of the personal data for the intended marketing activities is within the original purposes of use of the data. If not, prescribed consent for the intended change of use must be obtained from the customers beforehand. In example (1) in section 3.5.1 above, the use of former customers' personal data for marketing products or services of the new insurance institution would unlikely be within the original purpose for which the data was collected by the insurance institution which employed him previously. In the case of personal data extracted from public registers or directories, insurance institutions and insurance practitioners should ensure that the permitted use of the personal data includes the intended marketing use. For further information in

this regard, please refer to section II entitled "When collecting personal data from other sources" of the DM Guidance Note issued in October 2010 by the Privacy Commissioner.

Attention is also drawn to the section under heading "Consent obtained in doubtful circumstances" in the DM Guidance Note. It should be noted that "bundled consent" (as explained in the DM Guidance Note) would not be accepted as a valid or effective prescribed consent for any change of use of personal data.

3.5.3 Case Study – information from government directory

The Complaint

The complainant, a government servant, continued to receive telephone calls from insurance agents of an insurer promoting its insurance services despite previous opt-out requests having been made to the insurer. The callers told the complainant that her name and telephone number were obtained from the government directory published in the government's website at www.directory.gov.hk.

Outcome

According to the "*Use Restriction of Directory Information*" displayed on the website, the information was provided to facilitate official communication between the government and the public, and the information was not intended for marketing activities. In the circumstances, the use of the complainant's data for making the marketing calls was contrary to the requirement of DPP3. The insurer was held liable for the insurance agents' acts of contravention done on its behalf.

In addition, the insurer was also liable for failing to comply with the complainant's opt-out requests in violation of section 34 of the Ordinance.

3.6 Retention of Customers' Personal Data

3.6.1 Establish a Retention Policy

In order to comply with the requirements of DPP2(2) and section 26 of the Ordinance in relation to the duration of retention of customers' personal data, insurance institutions should devise and implement clear privacy policies and practices to ensure erasure of such data after the purposes of collection have been fulfilled. In determining the period of retention, insurance institutions should take into account the

purposes of use of the data and any relevant statutory requirements and applicable guidelines (e.g. sections 20 of Schedule 2 to the AMLO in relation to the retention of customers' records).

In general, insurance institutions may retain personal data of customers for not more than seven years after the end of the business relationship e.g. a customer withdrew his/her insurance policy for the purposes of, for example, complying with the various legal or regulatory requirements for keeping books of accounts or customers' records, the handling of potential litigation, etc. However, different types of personal data may warrant different periods of retention which may be shorter or longer than seven years, and each case has to be considered based on its own circumstances. Exceptional features in a particular case may justify a shorter or longer period of retention, such as the need:

(1) for the handling of current or impending legal actions or claims;
(2) for the handling of current enquiries or complaints by the customers concerned or regulatory or law enforcement bodies;
(3) to facilitate performance of a contractual obligation due and owing to the data subject concerned;
(4) for keeping the data as evidence when there are reasonable grounds for believing that a crime has been or will be committed, and destruction of the evidence will prejudice the investigation of the crime by relevant law enforcement bodies;
(5) for compliance with a lawful or statutory duty to retain personal data;
(6) for compliance with applicable codes of practices or guidelines issued by the relevant regulatory bodies not inconsistent with the requirements under the Ordinance.

Insurance institutions should note that indiscriminate retention of personal data will increase the risk of personal data leakage and misuse. If a complaint is made to the Privacy Commissioner, the insurance institution will be asked to explain and justify its retention of the relevant personal data at the material time.

In addition, to avoid unnecessary retention of the data and to minimize the risk of leakage and misuse, insurance institutions should establish policies and practices in relation to the retention of customers' personal data by their insurance agents or representatives, taking into account the purposes of retention and use of the data by the agents or representatives.

Insurance institutions and insurance practitioners should note the Privacy Commissioner's ***Guidance Note on Personal Data Erasure and Anonymisation*** for guidance on how personal data should be permanently erased and the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify individuals.

3.6.2 Case Study – data of unsuccessful insurance applicants

The Complaint

An unsuccessful insurance applicant complained to the Privacy Commissioner against an insurer for retaining his application data after rejection of his application.

Outcome

It was the practice of the insurer to retain the personal data of unsuccessful insurance applicants for an indefinite period of time. According to the insurer, the reasons for retaining the data indefinitely were: (i) to comply with the various legal requirements for keeping books of accounts; (ii) to comply with the guidelines and circulars of the regulatory authorities; (iii) to handle potential litigation, enquiries and complaints; and (iv) to check the completeness and accuracy of the information in the event of future applications from the same applicant.

It was revealed that unsuccessful insurance applications comprised two categories, i.e. those where money transactions were involved (e.g. where premium was paid together with the application) and those which involved no money transaction. In the former case where books of account have to be kept, it is justifiable to keep the relevant data for the statutory period prescribed by the applicable ordinances. However, where no money transaction is involved, the insurer should not retain the personal data indefinitely simply for the reason that the person may re-apply in future. For the purposes of handling any future enquiry, complaint or legal action, a reasonable period of retention should be fixed.

For unsuccessful insurance applications where money transactions are involved, the optimal period of retention of the personal data concerned should generally not exceed seven years. For cases where no money transaction is involved, a retention period of two years will generally suffice to fulfill the various purposes mentioned by the insurer.

An enforcement notice was served on the insurer requiring it to erase the personal data which had been retained longer than the aforesaid prescribed periods (unless special circumstances existed justifying a longer retention period). The insurer complied with the enforcement notice and erased more than 7,000 records.

3.6.3 Case Study – insurance documents of ex-clients

The Facts

An insurance agent collected a large quantity of copy documents of his clients during his employment in various insurance institutions. Later, he became bankrupt and lost his insurance agent licence. He continued to keep the copy documents until one day he abandoned 3 cartons of copy documents containing the personal data of over 2,000 individuals at the staircase next to his home premises. A neighbour reported the case to the Police and the copy documents were seized.

Outcome

After investigation, the insurance agent was prosecuted for contravening section 26 of the Ordinance. The insurance agent pleaded guilty to the charge and was fined.

3.7 Use of Customers' Data for Internal Training

3.7.1 Preserve Anonymity

The nature of insurance business inevitably involves frequent collection and use of customers' sensitive personal data. Insurance institutions and insurance practitioners owe their customers a duty to ensure that their data is handled with caution and care. As required by DPP3, personal data of customers shall only be used for purposes that are consistent with or directly related to the original purposes of collection of the data. Any sharing of the data within or amongst the staff or insurance agents or representatives of the insurance institutions should be avoided unless it is necessary for the purposes of providing insurance services to the customer concerned and on a "need-to-know" and "need-to-use" basis.

It is not uncommon for insurance institutions to use policy information of real cases as illustrations during training provided to staff and insurance agents and representatives. Insurance institutions and their trainers should however not share any information that

may enable identification of the customers or beneficiaries. The identities of those individuals in most situations are irrelevant to the purposes of training. It is privacy intrusive to share information of customers or beneficiaries with insurance agents or representatives or parties not related to the policies concerned. Wherever possible, insurance institutions and their trainers should use fictitious personal data and made-up scenarios for training purposes.

3.7.2 Case Study – disclosure of policyholders' identities in training material

The Complaint

A Regional Director of an insurer in a training session held in mainland China used the insurance policy information of the complainant, her children and ex-husband in the presentation materials and disclosed their personal data to 55 insurance agents attending the training. The complainant was a former Regional Manager of the insurer under the supervision of the Regional Director. The complainant's agency contract with the insurer was terminated on purported grounds of inappropriate practice relating to issuing policies to individuals connected to her, including her children and ex-husband.

Outcome

The insurer explained that the policy information was used in the training to illustrate the complainant's unethical practice. The insurer argued that it was necessary to reveal the parties concerned as someone the trainees knew so as to raise the trainees' vigilance and enhance deterrence.

It was clear that the purpose of collection of the personal data in question was for providing insurance services to the customers concerned. It is not within a customer's reasonable expectation that his personal data provided for insurance purposes would be used for training of insurance agents or shared with insurance agents unrelated to his policy. It would not be necessary to disclose the identities of the complainant or the other customers in the training material in order to raise awareness. Mere mention of the professional capacity or role of the individuals concerned would suffice.

Accordingly, the disclosure of the personal data in the training session constituted a contravention of the requirement of DPP3 by the insurer, through the acts of the Regional Director as its agent.

3.8 Access to, Storage and Handling of Customers' Personal Data by Staff and Agents

In compliance with the requirement of DPP4, insurance institutions should implement security safeguards and precautions in relation to the security of customers' personal data held by them and their staff and agents. The security level should reflect the sensitivity of the data and the seriousness of the potential harm that may result from a security breach. Generally, a top-down approach is expected for insurance institutions to establish security governance, policies, standards and procedures on the handling of personal data held by them and their staff and agents. Such measures are expected to ensure the confidentiality and integrity of personal data held, as well as to maintain the accountability of access to and use of such personal data. Relevant security measures should include the following.

3.8.1 Measures to Ensure Integrity, Prudence and Competence of Staff and Agents

Staff and Insurance Agents and Representatives

Insurance institutions should take reasonably practicable measures to ensure that staff and insurance agents and representatives having access to customers' personal data (collectively, the "**relevant staff**") are trained in personal data handling and protection, exercise due care in applying the insurance institutions' personal data privacy policies, and are subject to procedures designed to ensure compliance with those policies. In formulating and implementing policies and internal procedures pertaining to the security of customers' personal data, insurance institutions should take heed of the following:

(1) the policy is systematically and regularly communicated to the relevant staff;
(2) on-going training is provided to the relevant staff on matters relating to personal data protection;
(3) new recruits are provided with training on personal data protection as part of their induction into the organization;
(4) relevant policy manuals, training materials, and handbooks are periodically reviewed and updated;
(5) access to, and processing of, personal data are restricted on a "need-to-know" and "need-to-use" basis;
(6) the relevant staff are required to sign a secrecy or confidentiality statement that clearly specifies operational expectations in these respects;
(7) appropriate investigative procedures are engaged should there be a security breach

and action taken against the relevant staff responsible for the breach;

(8) random checks are made to ensure compliance with established policy and procedures.

Outsourced Contractor

If third parties such as IT contractors and waste disposal contractors are entrusted with the handling of customers' personal data, insurance institutions should ensure the safe handling and erasure of the data by the contractors and to prohibit further or other use of the data. Insurance institutions should consider taking the following precautionary measures to protect the personal data and must adopt contractual or other means to safe handling and erasure of the data by contractors:

(1) select a reputable contractor offering sufficient guarantees as to its ability to ensure the security of the personal data it handles;

(2) incorporate the following requirements in the service contract with the contractor:
   (a) the security measures required to be applied by the contractor to protect any personal data that they may collect, view or use;
   (b) the prohibition of the contractor from using or disclosing personal data for any purpose not specified in the contract;
   (c) the obligation on the part of the insurance institution and the contractor to comply with the requirements of the DPPs;
   (d) the timely return of personal data when it is no longer required for the contractor to provide its services, and timely deletion from the contractor's systems, and any backups;
   (e) the immediate reporting of any sign of security abnormalities or breaches in respect of personal data;
   (f) the contractor should warrant that its staff have been properly trained in personal data handling;
   (g) there be no sub-contracting without the explicit consent of the insurance institution if the sub-contracting will involve processing or use of personal data;
   (h) the contractor be responsible for the sub-contractor's conduct relating to personal data handling;

(3) information that contains personal data should not be released to the contractor unless it is absolutely necessary for the contractor to complete the task;

(4) information that contains personal data should not be released to the contractor for the purpose of system testing;

(5) information passed to the contractor that contains personal data should be properly

labelled;

(6) the contractor should be checked from time to time to confirm that it is carrying out the required security measures and obligations in handling the personal data given to it;
(7) the contractor should be checked from time to time to confirm that it has carried out appropriate checks on its staff who handle the personal data;
(8) proper records and trail should be kept of all the personal data that has been given to the contractor;
(9) clear instructions should be given to the contractor in respect of the use, transmission, storage and destruction of the personal data given to it.

Insurance institutions and insurance practitioners are advised to refer to the informatoin leaflet ***"Outsourcing the Processing of Personal Data to Data Processors"*** issued by the Privacy Commissioner for engaging data processors.

3.8.2 Security through Controlled Access to and Secure Storage of Customers' Personal Data

As customers' personal data would be made available to the relevant staff, insurance institutions should take appropriate measures to protect the data against unauthorized or accidental access, processing or erasure. Examples of these measures are:

(1) Only authorized staff or insurance agents or representatives on a need to know basis are allowed to access customers' personal data.
(2) Access to customer database is protected by security features e.g. password.
(3) Copy/backup from the database, and image exported from the database should be authorized, monitored and accounted for, and reports on these database operations should be produced and reviewed regularly.
(4) Prominent warning notice should be generated whenever an end user accesses the database, and the end user should not export or save any personal data from the database unless formally approved.
(5) If a portable electronic storage device (e.g. portable computer, USB flash drive) is used, ensure that only necessary data is stored, that such data is encrypted and that it is deleted after use.
(6) Ensure that documents containing personal data are not disposed of recklessly. Paper shredders can be used for destroying those documents. If personal data stored in computer will not be used anymore, the data should be thoroughly erased.
(7) Where personal data is stored electronically, ensure that there are adequate IT

security measures in place.

3.8.3 Secure Transmission of Documents containing Personal Data

When transmitting documents containing personal data of customers, insurance institutions and insurance practitioners should ensure that the data is protected against unauthorized or accidental access by unrelated parties. For example:

(1) in the case of transmission by mail or via another person – sealed envelopes should be used; no sensitive data (e.g. HKIC number) is visible through the envelope window; and mail should be marked "private and confidential" if intended for the eyes of the addressee only;
(2) in the case of fax transmission – dedicated fax machine, if available, is used at the receiving end; advance notification should be given to the recipient of the incoming fax; and check the accuracy of the fax number before sending;
(3) in the case of electronic transmission – encryption, "confidential mail boxes" and/or passwords for access should be used.

3.8.4 Insurance Agents or Representatives Working at Home or Outside Workplace

Insurance agents and representatives often take documents or policies containing customers' personal data away from the office for working at home or other places. It is essential that they safeguard the data from loss or unauthorized access by third parties. When meeting customers in public places, insurance agents and representatives should ensure that personal data contained in documents such as insurance applications and insurance policies is not seen, and conversations concerning sensitive customer information are not overheard, by unrelated parties.

Insurance institutions should provide clear policies and guidelines to the relevant staff for handling customers' data outside the workplace to the effect that:

(1) only data which is necessary for carrying out their work may be taken away from the workplace in specified circumstances;
(2) if the relevant staff member uses his own personal computer, it should be of adequate security standard. For example, it should have up-to-date anti-malware software installed and be free from file-sharing software such as Foxy;
(3) adequate security protection is provided by encryption of the personal data stored in portable computers and other portable storage devices; and
(4) the data should be securely erased after the work is finished.

In considering whether to allow the relevant staff to take customers' personal data away from the workplace, the following factors should be taken into account:

(1) whether there is a real, reasonable or urgent need to process the data outside the workplace;
(2) why processing of the data within office premises is not reasonably practicable; and
(3) the sensitivity of the data and the seriousness of the harm that could result in the event of a data leakage.

For practical advice on the personal data protection aspects of using portable storage devices, please refer to the ***Guidance Note on the Use of Portable Storage Devices*** issued by the Privacy Commissioner.

3.8.5 Case Study – leakage of customers' data on the Internet

The Incident

A database containing the personal data of about 600 customers of an insurer including their names, dates of birth, addresses, telephone numbers and details of the insurance policies had been leaked and was accessible by the public on the Internet.

Outcome

It was revealed that the leakage of the data was caused by the inappropriate grant of access right to the data by the insurer to its insurance agent. The insurance agent uploaded and stored the data in a web file server at his home. As a result, the data was accessible by anyone using Internet search engines.

It was found that the guidelines issued to its insurance agents and control measures taken by the insurer were clearly insufficient to guard against unauthorized access, transfer, storage and processing of customers' personal data outside office premises, which led to the occurrence of the incident. Consequently, the insurer was found in breach of the requirement of DPP4 for failing to take sufficient measures to ensure security of the data.

An enforcement notice was issued, and in compliance the insurer implemented remedial measures. The measures included reviewing its operational procedures and strengthening controls over the access, transfer and security of customers' personal data, and in particular strengthening control over the processing of customers' personal data outside office premises.

3.9 Handling of Data Access Requests

An individual may make a request to an insurance institution to be informed whether it holds his personal data and if yes, be supplied with a copy of such data. Such request, usually referred to as a "data access request", may be made by the individual himself or by a "relevant person" on his behalf. "Relevant person" refers to:

(1) a person authorized in writing by the individual to make the request;
(2) where the individual is under 18, a person having parental responsibility for him, e.g. one of his parents;
(3) where the individual is incapable of managing his own affairs, a person appointed by a court to manage those affairs;
(4) where the individual is mentally incapacitated, his guardian appointed, or the Director of Social Welfare or any other person in whom his guardianship is vested or by whom the appointed guardian's functions are to be performed, under the Mental Health Ordinance.

Insurance institutions and insurance practitioners are advised to refer to the guidance issued by the Privacy Commissioner from time to time on the handling of data access and correction requests. The "Important Notice to Data User" contained in the Data Access Request Form (Form OPS003) prescribed by the Privacy Commissioner under the Ordinance provides explanatory notes on the handling of data access requests. The following case studies highlight some of the areas which insurance institutions and insurance practitioners should pay attention to.

3.9.1 Case Study – medical report containing information of other individual

A customer made a data access request to an insurer for a copy of his pre-insurance medical check-up report. The insurer replied that it would not provide the medical report to the customer as it contained the personal information of the examining doctor.

In general, an insurer may not refuse to comply with a customer's data access request for a copy of his personal data contained in a pre-insurance medical check-up report on the ground that it contains other's personal data. The insurer may remove or redact the names and identifying particulars of other individuals before supplying a copy of the data to the customer.

3.9.2 Case Study – no excessive fee should be charged for complying with a data access request

A customer made a data access request to his insurance broker for copies of his "lab test reports" prepared during pre-insurance medical check-ups conducted at the request of an insurer. Medical expenses for the check-ups were paid for by the insurer. The broker told the customer that the insurer would charge him HK$464 for supplying copies of the reports as reimbursement to the insurer for the medical expenses.

In complying with a customer's data access request for his personal data contained in a medical report which was made at the expense of an insurer, the insurer may not charge the customer for such medical expenses. However, the insurer may impose a fee which shall not be excessive for the purpose of covering only those costs which are directly related to and necessary for complying with the data access request. It may include the labour costs of the staff member in locating, retrieving and copying the requested data as well as actual out-of-pocket expenses such as photocopying charges and postage.

3.9.3 Case Study – legal professional privilege

An employee made a claim to his employer for injury sustained in the course of work. He was required by a loss adjuster engaged by the employer's insurer to attend medical examinations. The employee then made a data access request to the insurer for copies of his medical reports of the medical examinations. The insurer did not reply to the employee's request as it considered that the reports were covered by legal professional privilege and may be withheld from the employee.

Although under the Ordinance legal professional privilege can be a ground for refusing to comply with a data access request, the insurer should inform the employee in writing of the refusal and the reasons for refusal within 40 days after receiving the request. This is required under section 21 of the Ordinance.

4 CONCLUDING NOTE

It is hoped that this guidance note will highlight privacy pitfalls in relation to the handling of customers' personal data, and help insurance institutions and practitioners

review their current personal data systems and adopt good practices. A sound privacy policy and practice is conducive to building customers' trust and confidence, and beneficial to insurers' businesses and the insurance industry as a whole.

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, Wanchai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk

Copyrights

Disclaimer

The information provided in this guidance note is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of the law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and power conferred to the Commissioner under the Ordinance.