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 Banking Industry

CONTENTS

1. INTRODUCTION

Banks and other financial institutions (collectively, "**Banks**") play an important role in the everyday lives of citizens in Hong Kong. They collect, hold, process and use enormous amount of customers' information in their daily operations, which may include names, contact details, identification document numbers, employment details, financial and credit information, etc. Most individuals consider their banking/financial information sensitive and should be handled with extra care. Banks should therefore ensure that their data privacy policies and practices comply with the requirements under the ***Personal Data (Privacy) Ordinance (Chapter 486)*** ("**the Ordinance**") in protecting their customers' personal data.

This guidance note aims to assist the banking industry in understanding and complying with the relevant requirements under the Ordinance as well as promoting good practices in relation to the collection, accuracy, retention, use, security of and access to 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 bank customers' personal data are their names, addresses, telephone numbers, identity card numbers, dates of birth, occupations, account information, financial information, etc.

2.2 Who is responsible?

Section 4 of the Ordinance provides that a "data user" shall not do any act, or engage in any practice, that contravenes a data protection principle ("**DPP**"). Apart from DPPs, other provisions in the Ordinance also bind a data user, for example, Part V relating to access to and correction of personal data, Part VIA relating to direct marketing, etc. "**Data user**" is defined in the Ordinance to mean a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data. There is no doubt that a bank is a data user in relation to the personal data it holds of its customers. Accordingly, banks must observe all the requirements under the Ordinance to protect the personal data privacy of their customers.

2.3 The six data protection principles

The six DPPs provided in Schedule 1 to the Ordinance set out fair information practices with which data users must comply in the handling of personal data. They regulate the collection, accuracy, retention, use, security, transparency of policies and practices, as well as access to and correction of personal data.

2.3.1 Purpose and manner of collection of personal data

DPP1 provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user who is to use the data. Collection of the data must be necessary for or directly related to that purpose, and the data collected should be adequate but not excessive for that purpose. In addition, it provides that collection of personal data shall be by lawful and fair means, and sets out the information that a data user must give to a data subject when collecting personal data directly from that subject.

Practical example:

*When collecting customers' personal data, banks should carefully consider the necessity of collecting each item of the information to be collected. For example, collection of a savings account customer's name and contact information is necessary for the provision of the account services to the customer, but collecting the customer's racial origin or religious affiliation would in general be excessive for such purpose. Where customers are required to supply their personal data, they should be provided with a Personal Information Collection Statement ("**PICS**"). Please refer to section 3.1 below for detailed guidance on PICS.*

2.3.2 Accuracy and duration of retention of personal data

DPP2 requires all practicable steps be taken to ensure that personal data is accurate and kept no longer than necessary. Where a data user transfers personal data, whether within or outside Hong Kong, to a "data processor" for processing on its behalf, it must adopt contractual or other means to ensure that the data is not kept longer than is necessary. "**Data processor**" means a person who processes personal data on behalf of another person and does not process the data for any of his own purposes. Examples of data processors are IT service providers, payroll service companies and waste disposal companies.

Moreover, section 26 of the Ordinance obliges a data user to 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 dictates otherwise.

Practical examples:

(1) Before sending a bank statement to a customer, it is important that the bank takes all practicable steps to ensure that the address of the customer is accurate and up-to-date. If delivered to the wrong address, the customer's financial data may be disclosed to unrelated third parties. Banks should therefore remind its customers regularly and provide them with a channel to notify any change in their contact information.

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

2.3.3 Use of personal data

DPP3 provides that unless prior "prescribed consent" has been obtained from the data subject, personal data shall not be used for a "**new purpose**", i.e. any purpose other than the purpose for which the data was collected or a directly related purpose. In this context, "**use**" includes disclose or transfer the personal data. Under section 2(3) of the Ordinance, "**prescribed consent**" means an express consent given voluntarily and which has not been withdrawn in writing. Prescribed consent may be given by a "**relevant person**" on behalf of a data subject who is:

(a) (i) a minor, (ii) incapable of managing his own affairs, or (iii) a mentally incapacitated person; and

(b) incapable of understanding the new purpose and deciding whether to give prescribed consent,

provided that the relevant person and the data user both have reasonable grounds for believing that the change of use is clearly in the interest of the data subject.

"**Relevant person**" refers to:

(a) the person having parental responsibility for a minor;

(b) the person appointed by court to manage the affairs of someone who is incapable of managing his own affairs;

(c) the guardian of a mentally incapacitated person under Parts IIIA or IVB of the Mental Health Ordinance (Chapter 136).

In addition, under section 64 of the Ordinance, a person commits an offence[1] if he discloses any personal data of a data subject obtained from a data user without the data user's consent with the intention:

(a) to obtain gain in the form of money or other property for himself or another; or

(b) to cause loss in the form of money or other property to the data subject.

A person will also commit an offence if he discloses, irrespective of his intent, any personal data of a data subject obtained from a data user without the data user's consent and the disclosure causes psychological harm to the data subject.

Practical examples:

(1) In general, unless prescribed consent has been obtained from the customer concerned, banks should not disclose the account data of a customer to his employer or family members.

(2) An ex-staff member of Bank A should not use Bank A's customers' personal data for soliciting business in the form of loan transfers for his new employer, Bank B.

(3) Bank staff should not without the bank's permission obtain a customer's prejudicial financial information from the bank's records and disclose it, for example, on the internet thereby causing psychological harm to the customer.

2.3.4 Security of personal data

DPP4 requires a data user to take all practicable steps to protect the personal data held by it against unauthorised or accidental access, processing, erasure, loss or use. Where a data user transfers personal data, whether within or outside Hong Kong, to a data processor for processing on its behalf, it must adopt contractual or other means to ensure that the data is so protected.

Practical examples:

(1) Customers' data stored electronically in database, computers or portable storage devices should be protected with adequate IT security measures and access control.

(2) In engaging a marketing company to carry out a customer opinion survey, banks must ensure the safe handling and erasure after use by the marketing company of the data transferred to it to safeguard against unauthorised access or use of that data.

[1] The maximum penalty for the offence is a fine of HK$1 million and imprisonment for 5 years.

2.3.5 Information to be generally available

DPP5 requires a data user to take all practicable steps to ensure openness and transparency about its personal data policies and practices, the kind of personal data it holds and the main purposes for which the data is used.

Practical example:

*Banks should formulate and make available to the public their Privacy Policy Statements ("**PPS**") stating in detail the kinds of personal data held, main purposes of using the personal data and their privacy policies and practices in place. The PPS may be displayed on the banks' websites.*

2.3.6 Access to personal data

DPP6 provides that a data subject has the right of access to and correction of his personal data held by a data user. According to sections 19 and 23 of the Ordinance, the data user is 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 Part V of the Ordinance.

Practical example:

A customer recently changed his nationality and notified the same to his bank. To ensure the bank has duly updated his nationality, he may make a request to the bank to be informed whether it holds information about his nationality in specific records, for example, his customer profile, and be supplied with a copy of such data within 40 days. Please refer to section 3.11 below for further discussion on data access request.

2.4 Code of Practice on Consumer Credit Data

Section 12 of the Ordinance empowers the Privacy Commissioner for Personal Data ("**the Commissioner**") to issue codes of practice for providing practical guidance in respect of any requirements under the Ordinance imposed on data users. The ***Code of Practice on Consumer Credit Data*** ("**the CCD Code**") was issued by the Commissioner to regulate the sharing and handling of consumer credit data by credit providers through credit reference agencies. It deals with issues of collection, accuracy, retention, use, security, access and correction as they relate to personal data of individuals who are, or have been, customers or applicants for consumer credit. The CCD Code covers, on one hand, credit reference agencies, and on the other hand, credit providers in their dealings with credit reference agencies and debt collection agencies. Failure to comply with the CCD Code will give rise to a presumption against the defaulting data user in any proceedings for non-compliance with the relevant requirement under the Ordinance.

Banks as credit providers should therefore refer to the CCD Code for guidance on the handling of customers' credit data.

2.5 Part VI A of the Ordinance – Direct marketing

2.5.1 The new laws on direct marketing

The ***Personal Data (Privacy) (Amendment) Ordinance 2012*** revamps the direct marketing regulatory framework by repealing the old section 34 of the Ordinance and replacing it with a new Part VI A, to take effect on 1 April 2013.

Under the new regime, a data user must, before using personal data in direct marketing, take the following "**specified actions**":

(1) inform the data subject:

(a) that it intends to so use the data;

(b) that it may not so use the data unless the data subject consents;

(c) of the kinds of data to be used;

(d) of the classes of products or services to be marketed; and

(2) provide the data subject with a response channel for communicating his consent.

The above information must be presented in a manner that is easily understandable and, if in writing, easily readable. The data user must not use the data in direct marketing without the data subject's consent and any such use with the data subject's consent must be restricted to the kind of data and the class of products or services as permitted by the data subject.

In addition, a data user must not provide personal data to another person ("**the recipient**") for use in direct marketing unless the data user has:

(1) informed the data subject in writing in an easily understandable and readable manner:

(a) that it intends to so provide the data;

(b) that it may not so provide the data unless the data subject consents in writing;

(c) that the provision is for gain (if that is the case);

(d) of the kinds of data to be provided;

(e) of the classes of persons to which the data is to be provided;

(f) of the classes of products or services to be marketed;

(2) provided the data subject with a response channel for communicating his written consent; and

(3) received the data subject's written consent.

Any such provision must be restricted to the kind of data, the class of transferees and the class of products or services as permitted by the data subject. In such case, the recipient need not take the above specified actions nor obtain the customer's consent again before using the data for direct marketing in relation to the permitted class of products or services if the data user has by notice in writing informed the recipient that the above requirements for the provision of the data have been complied with and specified the permitted class of products or services. However, the data user must cease to so provide the data and the recipient must cease to so use the data if the data subject so requires at any time.

When a data user uses personal data in direct marketing 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, which he is entitled to do at any time irrespective of whether he has earlier given consent to such use of his personal data, the data user must cease to so use the data.

The above is a brief description of the major requirements under the new direct marketing regime. There are also specific provisions regarding the treatment of pre-existing data, that is, personal data the use of which was controlled by the data

user before 1 April 2013. For a more detailed discussion on direct marketing, please refer to the Commissioner's ***New Guidance on Direct Marketing*** ("**the DM Guidance Note**").

2.5.2 Formulate and implement policy, procedure and guideline to ensure compliance

In order to ensure compliance with the requirements relating to direct marketing, banks should formulate and implement relevant privacy policies, procedures and guidelines, and take all practicable steps to ensure compliance by the staff. The requirements of communicating to the customers the intended use or provision of their personal data for use in direct marketing must be adhered to and the customer's right of self-determination over such use of the data must be respected. Consideration should be given to adopting the good privacy practices recommended in the DM Guidance Note. More importantly, top management should recognise the obligations of its bank, and support and promote the bank's efforts in compliance with the relevant requirements and establishing standard operation procedures and guidelines.

2.6 Liabilities of banks for acts of staff, agents and contractors

2.6.1 Liabilities of employers and principals

Under section 65(1) and (2) of the Ordinance, any act done or practice engaged in by an employee in the course of employment or by an agent for another person with the authority of that person shall be treated as done or engaged in by his employer or principal as well as by him. Accordingly, a bank is accountable for the acts done or practices engaged in by its staff in the course of providing its services to customers. A bank is also answerable for the acts or practices of its agents or contractors, for example IT contractors, debt collection agents or marketing agents, done or engaged in within the scope of authority given to them.

A defence is available to an employer for an act or practice alleged to have been done or engaged in by its employee if it can prove that it took practicable steps to prevent the employee from doing that act or engaging in that practice.

Banks are therefore advised to take the following precautionary measures.

2.6.2 Precautionary measures for staff

Banks should take practicable measures to ensure that their staff having access to customers' personal data are trained in personal data handling and protection, exercise due care in applying the banks' 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 customers' personal data, banks should take heed of the following:

(1) the policy is systematically and regularly communicated to staff;

(2) on-going training is provided to 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 organisation;

(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) staff are required to sign a secrecy or confidentiality statement that clearly specifies operational expectations in these respects and possible

sanctions against those in breach, or incorporate such statement into the staff manual or code of conduct;

(7) appropriate investigative procedures are engaged in the event of a breach and action taken against staff responsible for the breach;

(8) appropriate system controls are built in and regular internal audits and random checks are made to ensure compliance with established policy and procedures.

2.6.3 Precautionary measures for agents and contractors

If third parties such as debt collection agents, data programmers, IT contractors or confidential waste disposal companies are entrusted with the handling or processing of customers' personal data, banks should ensure the safe handling and erasure of the data. Banks should consider, where appropriate, taking the following precautionary measures to protect the data:

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

(2) incorporate the following requirements in the service contract with the agent or contractor:

(a) the security measures required to be applied by the agent or contractor to protect any personal data that it may collect, view, process or use;

(b) the prohibition on the agent or contractor from processing, using or disclosing personal data for any purpose not specified in the contract;

(c) the obligation on the part of the bank and the agent or contractor to comply with the requirements of the DPPs;

(d) the timely return of that personal data when they are no longer required for the agent or contractor to provide its service, and timely and complete deletion from the systems of the agent or contractor, and any backups;

(e) the timely reporting of any sign of irregularity in the security of or security breach in respect of that personal data;

(f) the agent or 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 bank if the sub-contracting will involve processing or use of personal data;

(h) the agent or contractor be responsible for the sub-contractor's conduct relating to personal data handling or processing;

(3) not to release information that contains personal data to the agent or contractor unless it is absolutely necessary for the agent or contractor to complete the task;

(4) not to release information that contains actual personal data to an IT contractor for the purpose of system testing (but use dummy data instead);

(5) information passed to the agent or contractor that contains personal data should be properly labeled;

(6) keep proper records and trail of all the personal data that have been given to the agent or contractor;

(7) give clear instructions to the agent or contractor in respect of the use, processing, transmission, storage and destruction of the personal data given to it;

(8) check the agent or contractor from time to time to confirm that it is carrying out the required security measures and obligations in handling or processing the personal data given to it;

(9) check the agent or contractor from time to time to confirm that it has carried out appropriate checks on its staff who handle or process the personal data.

Where a data processor is engaged, banks should also refer to the Commissioner's Information Leaflet: ***"Outsourcing the Processing of Personal Data to Data Processors"*** **("the Data Processors Information Leaflet")** for further guidance.

3. PROTECT CUSTOMER'S RIGHT TO PERSONAL DATA PRIVACY

The following notes aim to assist the banking industry in better understanding the application of the Ordinance in particular areas concerning customer's personal data. They promote compliance with the provisions of the Ordinance, as well as the adoption of good practices, in the handling of customers' personal data by banks.

3.1 Personal Information Collection Statement

3.1.1 Contents

In order to comply with the requirements of DPP1(3), banks are advised to formulate and provide customers with PICS containing the following information:

(1) **Purpose statement**: This is a statement of purposes for which the customer's personal data will be used after collection. Though the statement may be made in general or specific terms, the purposes must be explicitly stated. Banks should not use liberal or vague terms as it would not be practicable for the customer to ascertain with a reasonable degree of certainty how his personal data is to be used. A simple example of a purpose statement: "*The information collected from you will be used for the purpose of processing your application to open an investment account with us.*"

(2) **Transferee statement**: This should 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. For example: "*The data that you have supplied in this account opening form may be transferred to law enforcement agencies for the purpose of prevention of money laundering.*"

(3) **Optional or obligatory provision of data**: Unless it is obvious from the circumstances, banks should explicitly inform customers whether it is obligatory or voluntary for them to supply their personal data, and if obligatory, the consequences of failure to supply the data. Even if voluntary, it is good practice to also state the consequences of a failure to supply. For example: "*It is voluntary*

for you to supply your personal data in this complaint form regarding your complaint against the bank's services. However, if you fail to do so, we may not be able to process your complaint."

(4) **Data access and correction rights**: Banks must explicitly provide information on the customer's rights of access to, and correction of, his personal data, and the name, or job title, and address of the officer who is to handle the data access or correction request. For 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. Your request will be handled by our Customer Services Manager whose address is …. If you wish to make a request or have any queries, please contact our Customer Services Manager by … (specify here the address or means of contact)"*

3.1.2 What practicable steps to take

DPP1(3) requires a bank to take all practicable steps to give the above prescribed information to a customer on or before collecting his personal data from him (save that the information on data access and correction rights may be given on or before first use of the data). Although the Ordinance does not require the provision of the information in writing, it is prudent for the bank to inform the customer by way of a written notice (i.e. PICS). This may be done by incorporating the PICS in the service application form or by attaching the PICS as a separate notice. Where personal data is collected over the phone, unless the PICS has already been given to the customer before the call or it is not practicable to do so, the prescribed information should be given, for example in a recorded message prior to the collection of the personal data. In such cases, it is good practice to follow through by sending the PICS to the customer.

Banks may collect personal data from customers in different situations for different types of services, for example for opening a safety-deposit box or in a loan application. Banks should therefore ensure that the PICS used sufficiently deals with the particular circumstances in which personal data is collected.

Banks should communicate their message effectively in clear and simple language and in a form easily accessible, readable and understandable by reference to the actual circumstances under which the personal data will be collected, paying special attention to the different needs of the customers (in terms of literacy, first language used, etc.).

To ensure that a PICS is effective, it is necessary for banks to take into consideration the following factors:

(1) whether the layout and presentation of the PICS (including the font size, spacing, underlining, use of headings, highlights and contrasts) enable the PICS to be easily readable by customers with normal eyesight;

(2) whether the PICS is presented in a conspicuous manner (for example the PICS is in a stand-alone section of the service application form and its contents are not buried among the terms and conditions for the provision of the bank's services);

(3) whether the language used in the PICS is easily understandable (by the choice of simple words over difficult words, legal terms and convoluted phrases);

(4) whether further assistance from the bank such as help desk or enquiry service is available to assist the customer in understanding the contents of the PICS.

In the event of repeated collections of personal data from a customer for the same purposes, it is not necessary for the bank 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[2].

3.1.3 Case study

(1) Collecting additional data from savings account applicants[3]

The complaint

A bank required a customer applying for a savings account to provide his "education level" and "marital status". The bank explained that these personal data items were collected for promoting to the customer its products and services. There was no indication in the account application form that the supply of the two items was "optional".

Outcome

The data relating to "education level" and "marital status" are not necessary for the purposes of providing savings account services to the customer. Even though the data may assist the bank in carrying out customer profiling and segmentation such as to facilitate use in direct marketing, the bank should not collect such data unless they are provided by the customer voluntarily[4].

Despite the bank's clarification that the supply of the data was not obligatory, the Commissioner found that the bank had not taken all practicable steps to ensure that the customer was so informed, explicitly or implicitly. It thus contravened DPP1(3)(a)(i) of the Ordinance. The bank has subsequently revised its savings account opening form to indicate that the data items in question are optional information, and briefed its frontline staff to handle collection of personal data from customers accordingly.

(2) Collecting credit card applicant's personal data in on-street promotional activity[5]

The complaint

A credit card customer complained against the bank for passing his personal data to an insurance company to make marketing approaches to him. The bank collected the customer's data in a winter evening during an on-street promotional activity in which the customer signed a credit card application form. The bank relied on the cautionary note, declaration and terms in the application documents and the bank's PPS attached to the application form for disclosing the customer's data to the insurance company. In particular, the PPS provided that: "*Data held by [the bank] relating to a Data Subject will be kept confidential but it may provide such information to:- ... (xi) selected companies for the purpose of informing Data Subjects of services which [the bank] believes will be of interest to Data Subjects.*"

[2] See section 35 of the Ordinance.
[3] See the Commissioner's investigation report no.R11-8371 issued on 15 December 2011.
[4] Reference may be made to the DM Guidance Note.
[5] See the Commissioner's investigation report no.R11-1982 issued on 20 June 2011.

Outcome

In view of the customer's eyesight problem, age and the fact that the incident took place during an on-street promotional activity in a winter evening, the Commissioner considered that it was difficult for the customer to carefully read, consider and understand the cautionary note, declaration and terms in the application documents and the PPS. In addition, the Commissioner found that the PPS was printed in unreasonably small print, and that the classes of data transferees were described in such liberal and vague terms that it would not be practicable for the customer to ascertain with a reasonable degree of certainty who could have the use of his personal data. In conclusion, the bank was found to have contravened DPP1(3)(b)(i) of the Ordinance for failing to explicitly inform the customer of the classes of persons to whom his personal data might be transferred.

3.2 Collection of identification document number from non-account holder

3.2.1 Code of Practice on the Identity Card Number and other Personal Identifiers

There is no question that a bank may collect the identification document number of its account holder. The situation would be different in the case of a non-account holder who may require the service of a bank in carrying out for him an "occasional transaction" such as money changing, issuing a cashier order or wire transfer. In such a case, the bank may only collect the identification document number of a non-account holder where the transaction amount exceeds certain prescribed limits (see below).

According to DPP1(1), a bank shall not collect personal data from a non-account holder unless the collection is necessary for or directly related to the service offered to such customer. In addition, the collection of Hong Kong Identity Card Number ("**HKID Card Number**") or other identification document number is governed by the ***Code of Practice on the Identity Card Number and other Personal Identifiers*** ("**the PI Code**") issued by the Commissioner. A data user must not collect HKID Card Number or other identification document number of an individual unless permitted in the situations set out in paragraph 2.3 of the PI Code. Moreover, in accordance with paragraph 2.2.1 of the PI Code, the individual should be given the option of providing other identification document number, such as a passport number, in lieu of furnishing his HKID Card Number.

Of practical relevance to this issue is paragraph 2.3.1 of the PI Code, read together with the requirements relating to customer due diligence and record-keeping contained in Schedule 2 to the ***Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Chapter 615)*** ("**the AMLO**"). Paragraph 2.3.1 of the PI Code allows a data user to collect the HKID Card Number (or other identification document number) of an individual if a statutory provision requires the data user to do so. In considering whether the AMLO requires banks, which are institutions authorised under the ***Banking Ordinance (Chapter 155)*** ("**AIs**") to collect identification document numbers of non-account holders, sections 3(1)(b), 3(1)(c), 12 and 20(1) of Schedule 2 to the AMLO concerning customer due diligence and record-keeping obligations with regard to "**occasional transaction**" (as defined in section 1(1) of Schedule 2 to the AMLO) carried out for a customer are relevant. Based on current requirements, an AI may collect the identification document number of a non-account holder when carrying out for him any occasional transaction equal to or exceeding an

aggregate value of HK$120,000, whether carried out in a single operation or several operations that appear to the AI to be linked, except that in the case of a wire transfer, the aggregate value is HK$8,000 or above.

3.2.2 Case study – money changing

The complaint
The complainant went to a bank to change his HK$500 note into five HK$100 notes. Since he did not hold an account with the bank, the counter officer recorded the complainant's name and HKID Card Number according to the bank's policy.

Outcome
The Commissioner took the view that there was no prima facie evidence to suggest that the money changing (for an amount less than HK$120,000) involved money laundering or terrorist financing activities, hence there was insufficient ground to justify collection of the complainant's name and HKID Card Number in the circumstances. The bank subsequently ceased such practice.

3.3 Accuracy of customer's contact information

3.3.1 Avoid disclosing customer's personal data to unintended recipient

DPP2(1) requires banks to ensure the accuracy of customers' personal data. If the data is inaccurate, banks should either rectify or erase it. It is therefore important that before contacting a customer, for example sending documents containing personal data to a customer, banks should ensure that the contact information is accurate and up-to-date. Delivery to the wrong address may lead to disclosure of the data to third parties.

This however is not an absolute requirement. So long as a bank has taken all practicable steps to ensure accuracy, there is no breach of this requirement if the data turns out to be incorrect.

3.3.2 Case study – bank documents sent to wrong and incomplete addresses[6]

The complaint
A credit card customer provided her correspondence address in "Shek Tong Tsui" to a bank. Since there was no choice of "Shek Tong Tsui" in the pull down menu of the district field in the bank's system for inputting a customer's address, the bank's employee chose "Siu Lam" from the menu as the district for the address. The customer discovered the mistake when she received a letter (albeit wrongly addressed) from the bank. She then made a correction request to the bank by using its amendment form. The customer did not receive any further credit card statements from the bank and later learnt from the bank that her statements had been sent to an address without flat and floor information because its employee failed to input the flat and floor information into the system when processing her correction request. On both occasions, the bank's double-checking procedures failed to spot the mistakes.

Outcome
The Commissioner found that the mistakes were made by the bank due to carelessness of its employees and failure of its checking procedures. The bank had breached DPP2(1) for failing to take all practicable steps to ensure accuracy of the customer's address data. The Commissioner considered that by improving the bank's computer system and automated/manual checking procedures, similar mistakes could be avoided in future.

[6] See the Commissioner's case note no.2009C08 (published on the PCPD's website).

3.4 Retention of customers' personal data

3.4.1 Establish a retention policy

In order to comply with the requirements of DPP2(2) and section 26 of the Ordinance in relation to the retention of customers' personal data, banks should devise and implement clear privacy policies and practices to ensure erasure of the data when the purposes of collection have been fulfilled. In determining the period of retention, banks should take into account the purposes of use of the data and any relevant statutory requirements and applicable guidelines[7].

For example, banks may be able to justify the retention of customers' personal data for seven years after the creation of the relevant data or the end of the business relationship (as the case may be) for the purposes of 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, and each case has to be considered on its own circumstances. Exceptional circumstances may apply in a particular case which justify a longer period of retention, such as:

(1) for the handling of current or impending legal action or claim;

(2) for the handling of current enquiry or complaint by the customer concerned or a regulatory or law enforcement body;

(3) to facilitate performance of a contractual obligation due and owing to the customer concerned;

(4) for keeping as evidence when there is reasonable ground for believing that a crime has been or will be committed, and destruction of the evidence will prejudice the investigation of the crime by a law enforcement body;

(5) for compliance with a lawful or statutory duty to retain personal data;

(6) for compliance with applicable code of practice or guideline issued by a regulatory body not inconsistent with the requirements under the Ordinance.

Banks must exercise good judgment and care in determining the appropriate length of retention of customers' personal data with due regard to the purpose of collection of the data. Indiscriminate retention of personal data will increase the risk of data leakage and the costs of safeguarding the data against unauthorised access or other uses which may jeopardise the interests of the customers. If a complaint is made to the Commissioner, the bank concerned will be asked to explain and justify its retention of the relevant personal data at the material time.

Banks are also advised to refer to the 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.

3.4.2 Case study – retention of customers' bankruptcy data[8]

The complaint

A customer complained against a bank for retaining information about his bankruptcy long after his discharge from bankruptcy. It was revealed that the bank's practice was to

[7] For example, section 20 of Schedule 2 to the AMLO contains requirements in relation to the retention of customers' records.
[8] See the Commissioner's investigation report no.R11-6121 issued on 15 December 2011.

retain customers' bankruptcy data for 99 years. Bankruptcy data were provided periodically to the bank by the Official Receiver for investigation and seizure of the bankrupts' assets.

After commencement of investigation by the Commissioner, the bank reduced its retention period to 15 years from closure of customers' accounts and sought to justify it on various grounds.

Outcome

The Commissioner rejected the grounds submitted by the bank due to lack of justification. The Commissioner was of the view that the bankruptcy data should not be kept longer than eight years for the reason that a bankrupt would normally be discharged upon expiry of a period of four to eight years of the commencement of the bankruptcy. As such, the bank's retention of the data was longer than necessary, thus contravening section 26(1) and DPP2(2) of the Ordinance. The bank has subsequently revised its policy not to retain customers' bankruptcy data for more than eight years from the respective dates of the declaration of bankruptcy.

3.5 Intra-group sharing of customers' personal data

3.5.1 Inform customer of any intended sharing

In Hong Kong, banks typically belong to a group of companies, either as the head of the group, or as one of the member companies of the group headed by a holding company. These entities are involved primarily (though not necessarily exclusively) in providing financial services, such as banking, securities and insurance. There could well be situations where it is necessary to share customers' personal data within the group of companies for providing the services sought by the customers or directly related matters. In such cases, banks are advised to inform customers in their PICS of the details of any intended sharing. Other than the information prescribed in DPP1(3)(b)(i), it may include the kinds of data to be shared as well. Where appropriate, it is also good practice to inform customers of the security measures in place to protect the data during the sharing process and the safe disposal of the data after use.

3.5.2 Not to change the purpose of use of the data or share unnecessary data

As required by DPP3, the personal data of a customer shall only be used for a purpose that is the same as or directly related to the original collection purpose. In determining the original purpose of collection of personal data of a customer and whether there is a breach of DPP3, it is important to note that the PICS given to the customer at the time of collection of the data is not the only factor to be considered. Other factors may include, e.g. the nature of the transaction and the circumstances under which the data is collected. Unless prescribed consent is obtained, any sharing of the data within the bank's group of companies should be restricted to the purposes of collection or directly related purposes including the purpose of providing the banking service to the customer and on a "need-to-know" and "need-to-use" basis.

Further, the data being shared should be adequate but not excessive having regard to the purpose of the sharing. Any sharing of unnecessary data could result in breach of DPP3.

3.5.3 Keep track of the shared data and ensure proper disposal of the data after use

In order to ensure security and timely disposal of the personal data shared within the group, it is important to monitor the whereabouts of the data. Banks are advised to keep proper logs to record the movement of the data. If the purpose for which the data is shared has been

fulfilled, the bank providing the data as well as the group company receiving the data should ensure timely and complete erasure of the data from the latter's files and records unless there is justification for continued retention of the data.

3.5.4 Establish a group policy on sharing of customers' personal data

Where it is the practice of group companies to share customers' personal data within the group, a holistic approach to data protection system is clearly advisable. Hence, a banking group engaging in customer data sharing on a regular basis is advised to have in place a group-wide privacy policy and procedures governing such activities within the group. The policy and procedures should cover processes pertaining to (i) customer notification and (ii) the collection, holding, processing, accuracy, access, use, sharing, transmission, security and disposal of the shared data. The respective responsibilities of each of the group companies and their personnel involved in the handling of the data should be set out clearly.

3.6 Transfer of customers' personal data outside Hong Kong

Section 33 of the Ordinance prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. This section is not in force yet. In any case, any transfer of personal data, whether within or outside Hong Kong, must also comply with the requirements of DPP1(3) (notify the data subject as to the classes of transferees), DPP2 (not to transfer inaccurate data; prevent data transferred to data processor from being kept longer than necessary), DPP3 (not to change the purpose of use) and DPP4 (safeguard data security). Furthermore, if following the transfer, control is retained over the personal data by the data user, all provisions of the Ordinance continue to apply in relation to the transferred data. For example, if the data is transferred by a data user to its outsourcing agent situated outside Hong Kong for processing the data, the data user remains liable for all acts done by its agent in relation to the mishandling of the personal data.

Global transfers of information are now a common and essential component of daily banking activities. For the transfer of customers' personal data to places outside Hong Kong, banks should heed the recommendations set out below (though most of which also apply to transfer within Hong Kong).

3.6.1 Inform customers at the time of collection about the transfer

When collecting personal data which a bank intends to transfer to a place outside Hong Kong, the bank should inform the customer of the classes of the transferees. In addition, it is good practice to also inform the customer of the kinds of data to be transferred outside Hong Kong, the purpose of the transfer, and where the bank considers appropriate, the place to which the data is to be transferred. If no such transfer is intended, the bank may also wish to so inform its customers.

3.6.2 Not to change the purpose of use of the data and not to transfer inaccurate data

In compliance with DPP3, any transfer of a customer's personal data must accord with the purpose for which the data was originally collected or a directly related purpose.

Where there are reasonable grounds for believing that the data is inaccurate, no transfer should be made unless and until the data is rectified. This is required under DPP2(1).

3.6.3 Steps be taken to protect the data

DPP4(1) requires, inter alia, the safe transmission of personal data. In transmitting customers' data, banks must take security measures to guard against unauthorised or accidental access, processing, erasure, loss or use of the data. If the data is sent over the Internet, special care is needed to ensure that adequate security measures are in place, for example encryption of the data. In this regard, banks are advised to refer to the section under the heading "DPP4 – Security of Personal Data" in the Commissioner's ***Guidance Note for Data User on the Collection and Use of Personal Data through the Internet*** ("**the Internet Guidance Note**") for further guidance.

If a bank transfers personal data to a data processor for processing on its behalf, the bank must adopt contractual or other means to safeguard security of the data as required under DPP4(2).

3.6.4 Ensure proper disposal of the data after use

If the data is transferred to a company within a bank's group, the bank should ensure timely and complete erasure of the data after fulfillment of the purpose of the transfer as recommended in section 3.5.3 above.

Where the data is transferred to a data processor for processing on behalf of a bank, the bank is required by DPP2(3) to adopt contractual or other means to prevent the data from being kept by the processor for longer than is necessary.

For guidance on what contractual or other means the bank may take to ensure security and proper disposal of the data transferred to the data processor, reference may be made to the Data Processors Information Leaflet.

3.7 Disclosure of customers' personal data to law enforcement agencies and financial regulators

Banks should handle requests for disclosure of customer personal data from law enforcement agencies or financial regulators with caution. In the event that the disclosure is not within or directly related to the original purpose of collection, it can only be made if the situation falls within an exemption under Part VIII of the Ordinance in relation to the provisions of DPP3. Otherwise, prescribed consent must be obtained from the customer concerned.

3.7.1 Whether an exempted purpose

Part VIII of the Ordinance provides a number of exemptions from the provisions of DPP3. Sections 58 and 60B are the most relevant here.

Section 58(2) exempts personal data from DPP3 where the use of the data is for any of the purposes specified in section 58(1) and the application of DPP3 to such use would be "likely to prejudice" any of those purposes. The purposes referred to in section 58(1) include (but not exclusively):

(a) the prevention or detection of crime[9];

(b) the apprehension, prosecution or detention of offenders;

[9] As provided in section 58(6), crime means an offence under the laws of Hong Kong or if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place.

(c) the assessment or collection of any tax[10] or duty;

(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct[11], or dishonesty or malpractice, by persons;

(e) the prevention or preclusion of significant financial loss arising from (i) any imprudent business practices or activities of persons or (ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(f) discharging certain functions of a "financial regulator".

"Financial regulator" includes the Hong Kong Monetary Authority ("**HKMA**"), the Securities and Futures Commission ("**SFC**"), Hong Kong Exchanges and Clearing Limited, the Commissioner of Insurance and the Mandatory Provident Fund Schemes Authority.

In addition, section 58(2) creates a defence for a data user who can show, in any proceedings against it for using personal data contrary to DPP3, that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of the matters mentioned in section 58(1).

Another exemption from DPP3 is given under section 60B which exempts personal data the use of which is required or authorised by or under any enactment, by any rule of law or by a Hong Kong court order, or is required in connection with any legal proceedings in Hong Kong.

Depending on the particular circumstances of the case, disclosure of customers' data to law enforcement agencies or financial regulators may fall within one of the exemptions mentioned above.

For example, SFC may under section 183(1) of the ***Securities and Futures Ordinance (Chapter 571)*** issue to a bank a notice to produce certain records or documents which may contain a customer's account information. Disclosure of personal data by the bank pursuant to the notice would be exempted from DPP3 under section 60B of the Ordinance by reason that it is required by or under that ordinance.

In other cases, a bank may receive a law enforcement agency's request for a customer's personal data claiming that the data is required for an exempted matter under section 58(1) of the Ordinance. In order to invoke the exemption under section 58 of the Ordinance in relation to DPP3, it is important to consider whether the effect of non-disclosure in a particular case would indeed be so serious as to be "likely to prejudice" any such matter, as required by section 58(2)(b). In case of doubt, it is prudent for the bank to ask the requesting body the purpose for which the data is to be used, why the data is considered necessary or important for that purpose and, in particular, how the failure to disclose the data would be likely to prejudice that purpose. By asking for the supply of more information, the bank is put in a better position to invoke the defence under section 58(2) in proceedings or when a complaint is lodged against it for alleged contravention of DPP3 in disclosing the data. The bank

[10] As provided in section 58(1A), "tax" includes any tax of a territory outside Hong Kong if arrangements having effect under section 49(1A) of the Inland Revenue Ordinance (Chapter 112) are made with the government of that territory and that tax is the subject of a provision of the arrangements that requires disclosure of information concerning tax of that territory.

[11] Under section 2(9), any conduct by virtue of which a person ceases, or would cease, to be a fit and proper person for any office, profession or occupation as required by law is deemed to be "seriously improper conduct". In addition, according to case law, breach of a court order and a bankrupt police officer's serious indebtedness in breach of the Police General Orders are also examples of "seriously improper conduct".

being the data user in control of the data should satisfy itself as to the applicability of the exemption it relies on to disclose the data[12].

3.7.2 Prescribed consent

If disclosing a customer's personal data to a law enforcement agency or financial regulator is not within or directly related to the original purposes of collection of the data and no exemption is applicable to or is to be invoked for such disclosure, a bank should not make the disclosure unless prior prescribed consent has been obtained from the customer concerned. The prescribed consent must be expressly and voluntarily given by the customer and should be sufficiently clear and specific to cover the particular disclosure in question. Banks should also note that a "**bundled consent**" is not accepted by the Commissioner as constituting a prescribed consent for the purposes of the Ordinance. Example of a "bundled consent" situation is where a data user collects personal data from a customer through a service application form which is designed in such a way that renders it impracticable for the customer to refuse consent to the use of his personal data for purposes unrelated to the services to be provided to the customer.

3.7.3 Case study – disclosing account records to police for disciplinary investigation

The complaint

A bank received a letter from the Police requesting account information of the complainant, a police officer. The letter stated: "*Officers of [the Police] are currently conducting a disciplinary investigation, which involves the [complainant's] financial status. In order to assist our investigation, I would be grateful if you could furnish the Account Records of [the complainant] from … to …. I certify that the requested information is required for the purpose of disciplinary enquiry, which is exempted under section 58(1)(d) and (2) of the Personal Data (Privacy) Ordinance.*"

Without asking for any further information about the investigation from the Police, the bank released the requested account information which contained the complainant's personal data to the Police.

Outcome

The Commissioner found that the original collection purpose of the data by the bank did not cover such disclosure to the Police, nor was it within the complainant's reasonable expectation that his personal data would be so used by the bank.

During investigation, the Police explained to the Commissioner that the requested account information was relevant to their disciplinary investigation against the complainant for suspected serious pecuniary embarrassment which may involve a breach of paragraph 8, Chapter 6 (Conduct and Discipline) of the Police General Orders. However, based on information available, there was insufficient information to satisfy the Commissioner that the complainant's situation was sufficiently serious to constitute "seriously improper conduct" referred to in section 58(1)(d) of the Ordinance. Moreover, the Commissioner failed to see how the bank could rely simply on the Police's letter to satisfy itself that the disclosure fell within section 58(1)(d) and to hold the belief that failure to disclose the requested data would have been likely to prejudice the Police's investigation.

Accordingly, the Commissioner found that the bank had contravened DPP3 for disclosing the data to the Police.

[12] By virtue of section 51 of the Ordinance, the mere fact that the disclosure is permitted pursuant to an exemption does not in itself confer any right nor impose any requirement on any person to disclose or compel the disclosure of the data. According to case law (see High Court Case No. HCMP2487/2005), the burden rests squarely on the person who seeks to invoke an exemption to show that all the relevant prerequisites are met, which must be supported by cogent evidence.

3.8 Handling of personal data in debt collection

3.8.1 Inform customer of the possible use of his personal data for debt collection

In general, a bank may use a customer's personal data for recovery of any debts due and owing from the customer who is in default of payment, including transfer of the data to debt collectors for debt collection purposes. Such use is, in normal circumstances, directly related to the original purpose of data collection. As required by DPP1(3), the bank shall inform the customer before or at the time of collection of the data from him of such use of his data and the possible transferees of the data, for example debt collection agents. It is good practice for banks to also inform customers of their policies and practices in relation to debt collection, including, for example, when and what customer data would be passed to debt collection agents, the typical controls imposed by the bank over its debt collection agents in relation to the safe handling of such data, etc.

3.8.2 Avoid disclosing data to unrelated parties

Information showing the financial problems of a customer such as default in payment is commonly recognised as sensitive data, and should therefore be handled with extra care. Such data should not be disclosed to any third party unless there is a real need to do so.

In the course of debt collection, a bank or its agent may have to contact the customer (or his authorised representative, if applicable) ("debtor") through mail or telephone call. When sending a demand letter to the debtor, care should be taken to ensure that the address used is accurate, which is required by DPP2(1). In addition, the letter should be put in a sealed envelope marked "*private and confidential*" or "*to be opened by addressee only*" or words to like effect to ensure data security in compliance with DPP4. These are to avoid the debtor's personal data inside being accessed by unintended recipients. If a call is made to the debtor but answered by somebody else, for example his family member or a colleague, no information about the debt should be divulged in the call.

Unless authorised by law, public display of a debtor's personal data, for example by posting a demand notice on the front door of the debtor's residence, should not be made, as so doing is likely in breach of DPP3.

3.8.3 Engagement of debt collection agent

A bank may engage a debt collection agent to collect a debt from a customer on its behalf. According to section 65(2) of the Ordinance, any act done by the agent with the authority of the bank in the course of collecting the debt would be treated as done by the bank. When personal data is transferred by the bank to the agent, the bank is not thereby exonerated of its duty, as principal, to ensure compliance with the requirements under the Ordinance by the agent. The bank should therefore exercise proper care and diligence to monitor and regulate the conduct of its agent in the proper handling of the customer's data passed to it in the debt collection process.

In engaging debt collection agents, banks are advised to take note of the recommendations set out in section 2.6.3 above. In particular, banks need to take measures to prevent the agent from contravening the requirements under the Ordinance in the course of debt recovery, for example disclosing the personal data of the debtor, his referees or family members to unrelated third party by means of, say, public display or mail to neighbours, etc. It should be noted that reliance on simple agreement requiring the agent to abide by the laws of Hong Kong including the

Ordinance will not exonerate the banks from liability under the Ordinance[13]. Banks should put in place practical guidelines or limitations in respect of the collection and handling of personal data by the agent.

Moreover, banks should only disclose to the agent such information which is necessary for it to carry out its work. Excessive disclosure may constitute a breach of DPP3. In this connection, AIs should note that as provided in sections 9.4 and 38.4 of the ***Code of Banking Practice*** issued jointly by the Hong Kong Association of Banks and the DTC Association and endorsed by HKMA ("**the Banking Code**"), they should not pass information about referees (or third parties other than debtors or guarantors) to their debt collection agencies. If a referee is to be approached for information to help locate a debtor or guarantor, this should be done, without causing nuisance to the referee, by staff of the AI.

In addition, sections 2.16 to 2.18 of the CCD Code provide for matters relating to the provision of consumer credit data by credit providers to debt collection agents. Under section 2.16, a credit provider should by contractual means require its debt collection agent to follow such conduct as stipulated by the Banking Code in relation to debt collection activities and should satisfy itself of the reputation of the agent that the agent will so follow. Section 2.17 restricts the kinds of debtor's data that may be disclosed to the agent to identification and location data, the nature of the credit, and the amount to be recovered and goods to be repossessed. Lastly, section 2.18 requires the credit provider to check the accuracy of the data before providing it to the agent.

3.8.4 Case study

(1) Disclosure of debtor's default in payment to third party

The complaint

A debt collection agent appointed by a bank made a dunning call to a school where the debtor was employed as a teacher. According to the call recipient who was the janitor of the school, the caller stated that he was calling to collect debt from the debtor and asked the janitor to urge the debtor to return call.

Outcome

The Commissioner was of the view that by stating the purpose of the call as recovery of debt, the fact that the debtor had defaulted on payment had been disclosed to a third party (i.e. the janitor in this case) and this was contrary to DPP3.

After intervention by the Commissioner, the bank issued a written guideline to its debt collection agents requiring their staff to leave only their names and contact numbers where the call recipient was not the debtor. In the event that the recipient enquires about the purpose of the call and the identity of the caller, the staff member should simply mention "for personal matters" and disclose the name of the caller's organisation only.

[13] See the Commissioner's investigation report no.R10-11568 issued on 24 February 2010.

(2) Public display of personal data of debtor's relatives[14]

The complaint

A finance company passed the debtor's loan application form which contained personal data of the debtor's relatives to its debt collection agent with instructions to recover the debt on its behalf. The agent posted up the relatives' personal particulars in public places in pursuit of the debt.

Outcome

The Commissioner found that the public display of the relatives' data was not within their original collection purposes, thus in breach of DPP3. The finance company being the data user and the principal had not concerned itself with the proper handling of such personal data by its agent. The finance company did not restrict, by agreement or otherwise, the disclosure of the relatives' personal data by the agent in the course of debt collection. The Commissioner therefore concluded that the acts of contravention by the agent were done within the scope of authority given to it by the finance company in the recovery of the debt and thus the finance company was held liable for having contravened DPP3 by virtue of section 65(2) of the Ordinance.

3.9 Protection of personal data collected during off-site marketing campaign

3.9.1. Handling of personal data collected off-site

Banks from time to time may organise off-site marketing activities to promote their products, for example credit card services. It is sometimes necessary to collect customers' data and copies of identity cards during the process. As the activities take place outside a bank's office, this poses real challenges to the bank as the data user in discharging its obligations under DPP4 to take all practicable steps to ensure the safe storage and secure transmission of the data so collected. In such situations, the bank should take every precaution to ensure security of the data.

In this regard, banks are advised to formulate and provide clear policies, procedures and guidelines to the marketing staff for the secure handling of the data collected off-site, which should include practicable measures to ensure that:

(1) the data is not seen by or accessible to irrelevant parties during and after the collection process;

(2) forms and documents collected ("**application documents**") must be properly logged, for example using a control sheet;

(3) the application documents are securely stored in a locked container under the custody of a designated officer;

(4) adequate security protection is provided by encryption of any such data stored in portage storage devices;

(5) specific precautionary measures are implemented to ensure secure transmission of the application documents to the bank's premises where the documents are to be stored or processed;

(6) the staff are prohibited from bringing home any of the application documents;

(7) a designated officer is appointed to oversee security of the application documents.

[14] See footnote 13.

3.9.2. Case study – loss of application documents[15]

The complaint

A bank conducted a marketing campaign in a bookshop to solicit credit card applications on a Saturday. At the end of the campaign, the bank employee put all the application forms together with applicants' identity card copies in a briefcase and carried them home before returning to office the next working day. Unfortunately, the employee left the briefcase on a public light bus and lost all the documents.

Outcome

Investigation revealed that the bank did not provide adequate guidelines to its staff in relation to the handling of personal data collected during off-site marketing campaigns. Taking into account the sensitivity of the data collected and the harm that could be caused to the customers concerned as a result of the loss of data, the Commissioner found that the bank had breached DPP4.

In compliance with the Commissioner's directions, the bank implemented corresponding safeguard measures, including the transmission of the application documents to a nearby branch of the bank at the end of a marketing campaign instead of allowing its staff to bring them home.

3.10 Collection and security of personal data in e-banking environment

E-banking services bring benefits to banks as well as convenience to their customers. At the same time, there are inherent security risks in the Internet environment. In most cases, operations of e-banking would involve collection and transmission of personal data over the Internet and storage of personal data accessible through the Internet. In this connection, banks should refer to the Internet Guidance Note for detailed guidance on the collection, display and transmission of personal data through the Internet[16].

The following notes highlight some of the areas which banks should pay attention to in relation to the collection and security of personal data in the e-banking environment.

3.10.1 Collection of customers' personal data through the Internet

When a customer logs in a bank's e-banking system, the bank should, before collecting his personal data for, for example, transaction instructions, give the customer a PICS in accordance with DPP1(3). This can be done by giving an online PICS displayed in a clear and conspicuous manner, for example one accessible on the same web page or through a well signposted link. It should be easy to read and understand, and its contents must be consistent with any printed version distributed offline.

If the customer is required to fill in any online form to provide his personal data, the design of the form should follow that of the paper equivalent (if any). In particular, mandatory items and optional items to be collected should be clearly labelled.

Where cookies are used, it is good practice to explicitly state what kind of information, regardless of whether personal data is involved, is stored in the cookies. If the bank's website bars users who do not accept cookies, this should be made clear to the customer. If the customer is allowed to choose not to accept cookies for using the website, he should be provided with an option with clear information on the consequence

[15] See the Commissioner's case note no.2003C07.

[16] See also HKMA's guidance on general principles for risk management of e-banking in its ***Supervisory Policy Manual, Module TM-E-1 entitled "Supervision of E-banking"***.

(if any) of opting out. For details on the recommended best practices regarding the use of cookies, please refer to the Internet Guidance Note and the Commissioner's ***Information Leaflet: "Online Behavioural Tracking"***.

As good practice, the customer should also be informed of the specific security measures that are applied to online transmission of his personal data. It is also recommended that a link to the bank's PPS be provided to the customer for easy access.

3.10.2 Security of customers' personal data transmitted or accessible through the Internet

Security on the Internet is a challenge, so special care is needed to protect customers' personal data transmitted or accessible through the Internet. Banks should make reference to the Internet Guidance Note which contains discussion on the security measures that banks may take to protect such personal data[17].

3.10.3 Case study – unauthorised access to the account data of other customers through e-banking

The complaint

A customer logged in a bank's newly enhanced e-banking system and discovered that he could access account data of other customers including the account number, account balance and stock holding information.

Outcome

Investigation by the Commissioner revealed that the incident was caused by data conversion problems, mistakes by the bank's IT staff and failure of the system testing during the enhancement process. The bank was found in breach of DPP4 for failing to protect customers' personal data in the e-banking environment. Subsequently, the bank implemented improvement measures to prevent recurrence of the contravention.

3.11 Handling of data access request from customers

The ***Guidance Note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users*** ("**the DAR Guidance Note**") issued by the Commissioner gives general guidance to data users on the proper handling of data access request ("**DAR**") and the charge of DAR fees. Further, the "Important Notice to Data User" contained in the ***Data Access Request Form (Form OPS003)*** prescribed by the Commissioner under the Ordinance provides explanatory notes on the handling of DARs. In processing DARs from customers, banks should make reference to the above documents for more detailed guidance. The following notes and case study highlight important points that banks should take note of.

3.11.1 Customer and a relevant person can make a request

An individual may make a request to a data user 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" or DAR, may be made by the individual himself or by a "relevant person" on his behalf. "Relevant person", for the purpose of a DAR, in addition to the relevant person mentioned in section 2.3.3 above, also includes a person authorised in writing by the individual to make a DAR on his behalf.

Accordingly, a customer, or his "relevant person", may make a DAR to a bank for a copy of his personal data contained in, for example, his mortgage account records held by the bank.

[17] See also HKMA's ***Supervisory Policy Manual, Module TM-E-1 entitled "Supervision of E-banking"***.

3.11.2 Comply with customer's request within 40 days

Subject to certain exceptions and conditions, the bank is required by section 19(1) of the Ordinance to comply with the customer's DAR within 40 calendar days after receiving the same by either writing to the requestor that it holds the requested data and supplying a copy of it, or writing to the requestor that it does not hold the data, as the case may be.

3.11.3 Fee for complying with the request

Under section 28 of the Ordinance, the bank may charge a fee for complying with the customer's DAR provided that the fee is not "excessive". The fee should be confined to cover only those costs which are directly related to and necessary for complying with the DAR[18].

In general, the bank may charge direct labour costs and necessary expenses (for example copying charges and postage) incurred for locating, retrieving and reproducing the requested data for complying with the DAR. Redaction cost may be charged provided that it is for removing names and other identifying particulars of individuals other than the customer from the copy data to be supplied to the requestor. Redaction cost for removing personal data exempted from the DAR requirements may not be charged. Likewise, costs for seeking legal advice and office overheads should not be included in the DAR fee.

It may be more administratively convenient for a bank to impose a flat-rate fee for complying with customers' DARs so long as the flat-rate fee is lower than the direct and necessary costs for complying with a DAR. Banks charging flat-rate fees should therefore remain vigilant that the fee charged in a particular case (for example a simple and straightforward case where a single page of data is supplied to the requestor) must not be excessive.

3.11.4 Case study – failure to supply requested data within time

The complaint

A customer made a DAR to the bank for "*all records held by [the bank] in connection with [his account] excluding statements of accounts, transaction confirmations and contract notes*" spanning over a period of eight years. In response, the bank wrote to the customer seeking clarification on the scope of the requested data ("the 1st clarification"). The customer replied to the bank and clarified the scope of data as "*all contractual agreements or other documents signed by him, all written records of communications (including file notes of conversations and meetings) between [the bank] and him, and all risk profiles, records of investment objectives and other internal memoranda or file notes prepared by [the bank] in relation to the account*". The bank was not satisfied and requested further clarification of the scope from the customer ("the 2nd clarification") but to no avail. The bank subsequently provided certain documents to the customer. As the customer considered that some requested data was still lacking, he made a complaint to the Commissioner.

Outcome

After the Commissioner's intervention, the bank supplied a second batch of documents to the customer. The customer was satisfied that the two batches of documents supplied to him accorded with his DAR.

[18] See the DAR Guidance Note.

According to decisions of the Administrative Appeals Board, where the type and scope of data to which a DAR relates are obviously so unclear that further clarification is required before it can be complied with, the DAR may be regarded as invalid or ineffective, and the time to comply with the DAR does not start to run until the type and scope of the requested data are clarified[19].

The Commissioner considered that the customer's reply to the 1st clarification had adequately clarified the scope of the requested data. It was sufficiently clear to enable the bank to locate the requested data, hence the statutory time limit of 40 days for complying with the DAR started to run from the day of the customer's reply to the 1st clarification even though the bank further sought the 2nd clarification. Whether the scope of the requested data was too wide or unclear hence rendering the DAR invalid or ineffective would be determined objectively instead of solely by reference to the bank's attempt to seek further clarification. As the bank provided the two batches of documents to the customer far beyond 40 days after the customer's reply to the 1st clarification, it was in breach of section 19(1) of the Ordinance for failing to comply with the DAR within time.

3.12 Make privacy policies and practices generally available

3.12.1 Formulate a privacy policy statement

As required by DPP5, a bank shall take all practicable steps to ensure that its personal data privacy policies and practices, the kind of personal data it holds and their main purposes of use are made available to the general public. This can be done by drawing up a notice, usually called a PPS and making it generally available.

It is suggested that the PPS may cover the following information, where appropriate:

(1) a general statement of policy which expresses the bank's overall commitment to protecting the personal data privacy of the individuals who provide information about themselves to it. For example: *"We pledge to meet fully, and where possible exceed, internationally recognised standards of privacy protection in relation to personal data, and comply strictly with all the requirements under the Personal Data (Privacy) Ordinance. In doing so, we will ensure compliance by our staff with the policies and practices set out in this Statement and the strictest standards of security and confidentiality."*;

(2) the types of personal data collected and held by the bank;

(3) the main purposes of use of each type of data;

(4) the measures adopted by the bank to ensure the accuracy of personal data held by it;

(5) the personal data retention policy;

(6) the disclosure policy and practices in relation to the disclosure and transfer of personal data to third parties, whether within or outside Hong Kong, and the classes of possible transferees of the data;

(7) the policies and practices in relation to direct marketing, off-site marketing activities, e-banking, debt collection, outsourcing personal data processing, intra-group sharing of personal data, data matching, employee monitoring, etc.;

[19] See Administrative Appeal Nos. 17/2004 and 16/2008.

(8) the measures adopted by the bank to ensure security of the personal data held by it;

(9) the policy and practices in the handling of data access and correction requests;

(10) contact details for making enquiries about the bank's privacy policies and practices.

The privacy policies and practices contained in the PPS should cover all personal data that would be collected and held by the bank, including personal data of customers, staff, agents, business partners, etc.

3.12.2 Make the statement available to public

According to DPP5, banks must take all practicable steps to ensure that anyone, whether customers or non-customers, can have access to their privacy policies and practices. A bank may make available its PPS to the public by posting it on its website accessible or downloadable through a link in its home page and other pages where personal data are collected. The link should be clearly labelled, for example: "*Your Privacy*" or "*Privacy Policy Statement*". In addition, the bank should also prepare a paper form PPS to be provided to anyone who asks for it at the bank's headquarters and branches.

4. CONCLUDING NOTE

Banks engaging in the collection, holding, processing and use of vast amounts of customer data need to have a corporate-wide privacy strategy which applies in all their business processes and operational procedures. It is important that they manage customers' personal data properly throughout its entire life cycle, from collection to disposal and also with due regard to data integrity, use, security and access. This demands establishment and maintenance of robust privacy and risk management programmes with support and commitment from top management. Privacy-assuring banks will enjoy enhanced customer trust and loyalty, thus creating a win-win-win for the customers, their businesses and the banking industry as a whole.

Office of the Privacy Commissioner for Personal Data, Hong Kong
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