Inspection Report

published under Section 48(1) of the
Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong

Personal Data System of

An Estate Agency in Hong Kong

Report Number: R17-2201
18 December 2017

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data System of An Estate Agency in Hong Kong

This inspection report is published by the Privacy Commissioner for Personal Data, Hong Kong, pursuant to section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong in relation to an estate agency in the discharge of his powers and duties under section 48 of the Ordinance.

Section 36 of the Ordinance provides that:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "**personal data system**" is defined in **section 2(1)** of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*."

Section 48 of the Ordinance provides that:-

"*(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit.

……

(3) Subject to subsection (4), a report published under subsection (1)… shall be so framed as to prevent the identity of any individual being ascertained from it.

(4) Subsection (3) shall not apply to any individual who is-

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
18 December 2017

Inspection Report
published under Section 48(1) of the Personal Data (Privacy) Ordinance Chapter 486, Laws of Hong Kong

Personal Data System of an Estate Agency in Hong Kong

Executive Summary

Background

1. With the aim of raising the industry's awareness of the importance of personal data privacy, the Privacy Commissioner for Personal Data, Hong Kong (the **Commissioner**), jointly organised a campaign[1] with the Estate Agents Authority in 2008 and subsequently jointly published a booklet[2] explaining the practical skills in protecting customers' personal data.

2. Noting that the property market appeared to continue to boom and the total home sales volume was expected to rise, the Commissioner considered that it would be in the public interest to review the industry's regime in data privacy protection. The Commissioner therefore carried out an inspection (the **Inspection**) of the personal data system of a leading estate agency (the **Agency**), pursuant to section 36 of the Personal Data (Privacy) Ordinance (the **Ordinance**), Chapter 486 of the Laws of Hong Kong.

3. With a view to identifying good practices or inadequacies from the perspective of data privacy protection, the entire life cycle of the personal data involved in the Agency's personal data system, including its privacy policy, was examined. The Commissioner expected that the findings and recommendations made after the Inspection would also set a benchmark for the industry in ensuring compliance with the requirements under the Ordinance and the Data Protection Principles (**DPP**) in Schedule 1 to the Ordinance.

[1] The Personal Data Privacy Campaign for Estate Agency Trade
[2] Entitled "*Proper Handling of Customers' Personal Data by Estate Agents*", published in May 2009

Findings and Recommendations

4. Personal data protection could not be managed effectively if an organisation treats it merely as a legal compliance issue. Instead, organisations should embrace personal data protection as part of their corporate governance responsibilities and apply them as a business imperative, starting from the board room.

5. The Commissioner is mindful that customers' personal data has to be collected as required by the Estate Agents Practice (General Duties and Hong Kong Residential Properties) Regulation (Cap 511C) (the **Regulation**) of the Laws of Hong Kong. The findings after the Inspection showed that the Agency did make reasonably good efforts generally to ensure proper management of customers' data. In particular, the Commissioner was satisfied that the Agency had top management commitment to data privacy protection by designating a senior management officer to oversee and monitor the compliance of the personal data system. On the technical side, the Commissioner appreciated that the Agency prudently segmented the authorities and controlled the access rights of its database systems on a need-to-know basis, which would minimise the risk of unauthorised access or leakage of customers' data.

6. Practically, responsible organisations should formulate and maintain a comprehensive privacy management programme[3], which serves as a strategic framework to assist them in building a robust privacy infrastructure supported by an effective ongoing review and monitoring process to facilitate its compliance with the requirements under the Ordinance, covering the entire business practices, operational processes, product and service design, physical architectures and network infrastructure.

7. After the Inspection, the Commissioner noted that the Agency had attempted to devote its efforts in privacy management in accordance with its business nature and operation mode. No material deficiencies were found on the part of the Agency in privacy protection matters although some room for improvement was identified. The Commissioner was appreciative of the

[3] The Commissioner published a guide entitled "*Privacy Management Programme: A Best Practice Guide*" in February 2014, which outlined the good approaches for developing a sound privacy management programme.

general operation and life cycle of customers' personal data in the estate agency industry and highly recommended estate agencies should develop their own privacy management programme, which would not only effectively manage the customers' personal data, but also facilitate the agencies' compliance with the requirements under the Ordinance, build trust with customers and enhance their reputation as well as goodwill. Based on the elements of a comprehensive privacy management programme, the Commissioner also identified areas for improvement generally applicable to the industry and made the following major recommendations, which should also serve as a guide to compliance or examples of the best practices for all service providers within the industry:-

(1) Management Commitment and Governance Structure

The top management commitment of the Agency is highly appreciated, setting a role model for the industry to integrate the idea of data privacy protection into the organisation's governance by designating a data protection officer from top management to oversee the privacy management programme and data privacy related issues.

(2) Comprehensive Privacy Policies

Master privacy protection policies should be put in place to incorporate personal data protection into every major operation of an estate agency, for which regular review and update should be devised and carried out.

Policies should govern the following areas:-

(i) the manner of collection of minimum personal data by individual estate agents;
(ii) the standard retention period of documents and records containing personal data;
(iii) the ways the personal data is destroyed when the retention period expires;

(iv) the standards and requirements on the administrative measures as well as IT security to safeguard documents and records containing personal data; and

(v) the requirements and operational procedures of handling direct marketing activities and opt-out requests received.

(3) Controls and Ongoing Assessment

In order to monitor the compliance with the privacy policies, a regular and systemic compliance audit system should be devised and ongoing assessment be conducted.

(4) Data Breach Reporting Mechanism

Data breach reporting mechanism is one of the tools to effectively control the compliance with the privacy management programme. Estate agencies are advised to develop a data breach reporting mechanism with relevant guidelines governing the process of handling and reporting of data breach incidents.

(5) Handling of Vendors' and Purchasers' Personal Data

Personal data system would never operate effectively and efficiently if an organisation is not in control of the data. Accordingly, the risk of misuse or leakage of personal data would be anticipated. Practical guidance should be developed to request individual estate agents to submit all vendors' and purchasers' personal data collected or handled by them.

(6) Governance in Technical Aspect

Organisations heavily rely on information system to process business transactions and maintain relevant records and databases. Therefore, maintaining a healthy IT system free from cyber-attack is as crucial as other physical security measures. Estate agencies should designate personnel from top management to

oversee and measure the IT security, devise and formulate specific IT security policies based on their business models.

(7) Training and Education

Without a privacy-respectful culture, privacy protection policies would not be effective and efficient. Estate agencies should adopt a proactive approach in promoting compliance with personal data protection principles and in cultivating a respectful culture of data protection amongst staff members by regular training and education.

Introduction

Reasons for the Inspection

1.1 In Hong Kong, it has been reported that despite the implementation of further stamp duty policies and a new round of measures regarding property mortgage loans, the property market continues to boom and the total home sales volume is expected to rise from 55,000 in 2016 to 65,000 in 2017[4].

1.2 According to the Regulation, anyone who intends to purchase, sell or lease a property through an estate agent is required to complete the prescribed forms and provide his name, contact information and Hong Kong Identity Card (**HKID Card**) number to the estate agent. There are approximately 37,000 estate agent licences held by individuals in Hong Kong[5].

1.3 Given the vast volume and broad range of personal data (including sensitive data) handled by estate agents, the Commissioner considered that it would be in the public interest to carry out an inspection of the personal data system of an estate agency, pursuant to section 36 of the Ordinance.

[4] Source: http://www.rvd.gov.hk/en/property_market_statistics/index.html
[5] Source: https://www.eaa.org.hk/en-us/Information-Centre/Key-Figures/Licensee-Population

Inspection

Business Model of Estate Agencies

2.1 The Agency was selected in the Inspection also for the purpose of assisting the Commissioner in making recommendations to this class of data users in relation to the collection, holding, processing and use of personal data so as to promote compliance with the provisions of the Ordinance.

2.2 The Agency, similar to other estate agencies, provided estate agency services in the sale, purchase and lease of residential properties and car parking spaces through the channels of branches and websites. Among those, sale and purchase of properties constituted its core business.

Scope of the Inspection

2.3 The Inspection Team (the **Team**) examined the Agency's handling of personal data of customers from data collection to data disposal, with a view to identifying good practices or inadequacies from the perspective of data privacy protection during the entire life cycle of the personal data involved. The personal data cycle of the lease, sale and purchase of a residential property was chosen for detailed examination in the Inspection. Due recommendations relating to the promotion of compliance with the requirements under the Ordinance and the DPP 1 to 6 would be made.

2.4 DPP 1 to 6 cover the collection, accuracy, retention, use, security, transparency and access to personal data. The Agency's compliance with the direct marketing regulations under Part 6A of the Ordinance was also examined.

2.5 The six DPP and the direct marking regulations under sections 35B to 35H of the Ordinance are respectively reproduced at Annexes 1 and 2 for easy reference.

Methodology

2.6 The Inspection consisted of five major types of review work:-

Mystery visits

2.7 Mystery visits were conducted at the Agency's branches for the purposes of having a thorough understanding of the workflow and performance of individual estate agents, in particular their ways of handling personal data in their daily routines.

Policy review

2.8 A detailed and comprehensive policy on personal data handling is essential for ensuring a good and uniform practice. The Team examined the Agency's personal data privacy policy as documented in its policies, guidelines, notices, forms, and training materials.

Site inspections

2.9 Site inspections were conducted at the head office, selected branches, data centres and a storehouse of the Agency. These site inspections enabled the Team to (i) inspect the physical layout and security measures of the premises where customers' personal data was collected, processed and stored; (ii) inspect equipment and systems used for the collection, processing and storage of personal data of customers; and (iii) examine physical paper and electronic records retained in the premises and computer systems.

Walkthrough demonstration

2.10 With the aim of understanding what and how personal data was collected from customers and used, the Agency was asked to demonstrate the processes of purchasing and selling a property, updating an opt-out request, handling a customer's enquiry, etc. during site inspections.

Interviews and Enquiries

2.11 The Team made verbal and written enquiries with the Agency's staff before, during, and after the site inspections. Verbal enquiries were made through interviews with staff members ranking from management to operational levels at its head office and branches during the site inspections. These enquiries enabled the Team to understand how the staff members handled personal data, their familiarity with internal policies and guidelines relating to personal data privacy, and the training they provided and received.

2.12 The information sought through written enquiries assisted the Team in understanding the operation of the Agency's personal data system, reconciling the documentary evidence obtained with our observations at the site inspections and identifying any cause for concern.

Personal Data System and Data Flow

The Personal Data System

3.1 The personal data system examined at the Inspection not only covered the automated system used for processing personal data, but also the systematic operation of different departments and the relevant staff in the collection, holding, processing or use of personal data of the customers.

3.2 Customers' personal data was processed and handled through database systems, staff members at branches and head office, and document disposal contractors.

3.3 The table below lists the kinds of customers' personal data that was contained in the Agency's personal data system:-

Kinds of personal data	**Examples**
Name and personal identifier	● Name ● HKID Card or passport number ● HKID Card or passport copy
Contact information	● Correspondence address ● Contact telephone number ● Email address ● Fax number
Financial information	● Credit card number ● Cheque number
Recordings	● Audio record of telephone conversation ● CCTV record at branch offices

An Overview of a Customer's Personal Data Flow

3.4 It was obvious that the majority of personal data that an estate agency held was collected from customers who sold, purchased or leased residential properties. "Vendor" in this Report refers to a customer who intends to sell/ lease a residential property. "Purchaser" refers to a customer who intends to buy/rent a residential property.

Collection

3.5 A typical customer's personal data flow starts with the data collection, which may occur at branches, through phone calls and the Agency's websites. HKID Card number and/or a copy thereof, corresponding address and financial information would additionally be collected by an estate agent on the spot.

(i) At a branch

Paper records of Vendor's and Purchaser's personal data

3.6 It is provided under the Regulation[6] that an estate agent shall enter an estate agency agreement with a customer prior to advertising the property for sale/lease for the Vendor or arranging an inspection of a residential property for the Purchaser. In this regard, when a customer intended to sell or purchase or lease a residential property at a branch, his name, contact information and HKID Card number would be collected by completing and signing an Estate Agency Agreement for Sale/Purchase of Residential Properties in Hong Kong or an Estate Agency Agreement for Leasing of Residential Properties in Hong Kong (collectively the **Prescribed Form**).

3.7 For the purpose of avoiding fraud or misrepresentation of the identity of a Vendor, the Agency also collected the Vendor's HKID Card copy[7] to ensure that his name in the Preliminary Sale & Purchase Agreement of a residential property would be the same as the property owner's.

[6] Section 6
[7] Section 13(3)

Electronic records of a Vendor's personal data

3.8 Upon the receipt of the signed Prescribed Form from a Vendor, the estate agent entered and updated the Vendor's name, contact information and the sales instruction (e.g. selling price of the property) in the database systems.

Electronic records of a Purchaser's personal data

3.9 Unlike the record of a Vendor, a Purchaser's personal data including his contact information and purchasing preference (e.g. district of a property) would be a valuable asset to an estate agent. It was an understanding to the Team that most of the agents would not enter the Purchaser's personal data in the database systems so as to safeguard this data from being accessed by other estate agents.

(ii) Through phone calls

3.10 A customer could express his intention to sell or purchase or lease a residential property by calling a branch or an individual estate agent and providing his name and contact information. However, a customer would still be required to visit the branch to sign the Prescribed Form before the agent advertised a property or arranged an inspection of a property for the customer.

(iii) Through the Agency's website

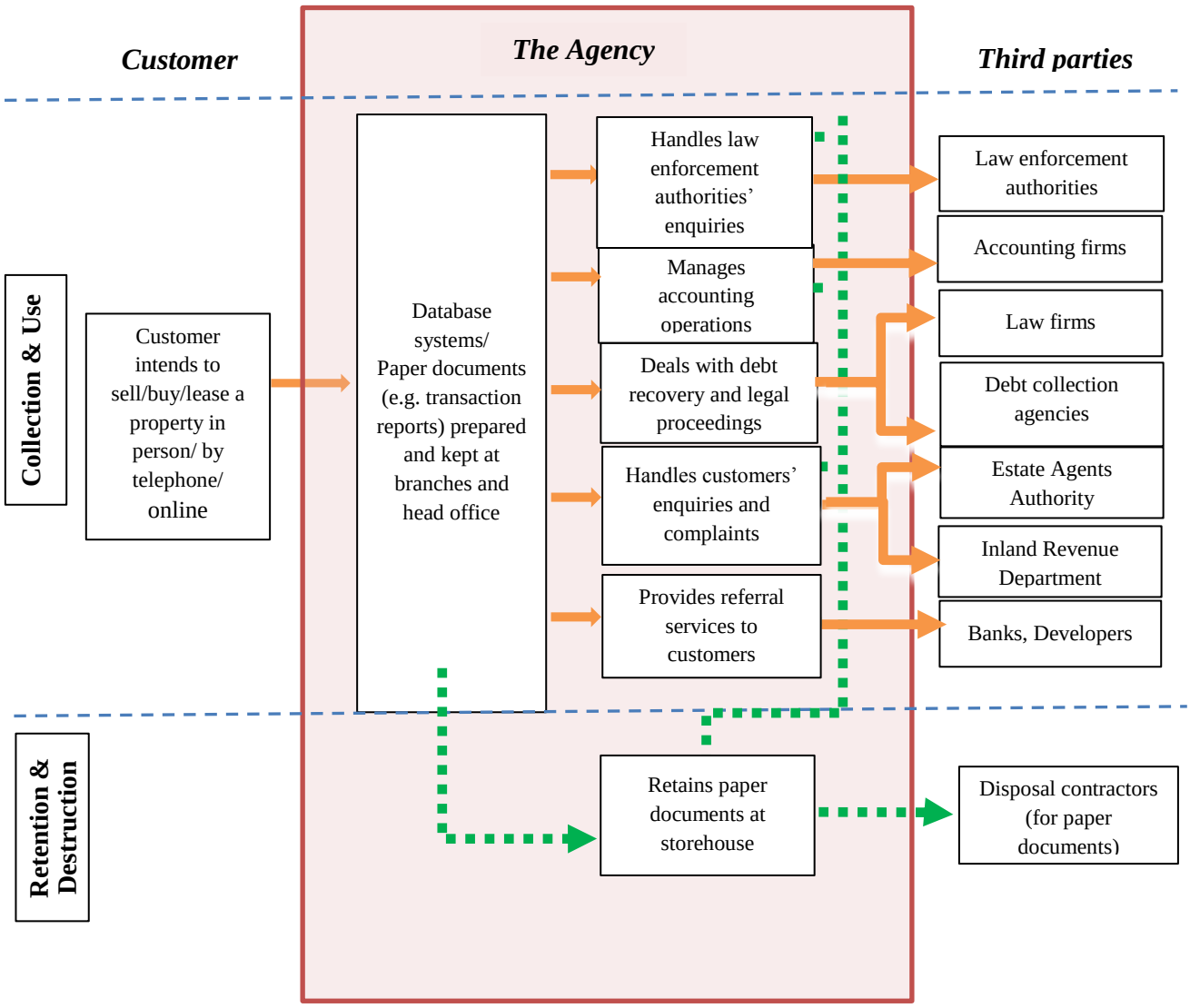
3.11 Similar to the collection of personal data through phone calls, a customer could submit his name and contact information through website to express his intention to sell or purchase or lease a residential property. Once the customer submitted his personal data for an appointment, a notification would be sent to the respective estate agent who would subsequently contact the customer inviting him to pay a visit to the branch and complete the Prescribed Form.

Use

3.12 A customer's personal data was used by the Agency in the course of providing estate agency services and making subsequent marketing activities. Furthermore, the Agency also used the personal data to:

(a) handle law enforcement authorities' enquiries;
(b) manage accounting operations;
(c) deal with debt recovery and legal proceedings;
(d) handle customers' enquiries and complaints; and
(e) provide referral services to customers.

3.13 The flow of a customer's personal data is illustrated as follows:



Retention

Paper records

3.14 Although there was no written policy setting out the retention period of documents containing customers' personal data, it was the general practice of the Agency that such paper records (e.g. signed Prescribed Forms, Preliminary Sale & Purchase Agreements, etc.) would be retained for at least five years and up to seven years. At branches, paper records containing personal data were

filed and stored in cabinets at restricted area behind the service desks or in a storeroom. At head office, paper records were stored in steel cabinets.

Electronic records

3.15 There was no retention policy governing electronic records of customers' personal data. Files containing personal data were stored in the individual computer of the staff at head office or in the computer shared by the agents at branches. System data was backed up to the server, the network attached storage and digital linear tape on a regular basis.

Destruction

Paper records

3.16 It was the Agency's policy that, when the cabinets at the head office or branches ran out of space, staff would request courier service, plastic boxes and labels from the head office for transporting the paper records to a storehouse. According to the disposal date marked on the label, responsible staff arranged the document disposal contractors to dispose of the paper records.

Electronic records

3.17 There was no policy in relation to the purging of customers' personal data. For working files containing customers' personal data that were saved in a staff member's own computer, he would be responsible for the deletion himself. On the other hand, before the disposal of an IT equipment, the hard drives would be removed from the servers/ workstations before the data was erased permanently by using data wiping software.

Findings and Recommendations

Preliminaries

4.1 Findings and recommendations made in this Report are based on the information provided by the Agency and the Team's on-site observations, which may not be exhaustive. They should be regarded only as a reflection of the compliance level of the matters at the Inspection.

Overview of Personal Data Protection Measures

4.2 Personal data protection could not be managed effectively if an organisation treats it merely as a legal compliance issue. Instead, every organisation should embrace personal data protection as part of its corporate governance responsibilities and apply them as a business imperative, starting from the board room.

I. Management Commitment and Governance Structure

4.3 The Agency assigned a director to oversee privacy matters. The department under his supervision was responsible to handle, among others, law enforcement authorities' enquiries, including the matters related to personal data protection. The Commissioner appreciated that the Agency had taken the privacy matters into account in its business operation and would encourage other estate agencies to demonstrate the same organisational commitment.

Recommendation

1. The top management commitment of the Agency is highly appreciated, setting a role model for the industry to integrate the idea of data privacy protection into the organisation's governance by designating a data protection officer from top management to oversee the privacy management programme and data privacy related issues.

II. Comprehensive Privacy Policies

4.4 The Agency laid down certain practical guidelines relating to the collection of personal data and the use of personal data in direct marketing in the form of internal notices, which were issued or updated before or in 2012. Those notices appeared to be made in a piecemeal fashion and there was a lack of a regular systematic updating and reviewing process. The Commissioner advises that when estate agencies provide guidance to their staff members in relation to personal data privacy issues, they should consider establishing a comprehensive and integrated policy, guidelines and procedures.

(i) The manner of collection of personal data by individual estate agents

4.5 The relationship between the Agency and its customer starts when the customer contacts the Agency (or its individual estate agents) stating his intention to sell, purchase or lease a property. The Team acknowledged that the Agency had devised a comprehensive Privacy Policy Statement & Personal Information Collection Statement (**PICS**). The PICS was in effect displayed in the communication channels of the Agency's websites. However, customers who visited or contacted the Agency's branches or an individual estate agent in person or through telephone calls might not be notified of the PICS.

4.6 Although it was set out in an internal notice that individual estate agents were required to verbally explain the purposes of personal data collection when signing the Prescribed Form or receiving customers' calls for the purposes of selling or leasing their property, or to provide a copy of the PICS when entering into any relevant agreements[8], the Team noted that most of the individual agents failed to do so, because:-

(i) they were not aware of the requirements stated in the internal notice and had no knowledge of the PICS; and
(ii) they focused on explaining the requirements of the Regulation (e.g. the arrangement of agency appointment and commission).

[8] For example, Preliminary Sale & Purchase Agreement, and Preliminary Tenancy Agreement.

4.7 Apart from signing the Prescribed Form in the Agency's branches, it was also a normal practice that individual agents would meet up the Purchasers at the property site and sign the Prescribed Form in public area. No guidelines or procedures governing individual estate agents (or the administration staff) on how the documents should be handled securely in transit, requesting to return the Prescribed Form or other relevant documents to the office on the same day. This would pose a security risk whereby passers-by could access the personal data registered on the Prescribed Form or during the identity verification process, and the Prescribed Form might be lost in transit.

(ii) The standard retention period of documents and records containing personal data

4.8 The Team noted that the Agency delegated the authority to the individual branch or the supervising district administration team to deal with its general administration work. All branches that the Team visited stored copies of the signed Prescribed Forms, Preliminary Sale & Purchase Agreements, Transaction Records and other related materials in their filing cabinets managed by one administration staff member.

4.9 The Team also found that although most of the branches acknowledged the maximum retention period of physical documents (i.e. seven years), the primary concern of document destruction was whether there was space for storage. Documents containing personal data stored beyond the retention period were also found.

4.10 There were no written policies or guidelines governing the retention of electronic personal data either. Deletion of electronic files stored in the hard disk of individual computer workstation or the database systems was not regulated. The Team noted that the Accounts Department had never deleted the scanned copies of transaction reports and found the earliest record retained being dated 1994. During the interview, staff members of the Accounts Department replied that they were not aware that those electronic files should be deleted after a considerable period. This is an example of data retention without justification.

(iii) The ways the personal data is destroyed when the retention period expires

4.11 Destruction of documents was handled by document disposal contractors. The Agency did not enter into any formal agreements with the contractors or impose any security requirements or monitoring mechanism for disposal.

(iv) The standards and requirements on the administrative measures as well as IT security to safeguard documents and records containing personal data

4.12 Hard copies of documents containing personal data for various operational purposes were stored in steel cabinets in storerooms or locked drawers in the head office or branches. Although password to storerooms in the head office or branches was not required, the storerooms were located in the restricted area of the head office or branches to which only the staff members of the Agency were allowed to have access. Documents were kept by the individual staff in their locked drawers at the head office or branches. Owing to the limited work space, the Team observed that some paper documents were left unattended on the staff members' desks or on the ground of the office.

4.13 In some branches, the administration staff members were designated to serve several branches and were not stationed at the same office with the relevant estate agents. The administration staff members had to pay visits to the branch offices daily to collect the documents, e.g. Preliminary Sale & Purchase Agreements, from the agents for filing and preparing transaction reports. The administration staff would put the documents in an A4-sized envelope for transit purposes.

4.14 The usable area of some branch offices was limited and therefore the branch management was concerned about the layout of the office with a view to maximising the work space. This caused the monitors of some computer workstations being exposed to customers visiting the branch and hence the contents shown on the monitors could be viewed by members of the public. Further, the Team noted that recycled papers (with land search results) were

used by a branch office when submitting documents to the Accounts Department.

(v) Direct Marketing

4.15 When entering into the preliminary agreements in relation to leasing or sales and purchases, a customer was given the option to object to the use of his personal data for direct marketing. A tick-box was also provided in the interface seeking to collect a customer's personal data on the Agency's website for a customer to indicate his consent to the use of his personal data for direct marketing. The Commissioner is satisfied with the arrangement and presentation of the direct marketing consent option.

4.16 The Agency maintained an opt-out list in Microsoft Excel form for customers who indicated their refusal to receive direct marketing materials, which was administrated by the head office. On the other hand, the Vendor's refusal to receive direct marketing materials would be marked in other database systems by individual estate agents. After assessing the procedures of the management of the opt-out list, the Commissioner considers that they are practically ineffective and might not be able to show the full picture of the opt-out requests received. The contributing factors include:-

(i) individual estate agents would possess the contact list of certain customers without registering the personal data in the database systems. Opt-out requests received from those customers to the agent might not be reported; and

(ii) after updating the opt-out requests by altering the property status in the database systems, most of the individual estate agents would not report the requests to the head office for updating the opt-out list.

Recommendation

2. Master privacy protection policies should be put in place to incorporate personal data protection into every major operation of the agency, for which regular review and update should be devised and carried out.

(i) Policies should govern the following areas:-the manner of collection of minimum personal data by individual estate agents;
(ii) the standard retention period of documents and records containing personal data;
(iii) the ways the personal data is destroyed when the retention period expires;
(iv) the standards and requirements on the administrative measures as well as IT security to safeguard documents and records containing personal data; and
(v) the requirements and operational procedures of handling direct marketing activities and opt-out requests received.

III. Controls and Ongoing Assessment

4.17 The Agency relied and trusted the departments and branches to regulate their own practice of handling personal data. However, there was no process for regular and systematic monitoring or audit on the protection of personal data conducted by the Agency, e.g. no audit checks on whether obsolete documents stored in the storehouse were contained in carton boxes securely and destroyed after seven years. The Team noted that there were documents containing personal data left unattended on the floor of the storehouse. The Commissioner considers that for the purposes of ensuring the policies developed are effective in practice, systemic audit in a timely manner is essential.

Recommendation

3. Estate agencies are advised to devise a regular and systemic compliance audit system and conduct ongoing assessment to ensure that there is due compliance with the policies, guidelines and procedures governing the handling of personal data.

IV. Data Breach Reporting Mechanism

4.18 The Team noted that there were no written guidelines or procedures governing the handling process of data loss or leakage. The Commissioner considers that developing clear and detailed written guidelines and procedures would definitely expedite the response to such incidents and help take prompt remedial measures to avoid serious loss.

Recommendation

4. Estate agencies are advised to devise data breach guidelines and procedures stipulating the process of handling of data breach incidents, which should include:-

   (i) the circumstances under which a data breach incident should be reported to the responsible department or the senior management; and

   (ii) the immediate assessment and measures to be taken to contain the breach and damage.

V. Handling of Vendors' and Purchasers' Personal Data

4.19 Being an estate intermediary, the Agency handled the personal data of both the Vendor and the Purchaser. The handling manner of those two types of personal data differed in the Agency.

4.20 As stated in paragraph 3.6, a property owner (i.e. Vendor) who wished to sell or lease his property had to sign the Prescribed Form with the Agency prior to putting up any sale advertisement. The Agency would then create a property file by inputting the information collected, including the Vendor's name, contact information and details of the property for sale/ lease into the relevant database systems. The details of the property were the primary parameters of the database systems and were accessible by all individual estate agents within the designated district. This was known as a mandatory practice.

4.21 However, the Agency posed no strict governance on the registration of Purchaser's personal data into its database systems. The Team acknowledged that such registration was accessible by others (e.g. supervisors of the agent), which led to the concern that business opportunities might be lost through the registration. The Team found that as a result most of the individual estate agents kept Purchaser's personal data, particularly contact information, in his own possession without registering the same in the database systems or notifying the collection to the Agency.

4.22 The Commissioner is of the view that individual estate agents acted in the capacity of the Agency's representative to collect personal data of Purchasers. Hence, the Agency was the data user responsible for (i) the control of the collection, holding, processing or use of such data and (ii) any subsequent breach of the requirements of the Ordinance on the part of the agents[9]. Without registering the personal data of Purchaser in the database systems or being notified of the collection, the Agency would lose control of the data. This would result in the following risks (not exhaustive) which might in turn cause a contravention of the requirements of the Ordinance:-

(i) excessive collection of personal data by the individual estate agent, e.g. date of birth is not necessary for seeking suitable properties (DPP1);
(ii) failure to notify the Purchaser of the purposes of collection and use of his personal data (DPP1);
(iii) long period of retention of Purchaser's personal data without justification by the individual estate agent (DPP2);
(iv) misuse of the personal data for the agent's own purposes (DPP3); and
(v) high risk of loss of the personal data in the agent's possession without any security measures adopted (e.g. data contained in portable storage devices without password protection or encryption) (DPP4).

[9] Section 65(2) of the Ordinance provides that any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.

4.23 The Commissioner has taken into account the common practice of treating potential customers' contact information as a valuable asset of an individual agent, particularly in the commission based industry, and considered that personal data privacy right as a whole should not be undermined by individual's business interests.

Recommendation

5. Estate agencies are advised to control the collection, holding, processing or use of personal data of all customers by developing relevant practical guidance so as to request individual estate agents to input personal data of both Vendor and Purchaser into the relevant database systems.

VI. Governance in Technical Aspect

4.24 After examining the IT security system of the Agency[10], the Team appreciated that the Agency had prudently segmented the authority for using its several database systems. In one database system, only individual estate agents were authorised to access the details of the property and the associated personal data within their work district. Further, any access to the telephone number of the Vendor was logged by the system. The number of granted access per day was also limited.

4.25 However, the Commissioner considers that there is still room for improvement on IT security of the Agency. The following areas, which should be included in a formal IT security governance organisation, were not properly addressed or implemented by the Agency:-

(a) a personnel in the senior management of the IT department should have been designated with IT security policy setting, execution and review responsibility;

[10] Including the physical security of IT equipment, operational security in handling personal data, access control mechanism, vulnerability management and disposal of IT equipment.

(b) company-wide IT security policies and appropriate guidelines and procedures applicable to personal data privacy should have been made available regulating the following matters:-

(i) regular password change and complexity requirements;
(ii) encryption or protection when sending out personal data by email;
(iii) the proper use of unencrypted portable storage devices;
(iv) security patch management for operating systems and applications;
(v) disposal policy of equipment with storage capacity; and
(vi) policy of security risk assessment procedures and guidelines in system developments.

Recommendation

6. Organisations heavily rely on information system to process business transactions and maintain relevant records and databases. Therefore, maintaining a healthy IT system free from cyber-attack is as crucial as other physical security measures. Estate agencies should designate personnel from top management to oversee and measure the IT security, devise and formulate specific IT security policies based on their business models.

VII. Training and Education

4.26 During the interviews, most of the staff members were unaware of the internal notices and practical guidelines issued governing the handling of personal data. They usually acted in accordance with the local practices of the department or branch or their own practices. For example, the Team noted the following practices, during the Inspection:-

(i) individual estate agents did fully explain the purposes and use of the Prescribed Form as required by the Estate Agents Authority but failed to advise the purposes of collecting and use of the personal data;

(ii) the retention period of documents containing personal data by some of the branches was based on the available space of the filing area. Overly long retention was also detected;

(iii) staff would download data containing personal data from computer workstations to their personal unencrypted USB thumb drives and bring the data home for further processing without approval; and

(iv) documents containing personal data had been used as recycled papers.

Recommendation

7. Estate agencies are advised to circulate and re-circulate the policies, guidelines and procedures on personal data protection on a timely and regular basis, disseminating them in an effective manner so that staff members are all aware of the relevant requirements (e.g. provision of hardcopy of the policies, guidelines and procedures requires signing off, as well as provision of the same through email and Intranet for easy reference).

Estate agencies are also advised to assign a department or team to perform a proactive role in building a privacy-respectful culture and promoting compliance of personal data protection. The assigned department or team should organise the trainings and refresher trainings on personal data protection frequently and comprehensively, which should include general trainings on the policies, guidelines and procedures, and technical trainings on specific aspects in relation to data protection (e.g. use of Internet and portable storage devices under the applicable IT security policy).

Conclusion

5.1 The Commissioner notes that the Agency has attempted to devote its efforts in privacy management in accordance with its business nature and operation mode. There being room for improvement on the part of the Agency, the Inspection also serves as a good opportunity for the Commissioner to assess the personal data system and provide recommendations as set out above to the Agency for enhancing and strengthening its privacy management, which would also be of useful reference for this class of data users for the purpose of ensuring compliance with the requirements under the Ordinance.

5.2 The Commissioner always advocates the use and benefits of a privacy management programme and strongly encourages all estate agencies to adopt the programme not only to effectively manage their customers' personal data, but also facilitate their compliance with the requirements under the Ordinance, build trust with the customers and enhance their reputation as well as goodwill.

5.3 The Commissioner wishes to thank for the co-operation of the Agency's staff, which was pivotal to the Team's understanding of the data flow in the Agency and its reasons for collecting, retaining and processing of personal data. The Commissioner appreciates the assistance rendered by the Agency's staff over and above their normal duties.

5.4 The Commissioner hopes that this Report will be of value to the Agency and other estate agencies, as well as the nurturing of the culture of "protect and respect personal data privacy".

Annex 1 - Data Protection Principles

1. Principle 1 - purpose and manner of collection of personal data

(1) Personal data shall not be collected unless-

(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that-

(a) he is explicitly or implicitly informed, on or before collecting the data, of-

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed-

(i) on or before collecting the data, of-

(A) the purpose (in general or specific terms) for which the data is to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which it was collected, of-

(A) his rights to request access to and to request the correction of the data; and

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

2. Principle 2 - accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that-

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used-

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure,

that the third party-

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes.

3. Principle 3 - use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 - security of personal data

(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to-

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2)—

data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2.

5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user is or is to be used.

6. Principle 6 - access to personal data

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data-

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Annex 2 - Use of personal data in direct marketing (s.35B to s.35H of the Ordinance)

35B. Application

This Division does not apply in relation to the offering, or advertising of the availability, of—

(a) social services run, subvented or subsidized by the Social Welfare Department;

(b) health care services provided by the Hospital Authority or Department of Health; or

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

35C. Data user to take specified action before using personal data in direct marketing

(1) Subject to section 35D, a data user who intends to use a data subject's personal data in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject—

(i) that the data user intends to so use the personal data; and

(ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use;

(b) provide the data subject with the following information in relation to the intended use—

(i) the kinds of personal data to be used; and

(ii) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and, if in written form, easily readable.

(5) Subject to section 35D, a data user who uses a data subject's personal data in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(7) In any proceedings for an offence under subsection (5), the burden of proving that this section does not apply because of section 35D lies on the data user.

35D. Circumstances under which section 35C does not apply

(1) If, before the commencement date—

(a) a data subject had been explicitly informed by a data user in an easily understandable and, if informed in writing, easily readable manner of the intended use or use of the data subject's personal data in direct marketing in relation to a class of marketing subjects;

(b) the data user had so used any of the data;

(c) the data subject had not required the data user to cease to so use any of the data; and

(d) the data user had not, in relation to the use, contravened any provision of this Ordinance as in force as at the time of the use,

then section 35C does not apply in relation to the intended use or use, on or after the commencement date, of the data subject's relevant personal data, as updated from time to time, in direct marketing in relation to the class of marketing subjects.

(2) If—

(a) a data subject's personal data is provided to a data user by a person other than the data subject (***third person***); and

(b) the third person has by notice in writing to the data user—

(i) stated that sections 35J and 35K have been complied with in relation to the provision of data; and

(ii) specified the class of marketing subjects in relation to which the data may be used in direct marketing by the data user, as consented to by the data subject,

then section 35C does not apply in relation to the intended use or use by the data user of the data in direct marketing in relation to that class of marketing subjects.

(3) In this section—

commencement date (本部生效日期) means the date on which this Part comes into operation;

relevant personal data (有關個人資料), in relation to a data subject, means any personal data of the data subject over the use of which a data user had control immediately before the commencement date.

35E. Data user must not use personal data in direct marketing without data subject's consent

(1) A data user who has complied with section 35C must not use the data subject's personal data in direct marketing unless—

(a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively;

(b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming—

(i) the date of receipt of the consent;

(ii) the permitted kind of personal data; and

(iii) the permitted class of marketing subjects; and

(c) the use is consistent with the data subject's consent.

(2) For the purposes of subsection (1)(c), the use of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data; and

(b) the marketing subject in relation to which the data is used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a use of personal data either through a response channel or other means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35F. Data user must notify data subject when using personal data in direct marketing for first time

(1) A data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.

(2) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(3) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(4) In any proceedings for an offence under subsection (3), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35G. Data subject may require data user to cease to use personal data in direct marketing

(1) A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject—

(a) has received from the data user the information required to be provided in relation to the use of personal data under section 35C(2); or

(b) has earlier given consent to the data user or a third person to the use.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) A data user who contravenes subsection (3) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(6) This section does not affect the operation of section 26.

35H. Prescribed consent for using personal data in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for using any personal data of the data subject in direct marketing, the data user is to be taken to have obtained the consent if the data user has not contravened section 35C, 35E or 35G.

— END —