Data Protection & Business Facilitation Guiding Principles for Small and Medium Enterprises

Introduction

As small and medium enterprises (SME) may not have their own legal and compliance departments, they risk breaching the requirements of the Personal Data (Privacy) Ordinance (the Ordinance) arising from inadequate knowledge of the Ordinance. To help SME understand and comply with the Ordinance, the office of the Privacy Commissioner for Personal Data, Hong Kong (the PCPD) issues these Guiding Principles after launching an online tool - Self-training Module on Protection of Personal Data for SME[1], with a view to providing specific examples and practical advice to SME:

I. Collecting customers' personal data

II. Use of customers' personal data

III. Safeguarding customers' personal data

IV. Operating online businesses or services

V. Operating business outside Hong Kong

VI. Marketing of products or services

VII. Recruitment

VIII. Installing CCTV for security purpose

IX. Collecting employees' personal data for monitoring

X. Outsourcing the processing of personal data

XI. Handling data access and data correction requests

I. Collecting Customers' Personal Data

In handling customers' purchase orders and service appointments, SME may collect customers' personal data, e.g. name, address, email address and sometimes Hong Kong Identity Card (HKID Card) number or date of birth. However, the data so collected must be necessary but not excessive. SME should pay special attention to the following:

(i) Collecting HKID Card number of a customer for identification

There is a misconception that HKID Card data is the silver bullet for identity authentication. As HKID Card number is a sensitive personal data, SME, as data users, should not require customers to furnish his HKID Card number compulsorily, unless authorised by law. If SME intend to collect HKID Card number from a customer, they must comply with the *Code of Practice on the Identity Card Number and Other Personal Identifiers*[2] issued by the PCPD and consider whether there are any less privacy-intrusive alternatives to the collection of HKID Card number.

Examples of excessive collection of HKID Card number:

✘ A beauty centre requested customers, with membership cards bearing their photos, to provide HKID Card numbers in booking appointments online for identification purpose at their subsequent visits.

[1] Upon completion of the course, SME can build their own privacy plan and get a report of how their organisations are currently handling personal data with recommendations. The course can be accessed via www.pcpd.org.hk/misc/sme_kit.

[2] Please refer to paragraphs 2.1 to 2.3 of the *Code of Practice on the Identity Card Number and Other Personal Identifiers*

✔ Requesting those customers to provide their membership numbers in booking appointments online, instead of HKID Card numbers, should suffice, as they can subsequently produce their membership cards for identification purpose when they seek services at the appointed time.

✘ When a cat owner purchased cat food at a veterinary clinic, the clinic collected the cat owner's HKID Card number for the purpose of identification of the cat owner and follow-up on the health condition of the cat in future.

✔ Collecting only the cat owner's name and telephone number would achieve the identification purpose.

(ii) Collecting date of birth of a customer for providing age-specific services and birthday discounts

If SME wish to collect a customer's date of birth with a view to offering age-specific products and services to him, collection of the customer's age or age range (e.g. aged 40-50), as opposed to the specific date of birth, should suffice. In respect of providing birthday discounts, a customer's month of birth, or date and month of birth should suffice, depending on the duration of the discounts and nature of the gifts.

(iii) Providing Personal Information Collection Statement to customers

Before collecting a customer's personal data, (e.g. requesting customers to fill in membership application forms), SME should provide him with the Personal Information Collection Statement[3], informing him of the purpose for collection and the class of persons to whom the data may be transferred, and the rights of access to and correction of his personal data.

Practical Suggestions:

- Although SME are not required to give the notice in writing under the Ordinance, it is a good practice to provide customers with the information in writing in order to enhance transparency and minimise misunderstanding.
- To ensure no excessive collection of personal data, SME should specify in their application forms what personal data is necessary for provision of their services or products, and what personal data is unrelated to such provision, e.g. marital status, education level, income, etc., and customers must be clearly informed of the purpose for collection of the unrelated data and that the provision of such data is entirely voluntary.

II. Use of Customers' Personal Data

Personal data collected from a customer shall be used only for the purpose for which the data is collected or for a directly related purpose (e.g. provision of products or services), unless prescribed consent is obtained from the customer.

Examples of change of the use of personal data:

- A beauty centre sold its customers' personal data originally collected for provision of beauty services to another beauty centre for profit.
- A wedding card company arbitrarily displayed at its retail store for promotion a wedding card designed by its customer which contained the customer's personal data.

SME also need to comply with the Ordinance to avoid improper collection and disclosure of customers' personal data in providing after-sales service or handling customer complaints.

Practical Suggestions:

- For general telephone enquiries on products or services, SME should consider giving replies without collection or authentication of the enquiring customers' identity.
- If no immediate reply can be given, only minimum personal data of the enquiring customer sufficient for the handling of enquiries should be collected. In general, customers' names and telephone numbers / addresses should suffice.

[3] Please refer to the *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement* issued by the PCPD

- Procedures and internal guidelines on handling of customer complaints should be formulated, e.g. if a complainant's identity is irrelevant to the handling of the complaint, SME should avoid disclosing the complainant's identity to the party complained against or third parties.

III. Safeguarding Customers' Personal Data

In handling customers' personal data, SME are obliged to take appropriate security measures to protect the data against accidental loss or unauthorised access with reference to the sensitivity of the data and the actual circumstances. In particular, when personal data is collected during outdoor marketing activities, extra care is required in the transmission of data.

Examples of lack of safeguards for customers' personal data:

✘ A clinic lost a patient's medical record, but it could not ascertain who last handled the record and the reason for its loss.

✔ A staff member should be assigned to check if the medical records taken out have been properly returned to their original place after the clinic is closed every day. Moreover, staff members who take out medical records outside consultation hours are required to enter a proper record.

✘ An optical shop requested a customer to write his personal data on a piece of scrap paper because it had run out of registration forms. The customer later found on the back of that piece of scrap paper another customer's personal data.

✔ The optical shop should cease using scrap papers containing personal data, and formulate a policy on the use of recycled paper for the staff.

IV. Operating Online Businesses or Services

When operating online businesses or services which involve the collection, display or transmission of personal data through the Internet, SME still have to comply with the Ordinance. For example, when operating online business, a less privacy-intrusive alternative should be adopted for identity verification purpose.

Example of less privacy-intrusive measure for identity verification purpose:

✘ An online shop required a customer to provide his HKID Card number for its staff members to verify the customer's identity at the time of collection of the pre-ordered goods.

✔ The shop could, instead, provide an unique invoice number to the customer at the time of placing order and ask him to provide that number to its staff at the time of collection of the pre-ordered goods.

SME are especially reminded that security is generally vulnerable on the Internet, and special care is needed to ensure that adequate security measures are implemented to protect the personal data from unauthorised access, and such measures are updated regularly to tackle evolving security risks[4].

Practical suggestions on how to protect your website:

- Install anti-virus software, firewall and security patches, to avoid network system, server and application being attacked by virus and malware.
- Encrypt sensitive information when transmitting, processing or storing the personal data.
- Regularly adopt safe erasure methods to irreversibly delete or destroy personal data according to a pre-determined schedule.

[4] Please refer to the *Guidance for Data Users on the Collection and Use of Personal Data through the Internet* issued by the PCPD

- If a contractor is engaged to maintain the website, a reputable contractor should be selected. See also Section X below.

Practical suggestions on online cashless transaction :

- Use secure online payment services, and as far as possible, use application programming interfaces and templates provided by the official payment service providers.
- Follow closely the instructions and guidelines issued by the official payment service providers.
- Remind customers of the risks they may face in submitting personal data (especially credit card data) online.

V. Operating Business Outside Hong Kong

Many SME may operate their businesses in the mainland or overseas. As data protection laws may vary from place to place, SME should observe the local laws in respect of personal data. For example:

- Cybersecurity Law of the People's Republic of China have come into force from 1 June 2017, which requires, among others, that personal information and important data collected or generated by an operator of a critical information infrastructure during its operation in the mainland shall be stored within the territory. If transfer of the information and data out of the territory is required owing to operational needs, security assessment should be conducted pursuant to the measures prescribed by government authorities.
- The European Union General Data Protection Regulation (GDPR) will come into effect in May 2018. Corporations and organisations in Hong Kong that offer goods or services to individuals in the European Union, or monitor the behaviour of individuals in the European Union should be aware that they may be subject to the requirements of the GDPR[5].

VI. Marketing of Products or Services

(i) Direct marketing

SME often directly promote their products and services to existing or target customers through telephone, email, etc. However, before using a customer's personal data for direct marketing, SME must notify the customer of the types of personal data that will be used; the classes of goods or services that will be marketed; and a response channel through which the customer can communicate his consent to the use of his personal data in direct marketing. If the customer does not give such consent, SME should not so use his personal data.

If SME intend to transfer the personal data to a third party for the latter's use in direct marketing, SME must notify the customer of the above information and obtain the customer's written consent. Moreover, SME which receive a customer's request for cessation of using his personal data in direct marketing must comply with the request without charge. Failure to comply with any of the above requirements[6] is a criminal offence.

SME should maintain a list of customers who have indicated their wishes not to receive further marketing approaches and adopt a system to comply with such indications (e.g. the list should be updated regularly and the updates should be distributed to the relevant staff.).

(ii) Personal data obtained from public domain

In identifying target customers through accessing and obtaining personal data from public domain e.g. a public register or a public search engine, SME should note that the protection afforded by the Ordinance also applies to such public personal data. Before using personal data obtained from public domain, due regard must be given to the data user's original purposes for making the personal data available in public domain. The restrictions, if any, imposed by the data users on further use of such data and the reasonable expectation of personal data privacy of the data subjects must be observed[7].

5 The PCPD will publish an information leaflet on this subject in early 2018. The leaflet will be uploaded to its website (www.pcpd.org.hk).
6 Please refer to the *New Guidance on Direct Marketing* issued by the PCPD
7 Please refer to the *Guidance on Use of Personal Data Obtained from the Public Domain* issued by the PCPD

Examples of improper use of personal data obtained from public domain:

- ✘ A financial institution obtained the bankruptcy record of an individual from public domain and issued a letter to him at the residential address disclosed promoting the service of "discharge of bankruptcy".
- ✘ Using the personal data obtained from the Government Telephone Directory for direct marketing.

(iii) Using social networking sites and mobile apps for marketing

Promoting and providing services to existing or target customers through social networking sites and mobile apps, SME must comply with the requirements of the protection of customers' personal data[8].

Practical Suggestions:

- When organising lucky draws or quizzes on social networking sites, SME should not ask participants to provide their personal data on public message boards.
- If a mobile app developed by SME collects users' personal data (e.g. name, email address, etc.) or access the data contained in their mobile phones (e.g. user's location, mobile phone's IMEI number, etc.), it should be clearly stated in its Privacy Policy Statement what data it will access, use, transmit and share, and provide sufficient reasons for such access.

VII. Recruitment

If SME solicit personal data from job applicants in a recruitment advertisement, they must identify themselves and state the purpose for which the data is to be used[9]. SME must comply with the Ordinance in the collection, retention, use and security of personal data of job applicants and employees, just like the handling of their customers' personal data.

Examples of improper collection of personal data in recruitment:

- ✘ In a recruitment advertisement, a company solicited job applicants' personal data without identifying itself by its name. Only its email address and telephone number were provided in the advertisement. Generally, it is not sufficient for an employer to state simply its email address, telephone number or fax number and insufficient disclosure of an employer's identity may constitute unfair collection of personal data of the job applicants.
- ✘ When recruiting waiters, a restaurant demanded applicants to provide date of birth, bank account number, marital status, spouse's name and HKID Card number, as well as the name and telephone number of an emergency contact person. Before any formal establishment of an employer-employee relationship, it would not be necessary for the restaurant to collect the above personal data solely for the purpose of identifying suitable candidates.

VIII. Installing CCTV for Security Purpose

When a CCTV system with recording function is installed in a shop for security purpose, it is inevitable that images of passersby will be captured. Hence, SME are advised to assess whether or not the design and use of the CCTV system are appropriate, necessary and proportionate in the given circumstances (e.g. CCTV cameras should not be positioned in a way that exceeds the scope of monitoring), and to adopt practical measures to notify passersby that they are subject to CCTV surveillance[10].

[8] Please refer to the information leaflet on *Privacy Implications for Organisational Use of Social Networks* and the *Best Practice Guide for Mobile App Development* issued by the PCPD

[9] Please refer to the *Understanding the Code of Practice on Human Resource Management – Frequently Asked Questions about Recruitment Advertisements* issued by the PCPD

[10] Please refer to the *Guidance on CCTV Surveillance and Use of Drones* issued by the PCPD

Practical Suggestions:

- Organisations should put up conspicuous notices stating the specific purpose of surveillance at the entrance of the monitored area, as well as inside the area.
- Covert CCTV surveillance should not be used without strong or overriding justifications.
- Organisations should regularly delete CCTV footages by irreversible and safe means, unless the footages are needed for specific purpose (e.g. reporting to the Police as evidence).

IX. Collecting Employees' Personal Data for Monitoring

If SME intend to use technology for monitoring employees, they should first assess whether such monitoring is appropriate for their business[11], and if so, try to adopt less privacy-intrusive alternatives as far as possible. Moreover, SME should be entirely open about their employee monitoring policies and adopt privacy protection practices in the management of personal data obtained from employee monitoring[12] schemes.

One of the recent technologies which is commonly used in employees monitoring is fingerprint identification. Although fingerprint identification devices have become easily affordable, employers should not compulsorily collect employees' sensitive fingerprint data solely because of the declining cost of such devices.

Examples of inappropriate use of fingerprint identification system to collect employees' fingerprint data:

✘ A dessert shop collected employees' fingerprint data for attendance record.

✔ Other than collection of fingerprint data, employers should provide their employees with less privacy-intrusive options (e.g. access card).

✘ A boutique required its employees to provide fingerprint data, before accessing its showroom, for the purpose of theft prevention.

✔ In fact, ordinary door locks, digital locks and chain locks could also achieve the purpose of theft prevention without involving collection and retention of personal data. For theft tracking, installation of CCTV cameras could be more effective.

X. Outsourcing the Processing of Personal Data

SME are responsible for the acts of a data processor engaged to process personal data on their behalf. Therefore, they should 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, or to prevent unauthorised or accidental access, processing, erasure, loss or use of the data[13]. Besides, SME should also prohibit the data processor from using or disclosing the data for a purpose other than the purpose for which the personal data is entrusted to it.

Examples of organisations being liable for the acts of their outsourced contractors:

✘ A supplier was engaged by a furniture company to deliver furniture to its customer, but the supplier discarded a delivery note containing the customer's surname, telephone number and address at the lift lobby on the same floor of the customer's flat.

✔ The furniture company was liable for the leakage of the customer's personal data owing to improper handling of delivery note by its supplier. After the incident, the furniture company issued guidelines on the handling of documents containing customers' personal data to all of its suppliers and requested them to communicate the guidelines to their frontline staff.

[11] Common employee monitoring includes telephone monitoring, email monitoring, Internet monitoring and video monitoring
[12] Please refer to the *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* issued by the PCPD
[13] Please refer to the information leaflet on *Outsourcing the Processing of Personal Data to Data Processors* issued by the PCPD

✘ An employment agency engaged a repairer to fix its computer. During the data backup, the repairer negligently uploaded a folder containing the data of the employment agency's customers onto the repairer's server, and the security loophole of that repairer's server made the data accessible to the public on the Internet.

✔ The employment agency was liable for the leakage of customer's personal data by the repairer's improper handling of computer files. They should adopt contractual means to prevent unauthorised or accidental access of personal data transferred to its outsourced contractors.

XI. Handling the Data Access and Data Correction Requests

Customers or employees have the right under the Ordinance to access and correct their personal data, and SME, as data users, have to comply with the data access and correction requests made by their customers or employees. A data user is required to comply with the request within 40 calendar days. If SME do not hold the requested data, they are still required to inform the requestor in writing within the same time limit, stating the reason. If SME do not know how to handle such requests, they should seek legal advice or refer to the guidance note issued by the PCPD[14], as soon as possible, to ensure compliance with the requirements under the Ordinance.

Concluding Note

Customers and members of the public have rising expectations with regard to protection of their personal data. SME therefore need to be proactive to gain their trust. In so doing, SME will further enhance their corporate reputation, competitive advantage and potential business opportunities.

[14] For details, please refer to the *Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users* and the *Proper Handling of Data Correction Request by Data Users* issued by the PCPD

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First published in December 2017