Guidance for Mobile Service Operators

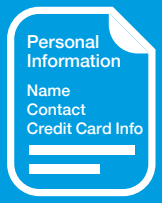
PCPD HK

PCPD.org.hk

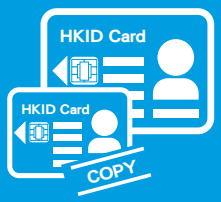
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong

Guidance for Mobile Service Operators

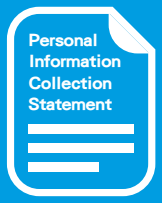
Handling Service Applications



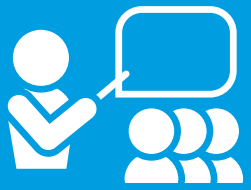
Consider carefully the necessity of collecting each item of personal data. Ensure the data collected is adequate but not excessive.



Collection of a Hong Kong Identity Card number / copy must be justified and permissible under the *Code of Practice on the Identity Card Number and other Personal Identifiers*.



Provide service applicants with a Personal Information Collection Statement stating clearly the purposes of collecting the data, the classes of persons to whom the data may be transferred, the consequences of failing to supply the data and the right of access to and correction of the data.



Provide clear policies, procedures and guidelines to the marketing staff / outsourced promoters conducting marketing campaigns outdoors to ensure the safe storage and secure transmission and handling of the personal data collected.

Audio-recording of a Conversation with Customers

Notify customers prior to the audio-recording and inform them of its purpose to avoid offending them or constituting unfair collection of personal data.

Carrying Out of Direct Marketing Activities

Notify customers and obtain their consent before using or providing their personal data in direct marketing.

Engaging Third Party Agent / Dealer

Be accountable for the acts done or practices engaged by its agents or contractors (such as IT contractors, debt collection agents or marketing agents) within the scope of the authority given to them.

Disclosure of Customers' Account Data

Obtain prescribed consent from a customer concerned if the customer's personal data is disclosed for a new purpose.

Guidance for Mobile Service Operators

Maintaining Customers' Service Accounts

Exercise due care when inputting customers' personal data into customers' database to ensure the accuracy of customers' personal data held.

When a customer requests a change of his account information, verify with the requestor that the request is from the genuine customer.

Formulate policies and practices to specify the retention period of different types of customers' personal data, and erase personal data that is no longer required for fulfilment of the collection purpose.

Ensure the addresses used to send dunning letters are accurate and the envelopes used have marked "private and confidential". Where a debt collection agent is engaged to collect overdue charges, disclose to the agent only such information necessary to carry out the action.

Measures to Protect Service Account Data

Use a password with high security level for the creation of an online account as the defaulted password, and remind customers to change it.

Restrict the access of customers' database by staff to protect the data against unauthorised or accidental access, processing or erasure.

Care must be taken in the arrangement and the design of the shop if customers' personal data is required to be processed in a public area (such as open-plan shops or service desks).

Handling of Data Access / Correction Requests

Respond to customers' data access / correction requests within 40 calendar days after receipt, by writing to the requestors that either it holds the requested data and supplying copies of them or it does not hold the data.

*For details, please refer to the content of "Guidance for Mobile Service Operators".

Guidance for Mobile Service Operators

Introduction

A mobile service operator collects, holds, processes and uses enormous amount of customers' information, which commonly includes names, contact details, identification document copies / numbers and credit card information, etc. A mobile service operator should therefore ensure that its data privacy policies and practices comply with the requirements under the Personal Data (Privacy) Ordinance (Chapter 486) (the "**Ordinance**") and the six Data Protection Principles ("**DPPs**") in Schedule 1 to the Ordinance. This Guidance Note sets out some illustrations and good practices for compliance with the Ordinance.

This Guidance Note supercedes the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**")'s *Personal Data Privacy: Guidance for Mobile Service Operators* issued in August 2000.

Handling Mobile Phone Service Applications

(i) Collection of personal data

In handling applications for mobile phone service (including mobile data service), a mobile service operator should carefully consider the necessity of collecting each item of personal data, and ensure the data collected is adequate but not excessive[1]. In general, collection of names, contact details and credit card information (if the election is to settle service bills by credit card) of service applicants should suffice.

Service applicants should be provided with a Personal Information Collection Statement ("**PICS**") stating clearly the purposes of collecting the data, the classes of persons to whom the data may be transferred, the consequences of failing to supply the data and the right of access to and correction of the data[2]. The PICS may be attached to documents that record the personal data concerned, such as a mobile service application form or service contract.

Tips:

- If a mobile service operator transfers its customers' personal data to a debt collection agency for recovery of outstanding service fees, it should have clearly stated in its PICS the potential data transfer to the debt collection agency, to effectively inform the customer at or before the time his personal data is collected for the purpose of service application. A mobile service operator should also ensure that its PICS is presented in a manner that is easily readable and understandable.

(ii) Collection of Hong Kong Identity Card number / copy

A Hong Kong Identity Card ("**HKID Card**") number is sensitive personal data, and a copy of HKID Card containing a HKID Card number is also sensitive. Collection of a HKID Card number / copy must be justified and permissible under the *Code of Practice on the Identity Card Number and other Personal Identifiers* (the "**PI Code**")[3] issued by the Commissioner.

Collection of an individual's HKID Card number may be justifiable if a mobile service operator and the individual enter into a service agreement that is

1 DPP1(1)
2 DPP1(3)
3 Paragraphs 2.1 to 2.3 and 3.1 to 3.4 of the PI Code

intended to establish or to evidence the legal rights, interests or liabilities on both parties[4].

Nevertheless, the collection of HKID Card numbers from the representatives of corporate customers (who act as contact persons, persons in charge, or persons who collect / receive the subscribed devices on their behalf) will be considered excessive as the representatives are not the subscribers themselves to the mobile services.

Tips:

- When a corporate customer subscribes for mobile services, a mobile service operator could check against the business registration and company search records to process the subscription. Upon collection of the subscribed devices (e.g. mobile phones or SIM cards), it would suffice for the mobile service operator to simply require the corporate customer's representative to show his staff card or business card for the purpose of verifying his employment identity. Presentation of an authorisation letter from the corporate customer or stamping the corporate customer's company chop on the acknowledgement of receipt would generally be considered as sufficient proof of authority.

Under paragraph 3.2.1.2 of the PI Code, a data user should not collect a copy of a HKID Card except where the use of the copy by the data user is **necessary** for any of the purposes mentioned in section 58(1) of the Ordinance (the prevention or detection of crime, etc.). The risk of fraud is rather remote if full payment for a fixed period of time has been pre-paid by a customer at the outset under his contractual relationship with his mobile service operator. In the circumstances, the mobile service operator could hardly justify the collection of an individual's HKID Card copy.

(iii) Handling of service applications off-site

When a mobile service operator conducts marketing campaigns outdoors, it should formulate and provide clear policies, procedures and guidelines to the marketing staff / outsourced promoters to ensure the safe storage and secure transmission and handling of the personal data so collected[5].

Tips:

- A mobile service operator should direct the marketing staff / outsourced promoters to deposit the personal data so collected to the nearby retail shops after work for safe custody instead of taking the data home.
- If a mobile service operator provides the marketing staff / outsourced promoters with mobile phone cameras for taking pictures of application documents (in lieu of using photocopier), it should remind the staff / promoters concerned to ensure a safe custody of the images saved in the mobile phones and to delete the images as soon as possible after transmitting the same to the mobile service operator's designated secured server.

Audio-recording of a Conversation with Customers

A mobile service operator sometimes, for the purpose of provision of services, audio-records the telephone conversation with a customer during which his personal data can also be recorded. Such audio-recording without prior notification might be considered by customers as offensive, and it might constitute unfair collection of personal data[6].

Tips:

- A mobile service operator is advised to: (i) notify customers prior to the audio-recording and inform them of the purpose of audio-recording; and (ii) give them a choice not to proceed with such audio-recording.

Maintaining Customers' Service Accounts

(i) Accuracy of service account data

To ensure the accuracy of customers' personal data held by it, a mobile service operator should exercise due care when inputting customers' personal data into its customers' database[7]. If the correspondence addresses maintained and used by a mobile service

4 Paragraph 2.3.4.1 of the PI Code

5 DPP4(1)

6 DPP1(2)

7 DPP2(1)

operator for communicating with its customers are inaccurate, customers' account information could be sent and disclosed to unintended recipients, while the customers themselves would not receive the intended correspondence.

Tips:

- Customers' personal data input into a customer database should be counter-checked by another officer to ensure accuracy.

(ii) Adequate verification procedures for change of account information

When a customer requests a change of his account information (e.g. service plan or address) online or through a customer service hotline, the mobile service operator must verify with the requestor that the request is from the genuine customer. The mobile service operator may adopt the practice of notifying the registered customer by SMS and / or email immediately thereafter so as to alert the customer and to identify any mischief.

(iii) Retention of service account data

Different types of personal data may warrant different retention periods depending on the nature and type of the data concerned. A mobile service operator should formulate its policies and practices to specify the period of retention of different types of customers' personal data and erase personal data that is no longer required for fulfilment of the collection purpose (including any directly related purposes)[8]. In formulating such policies and practices, a mobile service operator may take into account any statutory requirements affecting the length of the retention period[9].

(iv) Recovery action of overdue charges

Information relating to default payment is commonly recognised as sensitive data, and should therefore be handled cautiously. A mobile service operator must ensure overdue charges are correctly calculated and the addresses used to send dunning letters are accurate. Dunning letters should be put in a sealed envelope marked "*private and confidential*" or "*to be opened by addressee only*" or words to the like effect, to ensure data security.

Where a mobile service operator engages a debt collection agent to collect overdue charges, it should disclose to the agent only such information necessary for the latter to carry out the action. Generally, the data may include the identity and location particulars of the customer and the overdue amount. If a call is made to the debtor but answered by another person, for example, his family member or a colleague, no information about the debt should be divulged in the call.

Disclosure of Customers' Account Data

If a customer's personal data is disclosed for a new purpose, which is not within or directly related to the mobile service operator's original purpose of collection, it is permissible only if the disclosure is exempted under Part 8 of the Ordinance[10]. Prescribed consent[11] must otherwise be obtained from the customer concerned.

The exemption provisions under Part 8 of the Ordinance (in particular, sections 58 and 60B) and the caveat[12] contained in the licences held by telecommunication companies issued under the Telecommunications Ordinance (Chapter 106) have provided the legal basis for disclosure of customers' personal data to law enforcement agencies and the Commissioner for the purpose of investigation of suspected breach of the law (including the Ordinance) if the conditions therein contained are satisfied.

A mobile service operator may consider if the disclosure is required or authorised by or pursuant to a warrant / summons served on it, or is covered by a requirement under an enactment empowering the law enforcement agency to obtain information. A mobile service operator may seek information or clarification, if necessary, to ascertain the regulator's purpose of obtaining the personal data, in order to satisfy the exemption provision under section 58 of the Ordinance.

---

8 DPP2(2) and section 26 of the Ordinance

9 In general, a mobile service operator may retain records containing customers' personal data for seven years after the termination of the business relationship with its customers according to section 51C(1) of the Inland Revenue Ordinance (Chapter 112).

10 DPP3(1) and (4)

11 A prescribed consent should be given voluntarily and has not been withdrawn by notice in writing.

12 Under "General Condition 7 – Confidentiality of Customer Information" as stipulated in Telecommunications (Carrier Licenses) Regulation (Chapter 106V), the licensee shall not disclose information of a customer except with the consent of the customer, which form of consent shall be approved by the Authority (i.e. the Communications Authority), except for the prevention or detection of crime or the apprehension or prosecution of offenders or except as may be authorised by or under any law.

Measures to Protect Service Account Data

(i) Set default password with high security level

A mobile service operator should not use a password with low security level for the creation of an online account as the defaulted password. It should also remind customers to change the default password and give them tips on how to set passwords with a higher security level.

(ii) Access of service account data by staff

It is unavoidable for a mobile service operator to make customers' service account information available to its relevant staff in the course of performing their duties, but such availability can be restricted to protect the data against unauthorised or accidental access, processing or erasure.

Tips:

- To restrict access of customers' data to staff on a "need-to-know" and "need to-use" basis in relation to the staff's specific duties.
- To require staff to sign a confidentiality statement that specifies expectations and duties in safeguarding customers' data and possible sanctions against those in breach, or incorporate such statement into staff manual or code of conduct.
- To impose internal controls to monitor the access of customers' database by staff (e.g audit trail of the access to, disabling of the printing function of customer records).
- To adopt practices to deal with a breach of the company's policy and procedures concerning customers' personal data.
- To provide proper and regular training to staff on personal data protection.

(iii) Avoid accidental leakage of service account data

When a customer's personal data is required to be processed in a public area (for example, a retail shop which is freely accessible to walk-in customers) where data may be freely accessible by anyone, it may expose the mobile service operator to a higher risk of accidental leakage of data.

Tips:

- In a retail shop with an open-plan design, any computer terminals facing the public area may expose customers' personal data shown on the screens to people standing nearby.
- Verbal communication containing a customer's personal data may easily be overheard by others, especially when the service desks or booths are closely clustered. Care therefore must be taken in the arrangement and the design of the shop to avoid any accidental leakage of a customer's personal data.

Carrying Out of Direct Marketing Activities[13]

Under Part 6A of the Ordinance which regulates the use and provision of personal data for direct marketing purpose, a mobile service operator must notify customers and obtain their "consent" as specified before using or providing their personal data in direct marketing, unless the grandfathering provisions apply.

Tips:

- Since the Ordinance does not specify the manner in which a customer can exercise his opt-out right, a mobile service operator should comply with customers' opt-out requests whether made orally or in writing via any means of communication (e.g. email, telephone call, by post, or in person, etc.).
- A mobile service operator has to maintain and regularly update an opt-out list of customers who have indicated their wish not to receive further marketing approaches. Where the opt-out list is maintained by an online computer network, such new opt-out requests must be inputted as and when they are received. If the list is distributed to marketing staff instead of relying on a computer network, the marketing staff should be notified of the updates of the opt-out list at a frequency of no less than once per week.
- A mobile service operator must not attach advertisements to the electronic service bills sent to a customer who has opted out from its direct marketing activities.

[13] Reference may be made to *New Guidance on Direct Marketing* issued by the Commissioner

- To remind customers of the expiry of services, it is prudent to send "just reminders" for service termination by means of SMS or email to customers who have opted out from direct marketing activities. The mobile service operator must not promote or offer its services to these customers.

Engaging Third Party Agent / Dealer[14]

A mobile service operator is accountable for the acts done or practices engaged by its agents or contractors, for example, IT contractors, delivery contractors, confidential waste disposal companies, debt collection agents or marketing agents, within the scope of the authority given to them[15]. In a case of loss of documents containing customers' personal data (e.g. service bills and HKID Card copy) by an individual courier employed by delivery contractor of mobile service operator, the mobile service operator as well as the delivery courier would be liable for the failure to safeguard the security of the customers' personal data.

Tips:

- A mobile service operator should select a reputable agent or contractor with a good track record on data privacy protection. It should also adopt contractual or other means to ensure that its customers' personal data processed by its agents or contractors is duly protected[16].
- The written service agreement between the mobile service operator and its agents or contractors may contain the following non-exhaustive terms requiring the agents / contractors to :
  - ✓prohibit disclosure or use of customers' personal data for a purpose other than the purpose for which they are assigned to carry out;
  - ✓protect customers' personal data with adequate security measures (and if appropriate, specify those measures);
  - ✓timely return or destruction of customers' personal data when they are no longer required for the purpose the agents / contractors are assigned to carry out; and
  - ✓provide relevant documents and adopt measures to facilitate mobile services operators to check the compliance of requirements.
- A mobile service operator should not 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 e.g. dummy data instead of customers' personal data might be provided to an IT contractor for the purpose of system testing.
- A mobile service operator should also keep proper records and trail of all personal data that has been given to the agent or contractor.

Handling of Data Access / Correction Requests[17]

Unless under specified circumstances under the Ordinance, a mobile service operator is required to comply with its customers' data access requests ("**DARs**") within 40 calendar days after receipt, by either writing to the requestors that it holds the requested data and supplying copies of them, or writing to the requestors that it does not hold the data, as the case may be[18].

Tips:

- It is not sufficient for a mobile service operator, who received a customer's DAR for his personal data provided to a hotline staff during a telephone conversation, to invite the customer to visit its designated shop and listen to the relevant recording. Instead, it should respond to the DAR in writing and provide a copy of the requested recording if it holds and has collected the same.

[14] Reference may be made to the Commissioner's information leaflet: *Outsourcing the Processing of Personal Data to Data Processors*

[15] Section 65(2) of the Ordinance

[16] DPP2(3) and 4(2)

[17] Reference may be made to *Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users* issued by the Commissioner

[18] Section 19(1) of the Ordinance

- Raw data (i.e. outgoing call number, date, time and duration of each call in relation to a particular mobile phone number) kept by a mobile service operator may be traced to a particular subscriber by the information held by the mobile service operator and may therefore amount to personal data.

Concluding Note

Personal data protection cannot be achieved effectively if it is treated as a mere compliance issue, with little involvement of the top management. In order to meet the rising public expectation for privacy protection, a data user, such as a mobile service operator, should be proactive and preventive, rather than reactive and remedial. Furthermore, a robust privacy and risk management programme, with commitment from the top management, will enhance privacy protection of its customers, thereby winning customers' confidence, recognition and trust. The Commissioner's *Privacy Management Programme: A Best Practice Guide* outlines the building blocks of Privacy Management Programmes and provides insight and guidance for an organisation to develop and improve its own programmes according to its specific circumstances and nature of the industry.

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 August 2000
November 2016 (First Revision)