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

Guidance Note

Guidance for Data Users on the Collection and Use of Personal Data through the Internet

Introduction

Operating online businesses or services, whether by commercial enterprises, non-government organisations or public bodies, is now commonplace. In many cases, offering such transactions involves the collection of personal data.

The **Personal Data (Privacy) Ordinance** (the "**Ordinance**") provides for six data protection principles[1] ("**DPPs**"), which set out fair information practices on how personal data should be handled by data users. A data user is defined in the Ordinance, in relation to personal data, as "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data".

The information below seeks to assist data users (referred to as "organisations" in this Guidance Note) in complying with the Ordinance while engaging in the collection, display or transmission of personal data through the Internet.

DPP1 – Purpose and Manner of Collection

Adequate but not excessive personal data collection

DPP1(1) requires an organisation to collect only personal data that is necessary for the purposes for which the data is to be used, and that the data collected is adequate but not excessive for those purposes. For example, if no online purchase or delivery is to be made, generally it would not be necessary to collect the credit card number or residential address of a customer. Normally, date of birth should not be requested when all that is needed is the age of the respondent or a declaration that he/she is over a certain age. Another example is that the gender of a customer is often requested as a norm without justification for any purpose.

Lawful and fair collection

DPP1(2) provides that personal data shall be collected by means which are lawful and fair in the circumstances of the case. The purpose for which personal data is being collected should be stated in an open and straightforward manner, without trickery or deception. For example, collecting personal data by inviting applications for job vacancies that are non-existent or by inviting submissions to fake lucky draws is not a fair data collection practice. Special care is needed when collecting personal data from children. The language used in the collection process should be clear and simple. Organisations should suggest children to consult their parents before providing their personal data.

- **Identity of the organisation**. Sometimes, an organisation collects personal data via the Internet without revealing its contact information other than its web or email address. Very often, such web or email address does not disclose the actual identity of the organisation. This practice may be inconsistent with the requirement of fair means of collection.

  To provide more reliable contact channels, the organisation should disclose clearly its name, physical location and contact telephone and/or fax number, in addition to its web address and/or email address, on its website in the "About us" and/or "Contact us" section.

[1] Available at www.pcpd.org.hk/english/ordinance/ordglance.html

Collecting personal data through the Internet

DPP1(3) sets out the information that a data user has to provide to an individual on or before collecting personal data from that individual. Organisations often use online forms on their websites to collect personal data from individuals or ask them to submit their personal data via email. In doing so, organisations should take all reasonably practicable steps to ensure that individuals providing their personal data are supplied with the information required by **DPP1(3)**.

- **Provide an online Personal Information Collection Statement**. A practical way to comply with **DPP1(3)** is to provide the individual with an online Personal Information Collection Statement ("**PICS**"). **PICS** should be displayed in a clear and conspicuous manner (e.g. accessible on the same web page or through a well described link). It should be easy to read and understand, and its content must be consistent with any printed version distributed offline. Generally, a PICS should include the following information:

  - Whether it is obligatory or voluntary for the individual to supply the data, and where it is obligatory, the consequences for failure to supply the data;
  - The purposes for which the data is to be used;
  - The classes of person to whom the data may be transferred; and
  - The individual's rights to request access to a copy of his personal data and to request correction of the data, and the name or job title, and address, of the responsible person to whom such request may be made.

  For details on how to prepare a **PICS**, organisations may refer to "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement"[2].

- **Label clearly mandatory and optional fields**. If an organisation collects personal data by online form as well as paper form, the types of personal data thereby collected should be the same unless there is good justification. In particular, mandatory items and optional items to be collected should be clearly labelled and users should be allowed to proceed even if optional items are not filled in.

- **Use of cookies and online behavioural tracking**. If a website uses cookies, it is good practice to explicitly state what kind of information (regardless of whether personal data is involved) is stored in the cookies. If a website deploys third-party cookies, regardless of whether any personal data is involved, it should state clearly what kind of information such cookies collect, to whom the information may be transferred and for what purposes.

  If acceptance of the use of cookies is mandatory, this should be stated clearly on the website. If acceptance of the use of cookies is voluntary, users should be provided with such option with clear information on what the consequences will be if users decide not to accept cookies (for example, not accepting session cookies may affect the proper functioning of website).

  Where online tracking is involved, data users should adopt the fair and transparent practice recommended in the "Online Behavioural Tracking" Information Leaflet[3].

DPP2 – Accuracy and Duration of Retention

Accuracy of personal data

DPP2(1) requires a data user to take all reasonably practicable steps to ensure the accuracy of the personal data collected. Although it is not always possible to verify the accuracy of the personal data collected via websites, appropriate and practicable steps should still be taken to ensure the correctness of the personal data collected. For example, a "double confirmation" (sending a verification email message to the reported email address to confirm that the address has been entered correctly) may be required to ensure that any subsequent messages are sent to the correct address. In cases where online verification is not feasible, offline verification may need to be performed.

---

[2] Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

[3] Available at www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf

Duration of personal data retention

DPP2(2) requires a data user to take all reasonably practicable steps to ensure that the personal data collected is not kept longer than is necessary for fulfilment of the purpose for which it is or is to be used. In addition to having a policy setting out the retention period of the personal data collected, there should be a mechanism to ensure that both online and offline copies of the personal data concerned are erased after the retention period[4].

The engagement of data processors

Furthermore, **DPP2(3)** provides that where 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. Organisations may refer to the information leaflet "Outsourcing the Processing of Personal Data to Data Processors"[5] for more details.

DPP3 – Use of Personal Data

Display of personal data through the Internet

DPP3 provides that personal data should not be used for a new purpose unless prescribed consent (i.e. express and voluntary consent) is obtained from the data subject or his/her "relevant person" as defined under the Ordinance[6]. Disclosing or displaying personal data through the Internet may constitute the use of personal data. Hence, in order to comply with the requirements under DPP3, organisations should observe the following points:

- **State at the time of collection that the personal data will be displayed**. If personal data to be collected may later be displayed through the Internet or elsewhere, this intention must be made clear to the individual on or before collecting his personal data. An example could be an Internet-based service which makes available, through the Internet, private tutors' details to parents online. At the time of collecting personal data from the prospective tutors, a statement that such data may be displayed through the Internet should be presented to the tutors. Otherwise, before displaying the data in this way, the organisation must obtain express consent from the tutors.

- **Anonymise the personal data when displaying it**. Anonymous data from which it is not practicable to directly or indirectly ascertain the identity of the individual is not considered personal data under the Ordinance. Before displaying personal data through the Internet, organisations should consider whether anonymising the displayed data would equally serve the purpose. For example, when announcing the winners of a lucky draw or competition on a web page, consideration should be given to displaying the lucky draw ticket number only. This can prevent the improper use of any displayed personal data by third parties. Organisations should be mindful that simply removing names, addresses or other obvious identifiers may not be sufficient to make the data fully anonymous, and therefore should assess each case carefully to ensure re-identification is not practicable. Where personal data must be displayed in order to serve the purpose, the personal data to be displayed should be limited to the extent necessary to achieve the purpose.

- **Limit the purpose of use**. When displaying personal data through the Internet, there should be a statement limiting its further or secondary use. For example, a phone directory or membership directory should contain an announcement that the use of the data is limited only to the specific purposes mentioned. Where the use of the personal data for direct marketing is not allowed, it should be clearly stated.

---

[4] The Commissioner has published a Guidance Note on Personal Data Erasure and Anonymisation which is available at www.pcpd.org.hk/english/publications/files/erasure_e.pdf

[5] Available at www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

[6] For example, if the data subject is a minor, an organisation may obtain the prescribed consent from his parent. See the definition of "relevant person" under section 2(1) of the Ordinance.

DPP4 – Security of Personal Data

Securing the storage and transmission of personal data DPP4(1) requires a data user to take all reasonably practicable steps to implement security precautions, the level of which should be commensurate with the seriousness of the potential harm that could result from a data breach. Security is generally weak on the Internet, so special care is needed to ensure that adequate security measures are implemented for the storage and transmission of personal data.

- **Implement a top-down, Privacy by Design approach**. A top-down approach is required for organisations to ensure holistic protection of personal data. The level of acceptable risk must be decided before the appropriate policies, guidelines, procedures and measures are put in place to achieve that protection. A Privacy by Design approach should be adopted to ensure that personal data protection is built in as an integral part of any system at the feasibility stage and not as an after-thought.

- **Carry out risk assessment**. Not all personal data stored online or transmitted through the Internet requires the same degree of protection. The appropriate degree of protection depends on the sensitivity and volume of the personal data involved. On this basis, risk assessments should be carried out regularly for the various kinds of personal data that are stored or transmitted through the Internet. Organisations should then regularly devise and review appropriate policies, guidelines, procedures and measures to protect the confidentiality and integrity of the personal data in their systems. Such measures will also need to ensure the accountability of those persons who have access to such personal data and to track any action, such as reading/writing/modification, taken.

- **Set policies on the handling of personal data**. **Section 65(1)** of the Ordinance places liability on the employer for any act of his employees done in the course of employment, unless the employer can provide evidence to prove that it had taken such steps as are practicable to prevent the employee from infringing the requirements under the Ordinance. Hence, an organisation should set policies, procedures and guidelines on the handling of personal data and its staff should be regularly reminded to observe the same. Similar liability exists under section 65(2) of the Ordinance in the case of an organisation engaging an agent to handle personal data on its behalf. Hence, in selecting a service provider, an organisation should assess or examine the systems that the service provider has implemented to protect personal data privacy, including whether there are in place adequate security measures and practices.

- **Consider the use of technological safeguards**. If an organisation hosts an application or maintains a database which allows access to personal data online, it should implement sufficient measures to protect the personal data from unauthorised access, and update such measures regularly to tackle evolving security risks. Examples of such measures are listed below:

  - Encrypt personal data being transmitted to prevent unauthorised interception or access.
  - If personal data is stored on the Internet, it should be protected by access controls, encryption and/or other appropriate measures to prevent unauthorised access or alteration.
  - Controls on password complexity, re-tries and resets should be implemented to prevent passwords from being compromised.
  - A properly configured firewall should be used to protect Internet servers that contain personal data. Whenever appropriate, servers or databases holding or receiving personal data should be protected by a "three-tier architecture", so that Internet users are not allowed direct access to the personal data.
  - Develop formal security patch management procedures so that any security patches released by software vendors are applied in a timely manner.
  - Servers accessible through the Internet should be regularly scanned for vulnerabilities, and appropriate action should be taken to remedy any such vulnerabilities.
  - Do not use easily predictable methods (such as using sequential variables in URLs to retrieve personal data. This reduces the risk of unauthorised access of personal data by website visitors by guessing the URL.

- Do not store or request users to upload file containing personal data in webserver without proper protection such as access control and/or encryption, however short the period may be. Contemporary search engines are powerful enough to index files stored under the most obscure URLs.
- Consider installing a data loss prevention system which, among other functions, scans Internet communications for unauthorised disclosure of personal data.
- If multiple server roles or applications are hosted on a single server, cross-application access rights to the personal data should be tested to prevent unauthorised access to personal data from one application to another.
- Consider the use of privacy-enhancing technologies whenever possible to protect personal data privacy. Privacy-enhancing technologies are measures that help to minimise the risk of personal data exposure, such as encryption or hashing to maintain data confidentiality, robots exclusion protocol to prevent search engines from indexing websites, anti-robot verification to stop databases from being downloaded in bulk by automation.

➤ **Provide a privacy warning message**. A secure means of transmission of personal data should be offered to the data subject. Where un-encrypted data transfer is elected by an individual for the transmission of his or her personal data, an appropriate alert should be given to the individual about the risks prior to the transmission.

➤ **Avoid using known personal data for authentication**. It is recommended that personal data that may be obtained by third parties relatively easily, such as date of birth, ID card number or phone number, should not be used as initial password or confirmation/verification code.

➤ **Promote a privacy-aware culture in the workplace**. Every employee should be made aware of the importance of respecting the data privacy rights of individuals, both as a moral obligation and as a legal requirement. All personnel involved in the handling of personal data should be adequately trained in understanding the requirements of the Ordinance and the compliance procedures in place.

➤ **Set an action plan for data breach handling**. Data leakage on the Internet can spread quickly and widely, and the mishandling of leakage may cause irreparable damage to the reputation of an organisation. A transparent data breach handling system[7] should therefore be in place setting out a clear action plan to be followed to contain any breaches, and to mitigate the possible loss and damage caused to the data subjects concerned.

The engagement of data processors

DPP4(2) provides that 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 unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

For detailed guidance on drawing up the terms of data processing contracts, see the information leaflet "Outsourcing the Processing of Personal Data to Data Processors"[8].

DPP5 – Transparency of Policies and Practices

Openness of the organisation's personal data privacy policy

DPP5 stipulates openness by organisations about their policies and practices in relation to personal data. An organisation with a website should make its privacy policy statement ("**PPS**") either accessible or downloadable by web users.

[7] The Commissioner has published a Guidance Note on Data Breach Handling and the Giving of Data Breach Notifications which is available at www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf

[8] See footnote 5

- **Make the privacy policy statement easy to access**. One possible method of ensuring easy access is to set up the **PPS** as a linked page accessible from the home page or other pages where personal data is collected, e.g. a membership registration page or a customer agreement page. The link should be clearly labelled, for example, with a heading such as "Privacy Policy" or in the form of a button or icon carrying with similar meaning.

- **State the privacy policy clearly.** The **PPS** should inform users of the kinds of personal data held by the organisation and the main purposes for which the personal data is or is to be used. In addition, it may contain information about other matters relating to the privacy of personal data, such as the use, if any, of cookies by the organisation to track its visitors, the organisation's policy on direct marketing, and its security and retention policies in respect of personal data.

For details on how to prepare a **PPS**, organisations may refer to "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement"[9].

DPP6 – Access to Personal Data

Under **DPP6**, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data access requests[10] and data correction requests[11].

Direct Marketing Activities

Organisations engaged in direct marketing activities using personal data must comply with **Part VI A** of the Ordinance regarding direct marketing activities.

Organisations should refer to the "New Guidance on Direct Marketing"[12] for more details.

Data user should note that, **Part VI A** of the Ordinance concerning the requirements on direct marketing do apply regardless whether the personal data involved is obtained over the Internet or from data subjects or, and/or whether the direct marketing activities are conducted over the Internet or in conventional ways.

Organisations should also observe and comply with the relevant provisions under the Unsolicited Electronic Messages Ordinance (Cap. 593), which is administered by the Office of the Communications Authority, in carrying out direct marketing activities[13] by electronic messages.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Tel: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk

First published in December 2011
April 2014 (First Revision)

[9] See footnote 2

[10] See www.pcpd.org.hk/english/publications/files/DAR_e.pdf

[11] See www.pcpd.org.hk/english/publications/files/dcr_e.pdf

[12] See www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

[13] See www.ofca.gov.hk/en/industry_focus/uemo/index.html for more details