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

Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement

Introduction

This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement ("**PICS**") and Privacy Policy Statement ("**PPS**"). Both PICS and PPS are important tools used respectively for complying with the requirements of Data Protection Principle (**"DPP"1(3)** and **DPP5** under the **Personal Data (Privacy) Ordinance** (the "**Ordinance**").

The legal requirements

DPP1(3) specifies that a data user, when collecting personal data directly from a data subject, must take all reasonably practicable steps to ensure that:

(a) the data subject is explicitly or implicitly informed, on or before the collection of his personal data, of whether the supply of the personal data is voluntary or obligatory (if the latter is the case, the consequence for the individual if he does not supply the personal data); and

(b) the data subject is explicitly informed:
  (i) on or before the collection of his personal data, of the purpose for which the personal data is to be used and the classes of persons to whom the personal data may be transferred; and

  (ii) on or before the first use of the personal data, of the data subject's rights to request access to and correction of the personal data, and the name (or job title) and address of the individual who is to handle any such request made to the data user.

DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can ascertain its policies and practices in relation to personal data and is informed of the kind of personal data held by the data user and the main purposes for which personal data held by a data user is or is to be used.

What is personal data?

"**Personal data**" is defined under the Ordinance to mean any data:–

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.

Data users often specifically collect or access a wide range of personal data of individuals whose identities they intend or seek to ascertain. They should be mindful, however, that in some other cases the information they have collected, in its totality, could be capable of identifying individuals. For example, a business may collect information about the kinds of goods and services that their customers purchase and subscribe so that it could track the shopping behaviour of its customers for promoting goods and services that are of interest to selected groups of customers.

What are PICS and PPS, and how are they different?

A PICS (or its equivalent) is a statement given by a data user for the purpose of complying with the notification requirements under DPP1(3) of the Ordinance. While the Ordinance does not require the notification to be given in writing, it is good practice for the requisite information to be provided to the data subjects in writing in the interests of transparency and to avoid possible misunderstanding between the parties.

A PPS (or its equivalent) is a general statement about a data user's privacy policies and practices in relation to the personal data it handles. It is good practice to have a PPS in written form to effectively communicate the data user's data management policies and practices despite the Ordinance is silent on the format or presentation of a PPS.

For the purpose of complying with DPP1(3), a PICS should be provided to a data subject by a data user on or before collecting personal data directly from that data subject.

On the other hand, in order to fulfil the requirements of openness and transparency under DPP5, a PPS is required **AT ALL TIMES** if a data user controls the collection, holding, processing or use of personal data. Typically the PPS covers a wider scope and, in addition to some of the core elements of the PICS, may include other privacy related policies and practices such as data retention policy, data security measures, data breach handling, the use of special tools such as cookies on websites.

Specific details of a PICS

* **When and how should a PICS be given:** A PICS should be given to a data subject whenever a data user collects personal data from him. For instance, a data subject applying for services offered by the data user may be required to provide his personal particulars. A PICS in such situations will usually be found in the application form or in a notice posted conspicuously near the counter where collection of personal data occurs (e.g. the registration counter of a hospital).

The need for a PICS applies to the collection of information in both the physical world and the online environment. The most common example in which information of a data subject is collected online is in filling out an online registration form. The form should include a PICS, either as part of its text or by means of a hyperlink on the form. Similarly, information about a data subject may also be collected from him unbeknown to him (e.g. through the use of cookies[1]). A PICS is still required to be presented to the individual on or before collecting the data.

Example:

- *"When you visit this website, we may use cookie files to store and track information about your* (details to be specified by the data user) *or your actions for the purposes of providing our services to you on/for* (details to be specified by the data user)*."*

What goes into a PICS?

* **Statement of Purpose:** This is a statement of the purposes for which personal data will be used following collection.

Examples:

- *"The information collected from you will be used for the purpose of processing your purchase orders and managing your account with us."*
- *"The information collected by means of cookies on this website about you will be used only for compiling aggregate statistics on how visitors browse the website. Such statistics are collected for the purpose of managing and improving the design of the website."*
- *"Your name and address will be used by our leisure club for sending you newsletters and printed material about our recreational events for promoting healthy lifestyle."*

[1] Cookies is a small computer file that is sent from a website to the computer or mobile phone (referred to here as a "device") browser and stored in that device. Each website can send its own cookies to the browser but the browser only permits a website to access the cookies it has sent to the browser previously.

* **Statement as to whether it is obligatory or voluntary for the individual to supply his personal data:** On or before collecting any personal data from a data subject, the data user should inform the individual whether it is obligatory or voluntary for him to supply his personal data; and where it is obligatory for the data subject to supply his personal data, the data user should inform him of the consequences of failure to supply his personal data.

Examples:

- *"Please note that it is mandatory for you to provide personal data marked with asterisks. In the event that you do not provide such personal data, we may not be able to provide you with our products or services."*
- *"Please provide your telephone number in case we need to contact you about your comments on our services. You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your comments".*
- *Where cookies are used on websites to collect information about visitors: "Most web browsers are initially set up to accept cookies. You can choose to 'not accept' cookies by changing the settings but if you do so you may find that certain features on the website, including online banking, do not work properly."*

* **Statement of possible transferees:** This statement should declare the classes of persons to whom personal data collected from the data subjects may be transferred or disclosed.

  The classes of transferees of personal data should be clearly defined so that the data subject can ascertain the same with a reasonable degree of certainty. For example, a data user can specify in its PICS "*we may share your information with credit reference agencies*" to show the class of possible transferees.

  The data user should avoid using broad and general terms, such as "any person", "any business partners" and "any other person under a duty of confidentiality to us". Such statements, without further elaboration, serves little purpose in meeting the notification requirements of DPP1(3).

  If the data user is a member of a group operating a wide range of diversified businesses, the transfer of personal data of customers within the group will exceed the reasonable expectation of customers. In this regard, PICS should not contain statements such as *"you agree that we may disclose and transfer your personal data to any company within the ABC group, their respective subsidiaries and any company in which the same has an interest."*

  If the data user does not disclose personal data to third parties, it would be a good practice to mention this as it is likely to be viewed favourably by data subjects. For example, the following statement can provide assurance to customers: "*The information we collect about you will not be disclosed by us to any other party without your prior consent.*"

  If the data user intends to publish the personal data on a register or website which is open to the public, the data subjects should be explicitly informed of such practice in the relevant PICS.

Example:

- *"For the purposes of providing membership services to you, the information that we collect about you will be published through our website or made available for public access through our registration office."*

✲ **Direct marketing:** If a data user intends to use personal data of the data subject for direct marketing, or provide the personal data to third parties for use in direct marketing, it shall comply with the notification requirements under the Ordinance[2] and obtain the consent or an indication of no objection from the data subject before so using his personal data. Data users may embody the notification in the PICS which should be easily understandable and, if in written form, easily readable form. A response channel should be provided by the data users in the notification for the data subject to communicate his consent[3].

Example of a PICS given by a society or an association which offers special discounts on goods and services (e.g. recreational activities) to individuals who are interested to subscribe or participate:

- *"Your name, mobile phone number and home address collected by us will be used for providing you with information about recreational activities and special offers on household goods, food and entertainment to be provided or sponsored by us.*

  We cannot use your personal data unless we have received your consent or indication of no objection."

Please indicate your consent to receiving information relating to the above by signing and returning to us this Form by Fax # 1234 5678 or by sending it to any of our liaison offices.

_____

Name and signature
(dd/mm/yyyy)

or

If you do not wish to receive information on the above, please tick the box below:

☐ *I object to the proposed use of my personal data as stated above.*

_____

Name and signature
(dd/mm/yyyy)

(In both cases the data user may not use the personal data for direct marketing purpose unless a signed form is returned. In the latter case, if the form is returned with a signature but without a tick, it may be considered as an "indication of no objection".)

✲ **Statement of rights of access and correction and contact detail:** This statement is required to inform the data subject that he or she has the right to request access to and correction of his personal data that is held by the data user.

✲ **Notice of contact person for requesting access or correction:** The data subject should be informed of the name (or job title) and contact details of the individual who is responsible for handling any data access and data correction requests.

Example:

- *"You have the right to request access to and correction of information held by us about you. If you wish to access or correct your personal data, please contact our data protection officer at '1/F, No.1 Main Road, Hong Kong' or dpo@company.com."*

[2] Sections 35C and 35J of the Ordinance

[3] For details, please refer to the New Guidance on Direct Marketing issued by the Commissioner: http://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

Recommended good practices – PICS

* **The purpose statement should not be too vague and too wide in scope:** If the purpose statement is so crafted that the possibilities are endless, then it cannot qualify as a purpose. The data subject must be able to ascertain with a reasonable degree of certainty the purposes of use from a PICS. For example, "*the personal data that you provide us may be used by us as a source of data for other related purposes according to industry practice*" lacks sufficient certainty as "related purposes" therein arguably include "remotely related purposes". Also, the term "*industry practice*" is not an appropriate description of collection purpose in the PICS as it is not self-explanatory. The data user should specify the practice for the data subjects so that they can make an informed decision.

* **The language and presentation of the PICS should be user-friendly:** The PICS shall be presented in a manner that renders it easily readable and understandable in terms of its length, complexity, font size and accessibility.

* **Specific PICS to be used for specific collection purposes:** If a website has more than one online form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

* **Statement of security measures:** A PICS may include a notice about the security measures adopted by the data user in the handling of personal data (in particular if the personal data is collected online, the specific security measures that are applied to online transactions such as collection of credit card numbers).

Example:

- *"The information you submit in filling an online order form will be encrypted (a secure means of transmission) when it is sent electronically to us."*

* **Link to PPS:** A hyperlink can be provided on online forms for collecting personal data to draw the data subject's attention to the contents of the data user's PPS.

Specific Details of a PPS

* **When and how should a PPS be provided:** A PPS should be made available to anyone, in an easily accessible manner, no matter whether personal data is collected by the data user in the physical world or in the online world (e.g. through the use of cookies), or whether personal data is collected directly from the data subject.

  If a website of the data user only collects aggregated information about its visitors (e.g. statistics on the web pages visited, type of browsers used, location of the visitor, number of new or returning visitors etc.) but not any data that could be used to identify a data subject, it would be good practice for the data user to include a statement on its homepage to say clearly and exactly what it collects to alleviate the concerns of the data subjects in relation to personal data protection.

  If a data user operates a website, it is recommended that a web version of the PPS be made available by means of a prominent link at the top or at the bottom of the home page and every page of the website. More and more Internet users are looking for the privacy policies of the websites they visit before they go beyond the homepages. A prominent link to the PPS will therefore help reassure Internet users that the data user is privacy-conscious and transparent about its policy.

Example:

- *"When you visit our website we will record your visit only as a "hit". The webserver makes a record of your visit that includes your IP[4] addresses (and domain names), the types and configurations of browsers, language settings, geo-locations, operating systems, previous sites visited, and time/durations and the pages visited (visitor data). We use the visitor data for the purpose of maintaining and improving our websites such as to determine the optimal screen resolution, which pages have been most frequently visited etc. We use such data only for website enhancement and optimisation purposes. We do not use, and have no intention to use the visitor data to personally identify anyone."*

What goes into a PPS?

- **Statement of policy:** This would express a data user's overall commitment in protecting the privacy interests of the individuals who provide information about themselves to the data user.

Examples:

- *"We are committed to protecting the privacy, confidentiality and security of the personal information we hold by complying with the requirements of Personal Data (Privacy) Ordinance with respect to the management of personal information. We are equally committed to ensuring that all our employees and agents uphold these obligations."*
- *"We pledge to comply with the requirements of the Personal Data (Privacy) Ordinance. In doing so, we will ensure compliance by our staff with the strictest standards of security and confidentiality."*

- **Statement of practices:** This should include the kind of personal data held by the data user and the purposes for which it uses the data. The kind of personal data collected should depend on the actual operational needs of the data user. They may include identification information, contact details, financial details (income/savings/payments etc.), interests, preferences (language, webpage layout etc.), location information of mobile devices, browser details and IP addresses etc. Common purposes for which these types of personal data are used may include the delivery of goods/services, the management of accounts, the processing of orders, the facilitation of website access, the compilation of aggregate statistics on website usage, etc.

Examples:

- *"Your personal details, job particulars, salary and benefits, appraisal and disciplinary records collected and held by us will be used for the purpose of human resource management."*
- *"We will not provide your personal data to third parties for direct marketing or other unrelated purposes without your consent."*

Recommended good practices – content of PPS

- **DPP1: Collection of personal data from minors:** If a data user wants to collect personal data from young people and/or its website includes content of interest to young people, it should include in its PPS a statement on its practices in relation to the collection of personal data from young people. Generally, data users are not advised to collect personal data from minors (particularly those who are incapable of making an informed decision) without prior consent from a person with parental responsibility for the individual.

[4] IP stands for Internet Protocol. IP addresses are used by computers to identify other computers that connect to them.

✲ **DPP1: Collection of personal data from individuals without their knowledge:** If technical means such as cookies are used to collect information from individuals without their knowledge, the data user should include statements on this arrangement in the PPS. Matters that should be covered in the PPS include:

- when are such means used;
- what kind of information is collected by these means, in particular whether any personal data is collected;
- what the information is used for and any disclosure of the information to other parties.

The PPS should also state whether the website allows access by users who do not accept cookies, and what loss of functionality (if any) would result from not accepting cookies[5].

✲ **DPP2: Retention of personal data:** The PPS may state, in general terms, for how long the personal data will be retained. If a data user provides online facilities that allow a data subject to make a deletion request or directly delete his or her account or personal data held by the data user, the PPS should give details such as how it is done and whether the personal data or account so deleted is permanently removed from the system.

✲ **DPP3: Handling of sensitive personal data:** If a data user collects sensitive personal data (health, finance, location, etc.), the data user should explain how it uses, processes, handles and transfers such data. The data user should also make it clear in the PPS whether data subjects have the choice to have such personal data held by the data user erased and express their choice not to have the data shared or transferred.

✲ **DPP3: Disclosure of personal data:** If personal data would not be disclosed to other parties without the data subject's express and voluntary consent, it is advisable for such policy to be stated in the PPS. If personal data would be disclosed to third parties (such as to pass personal data to credit card companies for payment transactions and this is made clear under the PICS) or if the website will share visitor details (such as IP addresses and browser types) with other parties and organisations, all such practices should be made known in the PPS.

✲ **DPP4(1): Protection measures:** Data users are advised to state in the PPS how they ensure the security and confidentiality of the personal data collected. For example, if the data user has adopted protective measures such as restricting access of personal data to relevant employees on a "need-to-know" basis, providing relevant training to the employees to handle personal data properly and applying encryption to personal data when necessary, it is a good practice to state such measures in the PPS. This assures data subjects that their personal data is duly protected.

✲ **DPP4(2): Outsourcing arrangements:** If a data user engages service providers[6] to handle or process personal data (such as IT contractors, agencies for clearing payments, survey software/agencies, website analytics service provider, confidential documents disposal service agents etc.), the PPS should, as a matter of good practice, state clearly what personal data will be transferred to such third-parties and how such third-parties will ensure protection of the personal data collected.

---

[5] Data users may refer to our Information Leaflet on "Online Behavioural Tracking" issued by the Commissioner. http://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf

[6] A service provider includes a person who processes personal data on behalf of a data user, and does not process the data for any of his own purposes. Data users may refer to the Information Leaflet on "Outsourcing the Processing of Personal Data to Data Processors" issued by the Commissioner. http://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

- **DPP5: Transparency:** If an organisation does not collect or use personal data obtained from or about individuals, they should make this practice known through a PPS to assure the public of its commitments. This is particularly important when individuals believe or suspect their personal data is being collected or used. For example, in the case of individuals using an organisation's smartphone app, browsing its website, or visiting its premises that have CCTV cameras installed. Individuals may assume that their personal data is collected under these circumstances and if they do not see relevant information in the PPS about how the organisation handles their personal data, they may lose their confidence in the organisation.

- **DPP6: Access and correction:** In the interest of transparency, a data user is advised to state in the PPS its policy on handling data subject's requests to access and to correct their personal data held by the data user. It should include information on how a data user prefers to receive such requests (e.g. the requester needs to use the form[7] prescribed by the Commissioner); what the data user requires in order to be satisfied that the requestor is properly authorised and entitled to make the request[8]; and the amount payable[9], if any.

- **Answering enquiries about privacy policy and practices:** The PPS may also include the contact details (for example, office address and email address) of the officer in the data user's organisation who will answer enquiries regarding the data user's privacy policies and practices.

Recommended good practices – format of PPS

- **User-friendly language and presentation:** The PPS should be easily understandable and readable, taking into account factors such as content, font size, language used.

- **Layered presentation:** If the privacy policies and practices of a data user is so complex that it requires a lengthy PPS, the data user may consider using proper headings and adopting a layered approach in presentation. With this approach, a key statement in easily understandable language is presented to data subjects in the first instance, and more in-depth explanation is made available as a second-layer document. If a data subject wishes to learn more about a specific aspect of the data user's policies or practices, he can follow links (for online version) or references (for printed version) and move to the more detailed second-layer document for answers.

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

[7] The data access request form, OPS003, which can be downloaded from the Commissioner's website. http://www.pcpd.org.hk/english/publications/files/Dforme.pdf

[8] Reference can be made to the Guidance Note on "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users" issued by the Commissioner. http://www.pcpd.org.hk/english/publications/files/DAR_e.pdf

[9] Any fee charged by the data user for compliance with a data access request must not be excessive.