Personal Data Privacy and the Internet – A Guide for Data Users

CONTENTS

Introduction

This Guide is about the use of the Internet as a way of collecting, displaying or referring to personal data that is covered by the Personal Data (Privacy) Ordinance ("the Ordinance"). Generally speaking, the Ordinance regulates the collection, storage and use of data related to living individuals from which it is reasonably practicable to identify the individuals. It applies to data users in Hong Kong, whether they are individuals, private companies or public bodies. A "data user" is defined in the Ordinance 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 Ordinance is founded on six data protection principles (DPPs) that state the requirements on how personal data should be handled unless the Ordinance allows an exemption. Individuals should note that they are not exempt from compliance with the DPPs except where they collect and use personal data only for the management of personal, family or household affairs or for recreational purposes.

The main purpose of this Guide is to assist data users (referred to as "organisations" in this Guide) in complying with some of the more common applicable requirements of the Ordinance when they are collecting, displaying or transmitting personal data over the Internet.

(The six data protection principles in the Ordinance are set out at the end of this Guide together with a glossary of the terms used in this Guide)

Identity of the organisation

It is possible that an organisation may collect personal data via the Internet without publishing contact information other than its web address. Very often, the web address does not disclose the actual identity of the organisation. This practice may be inconsistent with the requirement of DPP1 which provides that personal data shall be collected by means which are fair in the circumstances of the case, i.e. it may be unfair for a data user to collect personal data without revealing its true identity.

=> Avoid the Web facade. Provide web pages that make available information "About the Organisation". Include the name, physical location and contact telephone/fax numbers of the organisation in addition to the web address or e-mail address. This would be a reliable channel through which a web user could contact the organisation.

Openness of the organisation's personal data privacy policy

DPP5 provides for openness by organisations about their policies and practices in relation to personal data, the kinds of personal data they hold and the main purposes for which personal data are used. This requirement can be complied with by preparing a privacy policy statement which sets out these matters. Organisations with web sites should have their privacy policy statements either accessible or downloadable by their web users.

=> Make the privacy policy statement easy to access. One possible method is to set up the privacy policy statement as a linked page accessible from the home page or other pages where personal data are collected, e.g. a registration page where registration is required for access or a customer agreement page. The link could be done with text such as "Your Privacy" or a button with similar wording.

=> State the privacy policy clearly. The privacy policy statement should inform web users of the kinds of personal data held by the organisation and the main purposes for which the personal data are or are to be used. In addition, it should give information about other matters relating to the privacy of personal data, such as, the use, if any, of "cookies" files by the organisation to track its visitors, the organisation's policy on "spamming", and its security and retention policies in respect of personal data.

=> Be a privacy-aware organisation. Organisations with web sites should keep abreast of developments in privacy compliance schemes and standards by international bodies such as the Electronic Frontier Foundation (EFF)(http://www.eff.org) or the World Wide Web Consortium (W3C)(http://www.w3.org). Consider participation in these and other similar initiatives. With

increasing concern about privacy issues by Internet users, organisations who are not "privacy-compliant" may be at a competitive disadvantage.

Collecting personal data on the Internet

DPP1 requires the lawful and fair collection of personal data and sets out the information a data user must provide to an individual when collecting personal data from that individual. Organisations often use on-line forms on their web pages to collect personal data from web users when providing services or request web users to 浭 end an e-mail* with personal details. In doing so, organisations should take all reasonably practicable steps to ensure that an individual providing his/her personal data is provided with the information required by DPP1. This applies to on-line forms on web pages that an organisation controls, as well as to paper forms which are used to collect personal data.

=> Provide a Personal Information Collection statement. An acceptable way to inform a person from whom personal data are collected is to provide a Personal Information Collection statement (PIC statement). A PIC statement should be easy to find, easy to read and easy to understand. As a minimum, it should cover the following information required by DPP1:

* The purposes for which the data are or are to be used;
* The classes of person to whom the data may be passed;
* The data subject's rights to request a copy of the data and correct any errors, and who should be contacted to make such requests.

=> Make the PIC statement an on-line notice. The PIC statement can be laid out on the same web page as each form, or it can be on another page, as long as every form carries a clearly visible, well-described link to that separate page. The link could be a button or icon that, when clicked, will allow access to the additional pages containing the PIC statement.

=> Collect data fairly. The purpose for which data are collected should be stated in a straightforward and open manner without trickery or deception. For example, building a candidate file by inviting applications to vacancies that are, in reality, non-existent would not be fair data collection. Similarly, collecting personal data for a fictitious lucky draw would not meet the requirements of DPP1. Special care is needed when a web page and any form on it are expected to collect personal data from children. The wording should be as complete, clear and simple as possible. In addition, the statement on the form may suggest that the child talks to a parent before filling in the form.

=> Collect adequate but not excessive data relevant to the purpose. When an organisation collects personal data, whether on the Internet or through any other medium, DPP1 requires that the items of information collected should be necessary for or directly related to the purpose of collection and not excessive for that purpose. For examples: If no purchase is to be made, generally it will be excessive and not relevant to request a credit card number. Often age is requested, when all that is needed is a statement that the respondent is over 18. The sex of a respondent is often requested but keeping a record of that might not be justified for the purpose for which the data are collected.

Displaying personal data on the Internet

DPP3 provides that personal data may be used only for the purpose of collection or a directly related purpose unless express consent is obtained from the data subject given voluntarily to use the data for a different purpose. "Use" in relation to personal data includes disclosure or transfer of the data. Organisations which engage in business practices that may involve disclosing personal data on the Internet should pay special attention to this requirement.

=> State that personal data will be displayed at the time of collection. If personal details are collected and are later to be displayed on the Internet or elsewhere, this intention must be made clear to the individual at the time of collecting the data. An example would be an Internet recruitment service which makes personal data on job seekers available through the Internet. At the time of collecting the data from the applicant, a statement that this will be done should be made. Otherwise, before displaying the data in this way, the organisation should obtain express permission

from the applicant.

=> Anonymise the personal data when displaying. Anonymous data from which it is not practicable to ascertain the identity of the individual is not personal data. Before displaying personal data on the Internet, organisations should consider anonymising the data as an additional precautionary step to avoid presenting detailed information that might be excessive or abused. For example, such consideration should be given when displaying personal details of the winners of lucky draws and competitions on a web page. In particular, names and ID card numbers should not be published together. Publishing the ID Card number alone would generally be acceptable, as it would provide the necessary and reliable information with a high degree of anonymity.

Making secure transmission of personal data on the Internet

DPP4 requires all practical steps to be taken by a data user to implement security precautions the level of which should reflect the seriousness of potential harm resulting from a security breach. Security is generally weak on the Internet and special care is needed to ensure that adequate security measures are implemented for the storage and transmission of personal data.

=> Use encryption when transmitting sensitive personal data. To satisfy the requirements of DPP4, it would be necessary for organisations to carry out a "harm test" on the personal data they seek and transmit on the Internet so as to implement the appropriate level of security measures. For example, organisations seeking detailed resumes from job applicants for vacant posts or credit card/bank account information for service payments would normally require a more stringent level of security measures in the transmission of such data than say, names or office addresses. Similar considerations should also be applied when sending e-mails that contain sensitive personal data over the Internet. The use of encrypted data transfer is one practical means of transmitting such data on the Internet and should be seriously considered.

=> Provide a privacy warrning message. If un-encrypted data transfer is used for the transmission by users of sensitive personal data, the web site should alert users about the risks in transmission or offer alternative secure means to the users in supplying the data. However, this does not lessen the obligations on organisations as regards the other requirements of DPP4. For example, an organisation that operates its own web server should take practicable steps to ensure that its server is protected against security attacks over the Internet and that a well organised and safe system of backups is in place.

E-mails carrying personal data on the Internet

Organisations may give their employees access to the Internet for sending and receiving e-mails. Some of these e-mails may contain personal data. DPP4 requires that all practicable steps should be taken to put in place measures for ensuring the integrity, prudence and competence of persons having control of and access to personal data. Section 65 of the Ordinance (which is set out at the end of this Guide) places liability on the employer for any act of their employees done in the course of employment that may have contravened a requirement of the Ordinance unless the employer can provide evidence to prove that precautionary measures have been taken to prevent the employee from doing that act. Adequate policies and procedures should therefore be put in place and staff should be regularly reminded to observe compliance with the requirements of the Ordinance. Areas in which guidelines are needed may include the following:

=> Set a policy on Internet e-mail communication. Not all personal data communicated via e-mail requires the same degree of security. The appropriate degree of security will depend on the sensitivity and volume of personal data communicated. Hence, a first step is to categorise the various kinds of personal data held by the organisation and the circumstances under which the staff are allowed to transmit these data via Internet e-mail. Organisations should also consider restricting the sending of sensitive personal data except by authorised personnel and to implement procedures ensuring that only authorised recipients have access to and custody of Internet e-mails containing sensitive personal data.

=> Consider the use of technological safeguards. If sending sensitive personal data by e-mails is

permitted, a practical means to prevent unauthorised interception or access is to encrypt the data before sending. In situations where encryption is not possible, or incoming Internet e-mails contain un-encrypted sensitive personal data or encrypted e-mails are decrypted and read, care should be taken to ensure that the data are stored in a secure location. For example, an organisation that operates its own web server can automatically route incoming Internet e-mails to a pre-determined server directory or confidential mailboxes that can only be accessed by authorised persons. An organisation that chooses an Internet Service Provider (ISP) for hosting their web pages will have to depend on the ISP for security protection. In such a situation, the organisation should examine the measures an ISP has implemented to protect personal data, for example, the availability of server software or hardware that provides adequate protection, before making a commitment to that ISP.

=> Promote a privacy-aware culture in the workplace. Every employee should be aware of the importance of respecting others' privacy rights both as a moral obligation and as a legal requirement under the Ordinance. All personnel involved with personal data should be fully aware of and adequately trained in privacy protection procedures.

Direct marketing activities on the Internet

Section 34 of the Ordinance (which is set out at the end of this Guide) requires a data user, on the first occasion it uses personal data for direct marketing, to offer the opportunity to the individual who is the subject of the data, at no cost, to opt-out of receiving further promotional or marketing contacts. This requirement also applies to Internet marketing activities, i.e. when an organisation sends unsolicited promotional and marketing mails to individuals over the Internet.

=> State that direct marketing is a purpose of use of personal data at the time of collection. DPP1 sets out the information an organisation must give to an individual when collecting personal data from that individual. An acceptable means to do this is by way of providing a PIC statement as an on-line notice (see section on "collecting personal data on the Internet"). If personal data are collected that may subsequently be used for direct marketing purposes, this purpose of use must be clearly stated in the PIC statement. The directing marketing purpose must be specific, clear and relevant to the functions and activities of the organisation.

=> Provide an opt-out choice to the individual. When an organisation uses personal data to send direct marketing mails over the Internet, it must provide a prominent message to offer the recipients an opportunity to opt-out from receiving any further mailings. The message should clearly and accurately inform the recipients of their opt-out choices along the following lines: "If you do not wish to receive further marketing mails from us, please write to us or send us an e-mail." The opt-out choice should also enable the recipients to op-out from sources other than the marketer's own database, such as external lists or databases rented by the marketer.

=> Maintain an opt-out list. To comply with opt-out requests, it is necessary to maintain a record of the individuals who have requested an opt-out from further marketing approaches. The record should be updated regularly as and when new opt-out requests are received. If the data source is the marketer's own customer database, it should place a suppression marker against the individual's data upon receiving the individual's opt-out request.

=> Set a policy on unsolicited advertising e-mails (spamming). An organisation should be open about its policy on sending unsolicited advertising e-mails to prospective consumers. In drawing up the policy, the following factors should be considered:

* the right of the individual to opt-out from receiving future unsolicited advertising e-mails;
* the channels available, whether by an e-mail, postal or telephone contact, to permit the individual to make an opt-out request;
* the system or procedures that are in place to comply with an individual's op-out request.

Data users who are Internet Service Providers (ISP) - other considerations

=> Handling personal data flowing through an ISP site. If an organisation operates an Internet server, it is legally not a data user in respect of any personal data received from another server and

passed on to a third party, provided it makes no use of the data for any of its own purposes. This applies to telecommunications organisations which provide the basic network for data transfer and ISPs which provide the "store and forward" function of data traffic and connectivity to the Internet. Personal data contained in web pages which the ISP hosts for its customers or e-mails in-transit would therefore not be the ISP's responsibility under the Ordinance. Even so, a good practice for an ISP would be to transfer the transit data to its destination immediately, by secure means of transmission, and delete the data from its server at the earliest opportunity according to its retention policy.

=> Handling personal data of subscribers. Subscribers to an ISP for its access service to the Internet are customers of the ISP. Inevitably, personal data will be collected from the subscribers for the purpose of account administration. In this respect, the ISP will be a data user as defined by the Ordinance as regards the customers' personal data that it collects, holds, processes and uses. Guidance provided in previous sections of this Guide is applicable to such data.

=> Using "clicktrails" information. Customers' activities and trails from site to site and stored on the server's log files as they surf the Internet, are personal data if it is possible to relate such clicktrails to an individual customer in any practicable way. The issue with clicktrails is that the information collected may be analysed such that a profile of the individual's interests and preferences can be built or sold, say for direct marketing purposes. It may also indicate personal interests or activities of a sensitive nature, e.g. regular accesses to a particular site. An ISP should not do this kind of analysis as the customer does not provide the data for such use. Indeed, most customers are probably unaware that such personal data about them may exist. ISPs should mention in their PIC Statements (see section on "collecting personal data on the Internet") that such data collected will only be used for the purpose of system maintenance and troubleshooting.

=> Handling access request regarding "clicktrails" information. The Ordinance provides an individual a right to request a copy of the personal data relating to him/her held by a data user. Access to data that relates to an identifiable individual needs only be provided if it would be reasonably practicable to access or process such data. Hence, if the clicktrails records are held in such a manner that access on the basis of attribution to particular individuals is not practicable, the ISP is not required to provide a copy in response to such an access request.

=> Offering a secure environment that meets service commitment. An ISP in offering services will hold information related to its customers including personal data. Such information is usually held in computers in an ISP's office. Provision of security measures to protect them from unauthorised access or hacker attacks is a responsibility of the ISP as required by DPP4. To meet this obligation, an ISP should provide a secure location for its computers, establish policies about confidentiality of customers' e-mails and not using information seen there, make known its policies on personal data to all staff, and remind staff of these from time to time. ISPs with 24-hour staff cover or giving staff remote server access have a particular responsibility in this area. ISPs should be privacy-aware and constantly strive to offer privacy enhancing capabilities to their customers. For example, an ISP with server software that is able to handle encryption of data will be welcomed by customers who wish to transmit sensitive personal data.

Data users who are public sector organisations - other considerations

=> Dissemination of public information on the Internet. The Internet is a highly suitable medium for the delivery of public information to the on-line community. In doing so, a public sector organisation could encourage users to visit its site, with trust and confidence, by reassuring them about its privacy protection practices. For example, the site may have an anonymous browsing policy for visitors who are not required to disclose any personal identifiable information. Such a practice should be included in the organisation's privacy policy notice which should be easily accessed or downloaded by users visiting the site (see section on "openness of the organisation's personal data privacy policy").

=> Public service on the Internet. Some public sector organisations have chosen to put their

service application forms on their web pages for downloading or on-line completion by members of the public. Such on-line forms, like paper forms, would normally result in the collection of personal data of the individuals. In this respect, the provision of a Personal Information Collection (PIC) statement is required (see section on "collecting personal data on the Internet"). If the submission of the completed on-line forms is allowed to be sent via the Internet, the public sector organisation should offer secure transmission of the data (see section on "Taking secure transmission of personal data on the Internet").

=> Conducting electronic business transactions on the Internet. Using the Internet to conduct business via electronic transactions is increasingly an important part of an organisation's effort to improve its services. This is as true for the public sector as it is for the private sector, and possibly more so. When engaging in transactions electronically with an organisation, members of the public will welcome a guarantee of their privacy from the organisation. In dealings with public sector organisations, the public expectation with respect to privacy protection is even higher because of the generally higher quantity of personal data required. In recognising such an expectation, a public sector organisation should consider the use of various privacy enhancing technologies in its implementation of electronic transactions so that the amount of personally identifiable information is kept to a minimum while the integrity, security and authenticity of the data contained in such transactions are adequately maintained.

Glossary

Clicktrails - these are information derived from an individual's behaviour, pathway, or choices expressed while visiting a web site. They contain the links that a user has followed and are logged on the web server (the ISP's computer, for those who do not run their web server) normally used for purpose of troubleshooting and system maintenance.

Cookie - A small computer file that is sent from a web server to an user's computer for the purpose of future identification of that computer on future visits to the same web site.

Electronic Frontier Foundation (EFF) - It is a non-profit civil liberties organisation working in the public interest to promote privacy, free expression and social responsibility in new media. Together with CommerceNet, it launches the TRUSTe program which is a non-profit, global initiative for establishing consumer trust and confidence in electronic commerce.

Internet Service Provider (ISP) - A company that provides access and connectivity to the Internet to members of the public and companies. Some ISPs also provide service to host web pages for their customers.

Encryption - Encoding information and messages in such a way that they cannot, in principle, be read by someone other than the intended recipient who has access to a key or password.

On-line submission - Specifically in the Internet context . . . sending data, usually entered on forms, through the Internet.

Privacy enhancing technologies - As opposed to privacy diminishing technologies, these are technical implementations that provide safeguards to the protection of data privacy. Common techniques include encryption, digital signatures, trusted third party concept, anonymous remailers operation, etc.

Server - Software that performs a function on request from another computer, or another computer program running on the same computer (the client), and hands back the result to the client.

Site - In the context of the World Wide Web, this is a collection of web pages, pictures and programs that will control how an Internet user's computer displays information in its browser, e-mail software or other software.

Spamming - The sending of unsolicited advertising of goods or services using e-mails.

Web pages - Screens of information and graphics that appear when a browser program is properly connected to a web site.

Web server - Computer software that accepts requests to show web pages and responds to those requests. Also supports other functions of World Wide Web activity.
World Wide Web Consortium (W3C) - It was founded in 1994 to develop common protocols for the evolution of the World Wide Web. It is an international industry consortium, jointly hosted by the Massachusetts Institute of Technology Laboratory for Computer Science in the United States; the Institute National de Recherche en Informatique et en Automatique in Europe; and the Keio University Shonan Fujisawa Campus in Asia.

DATA PROTECTION PRINCIPLES & SECTIONS 34 and 65
OF THE PERSONAL DATA (PRIVACY) ORDINANCE

Data Protection Principles

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

(1) Personal data shall not be collected unless -

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

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

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

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

(a) lawful; and

(b) fair in the circumstances of the case.

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

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

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

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

(b) he is explicitly informed -

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

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

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

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

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

(B) the name and address of the individual to whom any such request may be made,

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

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

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

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

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

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

(ii) the data are erased

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

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

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate and

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

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose

(including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than -

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

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

4. Principle 4 * security of personal data

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

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

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

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

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

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

5. Principle 5 * information to be generally available

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

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

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

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

6. Principle 6 - access to personal data

A data subject shall be entitled to -

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

(b) request access to personal data -

(i) within a reasonable time;

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

(iii) in a reasonable manner and

(iv) in a form that is intelligible;

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

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

(e) request the correction of personal data;

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

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

Section 34

34. Use of personal data in direct marketing

(1) A data user who -

(a) has obtained personal data from any source (including the data subject); and

(b)uses the data for direct marketing purposes, shall -

(i) the first time he so uses those data after this section comes into operation, inform the data subject that the data user is required, without charge to the data subject, to cease to so use those data if the data subject so requests;

(ii) if the data subject so requests, cease to so use those data without charge to the data subject.

(2) In this section, "direct marketing" (直接促銷) means -

(a) the offering of goods, facilities or services;

(b) the advertising of the availability of goods, facilities or services; or

(c) the solicitation of donations or contributions for charitable cultural, philanthropic, recreational, political or other purposes, by means of -

(i) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or

(ii) telephone calls made to specific persons.

Section 65

65. Liability of employers and principals

(1) Any act done or practice engaged in by a person in the course of his employment shall be treated for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

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

(3) In proceedings brought under this Ordinance against any person in respect of an act or practice alleged to have been done or engaged in, as the case may be, by an employee of his it shall be a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing that act or engaging in that practice, or from doing or engaging in, in the course of his employment, acts or practices, as the case may be, of that description.

(4) For the avoidance of doubt, it is hereby declared that this section shall not apply for the purposes of any criminal proceedings.

[The information provided in this Guide is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of the law, direct reference should be made to the Ordinance itself.]