CONTENTS

[This booklet is produced for general reference only. It does not provide an exhaustive guide to the relevant provisions of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of the law, readers should refer to the Ordinance itself.]

All copyright reserved by the Office of the Privacy Commissioner for Personal Data. Short extracts from this booklet may be reproduced in other publications, but the source of the material must be acknowledged. If you wish to reproduce the whole booklet for trade or business purposes, you must first seek permission from the Office of the Privacy Commissioner for Personal Data.

Office of the Privacy Commissioner for Personal Data November 1996

INTRODUCTION

This booklet has been prepared to assist data users, i.e. persons who control the collection, holding, processing and use of personal data, to comply with the Personal Data (Privacy) Ordinance (the Ordinance). Personal data in this context means recorded information relating to a living individual from which it is reasonably practicable to identify the individual concerned and that are reasonably practicable to access or process. This guide sets out an outline action plan for data users to undertake to comply with the key requirements of the data protection principles contained in the Ordinance.

The full text of the data protection principles is given in the appendix to this booklet. Other requirements and provisions of the Ordinance will be the subject of further guidance to be issued as necessary.

Compliance with the data protection principles and the other provisions of the Ordinance is of course required as a matter of law. However, organisations should not view compliance simply from the negative perspective of avoiding legal sanctions. It is advisable for organisations to view compliance in the positive light of the benefits this will bring in terms of improved customer and employee relations and improved record management, which will result in operational efficiency and planning gains.

Enquiries concerning the content of this guide and requests for copies of the previously issued "Personal Data (Privacy) Ordinance - A Guide For Data Users" and "A Guide For Data Users - No.2 - Compliance with Data Access And Correction Requests" should be directed to:

The Office of the Privacy Commissioner for Personal Data
Unit 2001, 20th Floor, Office Tower, Convention Plaza1 Harbour Road Wan Chai
Hong Kong

Before you begin: Commit to Action and Assign Responsibility

It is recommended that senior management in each organisation make a commitment to implementing the requirements of the Ordinance to safeguard the privacy of customers and employees with respect to personal data. This commitment should be made known throughout the organisation concerned. It is also recommended that each organisation assign responsibility for co-ordinating and overseeing compliance with the Ordinance to a particular individual or group of individuals. These

recommendations are not direct requirements of the Ordinance, but they will help ensure that the actions your organisation takes to comply with the Ordinance are carried out in a thorough and consistent manner.

ACTION 1 Collect Personal Data Fairly

[Data Protection Principle 1 - purpose and manner of collection of personal data]

Step 1: Identify means of collection

Identify each means by which you collect personal data. Such means may include the use of printed forms, face to face or telephone interviews, advertisements that solicit the submission of personal information or obtaining data about an individual from another person or organisation.

Step 2: Identify purposes of collection

For each means of collection of personal data identified in Step 1, identify the purposes for which the personal data are being collected.

Step 3: Identify functions and activities

Identify your organisation's functions and activities. This should be done by reference to the organisation's current scope of operations. Possible future functions and activities should not be included.

Step 4: Review means of collecting personal data

・Review each means of collecting personal data identified in Step 1 to ensure that they are lawful. Lawful here means lawful under both criminal and civil law. An obvious example of a means of collection of personal data that is unlawful under criminal law is theft. Examples of unlawful means of collection of personal data under civil law include means involving a breach of an enforceable contract or duty of confidence.

・Review whether each means of collecting personal data identified in Step 1 is fair in the circumstances in which the means is utilised. If any of your means of collecting personal data is unfair, cease to utilise it. For example, it would generally not be fair for persons collecting personal data not to identify themselves or to give false or misleading information about their identity. Other practices that would generally be unfair would be the giving of a misleading impression about the degree of confidentiality to which the personal data will be subjected or applying undue pressure to obtain personal data.

Step 5: Review purposes of collection

・Review each purpose identified in Step 2 to ensure that it is lawful. See Step 4 above for guidance on what is meant by lawful.

・Review whether each purpose identified in Step 2 is directly related to your functions or activities identified in Step 3. If any of your purposes do not meet this

test, cease to collect personal data for the purpose concerned.

・Review whether the personal data you are collecting are really needed for the purposes identified in Step 2. The personal data you collect should be adequate for such purposes, but not excessive. If you are collecting personal data that fail this test, take action to ensure that you cease to collect the data concerned. For example, a form used for collecting personal data from an individual for certain purposes may also collect data about his or her relatives that are neither necessary nor relevant to those purposes. In such a case, the parts of the form that ask for the unnecessary personal data should be removed. If personal data sought by one part of a form are necessary in relation to some classes of individual, but not others, care should be taken to structure the form so that only the former are asked to complete the part concerned.

Step 6: Identify classes of transferees

Identify any classes of persons to whom personal data collected by each means of collection identified in Step 1 may be transferred. For example, a company may regularly pass on personal data collected by a particular form to subsidiary companies within the same group.

Step 7: Inform individuals of purposes of collection, etc.

For each means of collection identified in Step 1, where the personal data are collected from the subject of the data (data subject), draw up and implement arrangements to ensure the data subject is informed :

・explicitly or implicitly, of whether it is obligatory to supply the data being collected, such as where there is a legal obligation to do so, and, if so, the consequence if the data subject does not do so; and

・explicitly, of:

  ・the purposes of collection identified in Step 2 (which may be expressed in general or specific terms);

  ・the classes of person to whom the data may be transferred identified in Step 6;

  ・the rights of the data subject to request access to and correction of the personal data; and

  ・the name and address of the individual in your organisation to whom personal data access and correction requests may be made. Possible arrangements for informing data subjects of these matters include printing them with reasonable prominence on the relevant form as a personal information collection statement, inviting the data subject to read a printed notice that sets them out or orally informing the data subject of them.

ACTION 2 Limit the Use of Personal Data

[Data Protection Principle 3 - use of personal data]

・Review whether the personal data you hold are only used (which includes disclosed or transferred) for the purposes identified at Step 2 under Action 1 above for which they were to be used at the time of collection, or for a directly related purpose.

・If you are using personal data for a different purpose, check whether the data subjects concerned have given consent for this change of use. To be effective, such consent must be express and given voluntarily. If such consent has not been given, you must either obtain it or stop using the data for the purpose concerned.

ACTION 3 Ensure Accuracy

[Data Protection Principle 2 - accuracy and duration of retention of personal data]

・Review whether your arrangements for checking and updating personal data meet the requirement to take all reasonably practicable steps to ensure accuracy having regard to the purposes for which the personal data are used. For personal data to be accurate, all statements of purported fact contained in the data should be correct. The accuracy requirement is not directly concerned with statements of pure opinion, although all reasonably practicable steps should be taken to ensure that any facts cited in support of such an opinion are correct.

・Where a purpose requires the holding of historical personal data, accuracy is a matter of whether the data correctly reflect the position at the time to which they refer. For example, a purpose may require the holding of data about a person's past income. In such a case, a correct statement of that person's income at a particular time in the past that is recorded by reference to that time would meet the accuracy requirement.

・Review whether you have reasonable grounds for believing that personal data held by you are inaccurate having regard to the purposes for which they are used. If you have doubts about the accuracy of personal data you hold, you must either correct or delete the data concerned.

・If you disclose or transfer personal data to third parties, ensure that you have arrangements for forwarding corrections to the parties concerned.

・Review whether your arrangements for disposing of obsolete records meet the requirement that personal data shall not be kept for longer than is necessary for the purposes for which they are used. Consider, if you have not already done so, the adoption of standard review and retention periods for different types of

personal data. If you need to keep personal data for statistical purposes, consider whether such purposes can still be achieved if the data are made anonymous by removing information that makes it possible to identify the subject of the data.

ACTION 4 Ensure Security

[Data Protection Principle 4 - security of personal data]

・Implement arrangements for ensuring an adequate level of protection for the personal data you collect, hold, process or use against unauthorised access, processing, erasure or other use.

・While there are no hard and fast rules on what constitutes an adequate level of security in a particular case, the greater the sensitivity of the data and harm that would be caused by unauthorised access, etc., the higher the level of security should be. In deciding whether your security precautions provide an appropriate level of protection, you should have regard to:

・the location of the data, for example, whether they are held in an area to which access is restricted;

・security measures incorporated into the equipment in which the data are held, such as, the use of computer passwords;

・measures for ensuring the integrity, prudence and competence of persons having access to the data; and

・measures for ensuring secure transmission.

ACTION 5 Adopt Openness

[Data Protection Principle 5 - information to be generally available]

・Be prepared to inform anyone on request of the kinds of personal data you hold and the main purposes for which you use personal data, as well as your policies and practices in relation to personal data.

・One way to meet this requirement is to draw up a written statement of these matters to be provided on request. Any such statement should be regularly reviewed to ensure that it remains up to date.

ACTION 6 Comply with Data Access and Correction Requests

[Data Protection Principle 6 - access to personal data]

・Familiarise yourself with the requirements for complying with requests by individuals to ascertain whether you hold data pertaining to them, to obtain a copy of such data and to correct such data (see A Guide for Data Users - No.2).

・Ensure you have administrative arrangements for handling such requests. For example, you need to designate an individual as having the responsibility for receiving requests of this nature (see Step 7 under Action 1 above). That individual will need to have the authority to seek a response to a particular request from those responsible within the organisation for any data to which it relates. It is also advisable to have in place a system for checking progress in responding to such requests to ensure that they are dealt with within the 40 day period prescribed by the Ordinance.

APPENDIX Personal Data (Privacy) Ordinance(Chapter 486)

SCHEDULE 1DATA 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

(iii) 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.

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 resonable 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).