Code of Practice on
the Identity Card Number and
other Personal Identifiers

Office of the Privacy Commissioner for Personal Data

12/F, 248 Queen's Road East, Wanchai, Hong Kong

Tel: 2827 2827

Fax: 2877 7026

December 1997

CONTENTS

INTRODUCTION

THIS CODE OF PRACTICE has been issued by the Privacy Commissioner for Personal Data ("the Commissioner") in the exercise of the powers conferred on him by section 12(1) of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Ordinance"), which empowers him to issue Codes of Practice "for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users", and pursuant to section 12(8) of the Ordinance, which provides that the Commissioner shall approve a code of practice in respect of all or any requirements of the Ordinance in so far as they relate to personal data that are personal identifiers.

This Code was identified by notice in the Gazette on 19 December 1997. The relevant Gazette Notice, as required by section 12(2), specified that the Code has been approved with effect from 19 December 1997 in relation to the following requirements of the Ordinance: section 26, Data Protection Principles 1, 2, 3 and 4 in Schedule 1.

The provisions of the Code are not legally binding. A breach of the Code by a data user, however, will give rise to a presumption against the data user in any legal proceedings under the Ordinance. Basically the Ordinance provides (in section 13) that:

(a) where a Code of Practice has been issued in relation to any requirement of the Ordinance;

(b) the proof of a particular matter is essential for proving a contravention of that requirement;

(c) the specified body conducting the proceedings (a magistrate, a court or the Administrative Appeals Board) considers that any particular provision of the Code of Practice is relevant to that essential matter; and if

(d) it is proved that that provision of the Code of Practice has not been observed;

then that essential matter shall be taken as proved unless there is evidence that the requirement of the Ordinance was actually complied with in a different way, notwithstanding the non-observance of the Code of Practice.

Aside from legal proceedings, failure to observe a Code of Practice by a data user will weigh unfavourably against the data user in any case before the Commissioner.

CODE OF PRACTICE ON THE IDENTITY CARD NUMBER AND OTHER PERSONAL IDENTIFIERS

The italicized parts in the text are guiding notes and are not themselves part of the Code.

I. DEFINITIONS

Unless the context otherwise requires, the terms used in this Code have the following meanings.

1.1 “Personal identifier” means an identifier -

(a) that is assigned to an individual by a data user for the purpose of the operations of the data user; and

(b) that uniquely identifies that individual in relation to the data user,

but does not include an individual's name used to identify that individual.

(Section 2 of the Ordinance refers.)

For the avoidance of doubt, an e-mail address is deemed not to be a personal identifier for the purposes of the Code.

1.2 “Identity card” means an identity card issued under the Registration of Persons Ordinance (Cap. 177).

1.3 “Identity card number” means the personal identifier on an identity card whether in its original or an altered form.

1.4 “Furnishing” or “provision” of a copy of an identity card may include the furnishing or provision (as the case may be) of the identity card solely to enable the making of a copy thereof immediately, to the extent such furnishing or provision in the circumstances does not constitute an offence under the Registration of Persons Ordinance (Cap.177).

Note : It is an offence under section 7AA of the Registration of Persons Ordinance for any person to transfer an identity card to another person without lawful authority or reasonable excuse.

1.5 “Copy of an identity card” means a visual representation or a reproduction of an identity card in a permanent form.

1.6 Words and expressions importing the masculine gender include the feminine, and words and expressions in the singular include the plural, and vice versa.

II. THE IDENTITY CARD NUMBER

The following paragraphs seek to give practical effect to the Personal Data Collection Limitation Principle (Data Protection Principle 1):

2.1 Unless authorized by law, no data user may compulsorily require an individual to furnish his identity card number.

2.2 Without prejudice to the generality of paragraphs 2.1 and 2.3, before a data user seeks to collect from an individual his identity card number, the data user should consider whether there may be any less privacy-intrusive alternatives to the collection of such number, and should wherever practicable give the individual the option to choose any such alternative in lieu of providing his identity card number. Such alternatives may include but are not limited to the following:

2.2.1 the identification of the individual by another personal identifier of his choice;

Note: A common example would be the furnishing of the individual's passport number.

2.2.2 the furnishing of security by the individual to safeguard against potential loss by the data user;

Note: A common example would be the furnishing of a deposit for bicycle hire.

or

2.2.3 the identification of the individual by someone known to the data user.

Note: A common example would be the identification of a visitor to a building by the tenant in the building whom he visits.

2.3 A data user should not collect the identity card number of an individual except in the following situations:

2.3.1 pursuant to a statutory provision which confers on the data user the power or imposes on the data user the obligation to require the furnishing of or to collect the identity card number;

Note 1: For an example of a statutory power to require the furnishing of ID card number, section 5 of the Registration of Persons Ordinance (Cap. 177) confers on a public officer the power to require any registered person in all dealings with Government to furnish his ID card number and, so far as he is able, the ID card number of any other person whose particulars he is required by law to furnish.

Note 2: For an example of a statutory obligation to collect an identity card number, section 17K of the Immigration Ordinance (Cap. 115) provides:

(1) Every employer shall keep at the place of employment of each of his employees a record of:-

(a) the full name of the employee as shown in his identity card or other document by virtue of which he is lawfully employable; and

(b) the type of document held by the employee by virtue of which he is lawfully employable, and the number of that document."

2.3.2 where the use of the identity card number by the data user is necessary:

2.3.2.1 for any of the purposes mentioned in section 57(1) of the Ordinance (safeguarding security, defence or international relations in respect of Hong Kong);

2.3.2.2 for any of the purposes mentioned in section 58(1) of the Ordinance (the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, etc.); or

2.3.2.3 for the exercise of a judicial or quasi-judicial function by the data user;

Note: An example of the exercise of a quasi-judicial function would be the Administrative Appeals Board hearing an appeal brought to it by an individual under the Administrative Appeals Board Ordinance (Cap.442).

2.3.3 to enable the present or future correct identification of, or correct attribution of personal data to, the holder of the identity card, where such correct identification or attribution is or will be necessary:

2.3.3.1 for the advancement of the interest of the holder;

Note: For example, a doctor may require a patient's ID card number to ensure that his past medical records are correctly attributed to him to enable better treatment.

2.3.3.2 for the prevention of detriment to any person other than the data user;

Note: The ID card number provided by a patient in the previous example may also prevent medication being given wrongly to that or some other patient as a result of misidentification.

or

2.3.3.3 to safeguard against damage or loss on the part of the data user which is more than trivial in the circumstances;

Note: For example, a driver in a motor accident may collect the ID card number of the other party to facilitate a future claim.

2.3.4 without prejudice to the generality of paragraph 2.3.3, for the following purposes:

2.3.4.1 to be inserted in a document executed or to be executed by the holder of the identity card, which document is intended to establish or to evidence any legal or equitable right or interest or any legal liability on the part of any person, other than any right, interest or liability of a transient nature or which is trivial in the circumstances;

Note: A common example would be the execution by an individual of a contract or an assignment of real property. As a counter-example, individuals who sign up in a signature campaign should not also be asked to put down their ID card numbers, as the transaction is intended not to require any present or future identification of the individual, nor involve any right, interest or liability on his part.

2.3.4.2 as the means for the future identification of the holder of the identity card where such holder is allowed access to premises or use of equipment which the holder is not otherwise entitled to, in circumstances where the monitoring of the activities of the holder after gaining such access or use is not practicable;

Note: A common example would be the entering of ID card numbers of visitors in a log-book located at the entrance of a government, commercial or residential building, subject to other alternatives for visitors to identify themselves as given in paragraphs 2.2.1 and 2.2.3 above.

or

2.3.4.3 as a condition for giving the holder of the identity card custody or control of property belonging to another person, not being property of no value or of a value which is trivial in the circumstances.

Note: A common example would be car-rental. A counter-example would be the renting of a beach umbrella, the value of which would obviously be too trivial to justify the collection of the ID card number of the customer.

The following paragraph seeks to give practical effect to the Personal Data Accuracy Principle (Data Protection Principle 2(1)):

2.4 A data user should not collect from an individual his identity card number except by:

2.4.1 means of the physical production of the identity card in person by the individual;

2.4.2 accepting the number as shown on a copy of the identity card which the individual chooses to provide rather than present his identity card in person;

Note: A data user is, however, not obliged to accept an ID card number so provided by an individual. Furthermore, where a data user has a general policy of accepting copies of identity cards provided by individuals pursuant to this paragraph, the requirements of paragraph 3.7 should be complied with.

or

2.4.3 first accepting the number as furnished, and later checking its accuracy and authenticity by means of the physical production of the identity card in person by the holder, or if that is not reasonably practicable, by means of a copy of the identity card provided by the holder, before the number is used for any purpose.

Note: For example, in the case of an application for a vacancy in the civil service, the ID card number of the applicant as shown on the application form should not be used for integrity checking until it has been verified by examination against the ID card produced by the applicant at a subsequent occasion.

The following paragraph seeks to give practical effect to section 26 and to the Personal Data Duration of Retention Principle (Data Protection Principle 2(2)):

2.5 Without prejudice to the general requirements of the Ordinance:

2.5.1 Where paragraph 2.3.4.2 applies, the data user should take all reasonably practicable steps to erase the record of an identity card number upon the holder of the identity card leaving the premises or ceasing to have the use of the equipment concerned (as the case may be), or within a reasonable time thereafter; and

2.5.2 where paragraph 2.3.4.3 applies, the data user should take all reasonably practicable steps to erase the record of an identity card number upon the holder of the identity card ceasing to have custody or control of the property concerned, or within a reasonable time thereafter.

The following paragraph seeks to give practical effect to the Personal Data Use Limitation Principle (Data Protection Principle 3):

2.6 Subject to any applicable exemption from Data Protection Principle 3 in the Ordinance, a data user who has collected the identity card number of an individual should not use it for any purpose except:

2.6.1 for the purpose for which it was collected pursuant to paragraph 2.3;

Note: Where a data user has collected an ID card number for more than one purpose pursuant to paragraph 2.3, it may use the number for any of those purposes. For example, an employer who has collected the ID number of an employee may use such number to show its compliance with the relevant statutory requirement. It may also use such number for providing medical insurance to the employee in advancement of his interest.

2.6.2 in carrying out a "matching procedure" permitted under section 30 of the Ordinance;

2.6.3 for linking, retrieving or otherwise processing records held by it relating to the individual;

2.6.4 for linking, retrieving or otherwise processing records relating to the individual held by it and another data user where the personal data comprised in those records have been collected by the respective data users for one particular purpose shared by both;

Note: For example, employees' ID card numbers may be used for the linking of their records held by different data users under the Mandatory Provident Fund system. On the other hand, customers' records held by two banks which comprise of personal data collected by each one of them for the purpose of marketing its own services should not be linked via ID card numbers contained in such records.

2.6.5 for a purpose required or permitted by any other code of practice from time to time in force under section 12 of the Ordinance; or

2.6.6 for a purpose to which the holder of the identity card has given his prescribed consent.

Note: Under section 2(3) of the Ordinance, "prescribed consent" means express consent given voluntarily which has not been withdrawn by notice in writing.

The following paragraphs seek to give practical effect to the Personal Data Security Safeguard Principle (Data Protection Principle 4):

2.7 Unless otherwise required or permitted by law, a data user should take all reasonably practicable steps to ensure that an identity card number and the name of the holder are not:

2.7.1 displayed together publicly;

Note: For example, ID card numbers should not be displayed with the names of the holders in newspaper notices, unless required or permitted by law. On the other hand, the public display of ID card numbers for the purpose of identification, without the names or other identifying particulars of the individuals concerned, would not be affected by this paragraph.

or

2.7.2 made visible or otherwise accessible together to any person, other than a person who needs to carry out activities related to permitted uses of the identity card number.

Note: For example, a visitors' log book kept at the entrance counter of a building containing the names and identity card numbers of visitors should be kept under secure conditions at all times to prevent access by any persons other than the building management in the discharge of its duties.

2.8 A data user should not issue to an individual any card (not being an identity card or driving licence) bearing in a legible form the identity card number of that individual, including such number in its original or an altered form from which it is reasonably practicable to deduce the identity card number.

Note: For example, no staff card should be issued to an employee which bears on its face the staff number of the employee, being actually his ID card number in an altered form. To enable identification of the employee in legible form by an outsider, the presence of a photograph of that employee on the card which also bears a staff number (not related to his ID card number) will be sufficient. This paragraph does not affect the issuance of cards which have the ID card numbers of the holders printed on them in bar code or other form that is not directly legible. This paragraph commences operation 6 months later than the rest of the Code (see paragraph 7.1).

III. COPY OF AN IDENTITY CARD

The following paragraphs seek to give practical effect to the Personal Data Collection Limitation Principle (Data Protection Principle 1):

3.1 Unless authorized by law, no data user may compulsorily require an individual to furnish a copy of his identity card.

3.2 A data user should not collect a copy of an identity card except:

3.2.1 where the use of the copy by the data user is necessary:

3.2.1.1 for any of the purposes mentioned in section 57(1) of the Ordinance (safeguarding security, defence or international relations in respect of Hong Kong); or

3.2.1.2 for any of the purposes mentioned in section 58(1) of the Ordinance (the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, etc.);

Note: The above-mentioned purposes include the prevention, preclusion or remedying of unlawful or seriously improper conduct, or dishonesty or malpractice, by person (section 58(1)(d) refers). This paragraph would therefore include the collection from an individual of a copy of his identity card for the prevention or detection of any collusion between the individual and the staff member of the data user handling his case, in a transaction which offers a substantial opportunity for corruption to arise, for example, the processing of an application for public housing. It would also include the collection from an individual of a copy of his identity card for the prevention or detection of impersonation by such individual using a forged, lost or stolen identity card, in a transaction where such risk is not remote, for example, in the case of a solicitors' firm acting for an individual in the sale and purchase of real property.

or

3.2.2 where the collection of the identity card number of the individual by the data user is permissible under Part II of this Code, and the copy of the identity card is collected furthermore by the data user:

3.2.2.1 in order to provide proof of compliance with any statutory requirement on the part of the data user;

Note: For example, an employer may collect a copy of the identity card of an employee as proof of compliance on the part of the employer of section 17J of the Immigration Ordinance (Cap.115), which requires the employer to inspect the ID card of a prospective employee before employing him.

3.2.2.2 in order to comply with a requirement to collect such copy as contained in any code, rules, regulations or guidelines applicable to the data user issued by a regulatory or professional body, which requirement has been endorsed in writing by the Privacy Commissioner as being in accordance with Data Protection Principle 1 of the Ordinance;

Note: For example, banks are permitted under this paragraph to collect copies of the identity card of their customers in compliance with the relevant requirement contained in the Money Laundering Guidelines issued by the Hong Kong Monetary Authority, which requirement has been endorsed in writing by the Privacy Commissioner.

3.2.2.3 as the means to collect or check the identity card number of the individual, who has been given the alternative of physical production of his identity card in lieu of collection of such copy by the data user but has chosen not to do so;

Note: A common example of such collection would be the Transport Department receiving applications for driving licence, which individuals may choose to make either in person or by post. Even where the predominant way for a data user to collect ID card numbers is through the collection of ID card copies sent to it by mail or by fax, e.g. in the case of a service provider without any retail outlets, an option should still be made available for individuals who prefer to do so to present

their ID cards in person in lieu of providing ID card copies to the data user. In the example of the above service provider, this may mean allowing customers to attend the office of the service provider to show their ID cards.

3.2.2.4 to enable the issuance of an officially recognized travel document;

or

3.2.2.5 for the exercise of a judicial or quasi-judicial function by the data user.

3.3 For the avoidance of doubt, nothing in paragraph 3.2.2 permits a data user to collect a copy of the identity card of an individual:

3.3.1 merely to safeguard against any clerical error in recording the name or identity card number of the individual;

Note: For example, while the ID card number of an individual may be recorded upon his admission to a building, his ID card copy should not be taken.

or

3.3.2 merely in anticipation of a prospective relationship between the data user and the individual.

Note: For example, while it may be justifiable for an employer to obtain the identity card number of a job applicant say for checking it against those of previous unsuccessful applicants, no ID card copy should be collected until the individual is successfully recruited.

3.4 Notwithstanding paragraph 3.2, the Immigration Department may collect a copy of the identity card for a purpose directly related to its operations where this is necessary to carry out the purpose concerned.

The following paragraphs seek to give practical effect to the Personal Data Accuracy Principle (Data Protection Principle 2(1)):

3.5 Where a data user collects a copy of an identity card from the holder in person, the data user should always check it against the identity card produced by the holder.

Note: For example, a solicitor's clerk collecting an ID card copy from a new client should always check it against the original ID card produced by the client.

3.6 Where a data user has a general policy of accepting copies of identity cards collected from the holders in person by a third party, the data user should take all reasonably practicable steps to ensure that such copies have been checked against the identity card produced by the holder upon collection by the third party.

Note: For example, in the case of the hire-purchase of a car, the finance company which accepts from the car dealer the ID card copy of a buyer should require that the car dealer has checked the ID card of the buyer before collecting the copy.

3.7 A data user who has a general policy of accepting copies of identity cards provided by individuals as the means to collecting or checking the identity card number should:

3.7.1 provide adequate training to any member of its staff responsible for collecting such copies to reasonably enable him to detect any irregularity which may appear on the face of a copy of an identity card;

3.7.2 set up a system of control whereby no copy so provided is accepted unless it has been carefully examined and no irregularity is found upon such examination;

3.7.3 ensure that for any copy so accepted and subsequently retained, there is some indication on record that it has been collected without being checked against the original identity card.

The following paragraph seeks to give practical effect to the Personal Data Use Limitation Principle (Data Protection Principle 3):

3.8 Subject to any applicable exemption from Data Protection Principle 3 provided by the Ordinance, a data user who has collected a copy of the identity card of an individual should not:

3.8.1 use the identity card number contained in the copy for any purpose except for a purpose which is permissible under paragraph 2.3 of this Code;

3.8.2 use the copy or any item of personal data contained in such copy other than the name and identity card number for any purpose, except for the purpose for which it was collected pursuant to paragraph 3.2 or 3.4 or for a purpose to which the holder of the identity card has given his prescribed consent.

Note: For example, where a securities dealer has collected the ID card copy of a client in compliance with the relevant regulations of the stock exchange, information shown on the ID card copy such as sex, date of birth etc. should not be used for direct marketing purposes. The meaning of the term "prescribed consent" is given in the note to paragraph 2.6.6.

The following paragraphs seek to give practical effect to the Personal Data Security Safeguard Principle (Data Protection Principle 4):

3.9 Save where it is required or permitted by law to do the contrary and subject to paragraph 3.10, a data user should not keep a copy of an identity card in paper form unless it is marked clearly and permanently on such copy, across the entire image of the identity card, the word "copy", or "副本" in Chinese, or other words in English or Chinese to the same effect. Where the copy is collected by the data user in the presence of the holder of identity card, such marking should be made at the time of collection in the presence of the holder.

Note: A corollary of this is that an individual who in person provides his ID card copy to a data user has the right to (and in fact should) insist on the marking of the copy being done before him.

3.10 Paragraph 3.9 does not apply to a copy of an identity card:

3.10.1 existing in a form other than paper form or pending conversion into such a form within a reasonable period;

Note: Common examples of different forms in which copies of identity cards are kept are imaged and microfilmed forms.

or

3.10.2 collected by a data user before the date on which paragraph 3.9 commences operation until such copy is used by the data user after such date.

Note: The date of commencement of operation of paragraph 3.9 is given in paragraph 7.1.

3.11 A data user who collects a copy of an identity card should ensure that such copy is treated by all staff members concerned as a confidential document, and is kept under reasonably secure conditions with access restricted to individuals who need to carry out activities related to permitted uses of the copy.

3.12 Without prejudice to the generality of paragraph 3.11, a data user should not transmit a copy or image of an identity card, nor invite the transmission to itself of such copy or image, unless it has taken all reasonably practicable steps to ensure that no individual will have access to the image or copy so transmitted except the intended individual recipient or someone acting on the instructions of such intended recipient. Such steps should include:

3.12.1 in the case of fax or Internet transmission through a public network:

3.12.1.1 wherever practicable, the employment of technological safeguards to ensure secure transmission of the data and to prevent unauthorized access to the data transmitted;

Note: Some examples of such technological safeguards currently available include encryption, fax "padlocks", "confidential mail boxes", "automatic routing to a dedicated computer directory", passwords for access, etc.

and

3.12.1.2 the employment of other safeguard of a non-technological nature, such as the using of a dedicated fax machine for such transmission and advance notification of an incoming fax; or

3.12.2 in the case of sending a copy of an identity card by mail, making sure that the copy is contained in a sealed envelope and the image of the identity card is not visible from the outside.

IV. PERSONAL IDENTIFERS OTHER THAN THE IDENTITY CARD NUMBER

The following paragraphs seek to give practical effect to the Personal Data Collection Limitation Principle (Data Protection Principle 1):

4.1 Subject to paragraph 4.2, paragraphs 2.1, 2.2 and 2.3 apply with the modifications set out in paragraph 4.3 to personal identifiers other than the identity card number in the same way as they apply to the identity card number.

4.2 Where a data user has assigned a personal identifier other than the identity card number to an individual in relation to its function or activity, such personal identifier may subsequently be collected when such collection is necessary for a purpose that is directly related to that function or activity.

Note 1: This allows a data user that has assigned a personal identifier to an individual to collect that personal identifier for a purpose that is directly related to its operations. For example, a company may assign an employee number to its employees, which it may record for security purposes each time an employee enters or leaves a restricted area within the company premises.

Note 2: The paragraph also allows other persons to collect the personal identifier for purposes that are directly related to the operations of the assigning data user. For example, where a company dispatches an employee to a private household to carry out a service, the householder may record the employee number of the service engineer in order to identify the employee in, say, subsequent communication with the company.

4.3 The modifications referred to in paragraphs 4.1, 4.4, 4.6 and 4.7 are as follows:-

4.3.1 references to "identity card number" are to be construed as references to "personal identifiers other than the identity card number";

4.3.2 references to the "holder" of an identity card are to be construed as references to "the individual to whom the personal identifiers relates";

4.3.3 references to "identity card" are to be construed as references to "the original of the identification document, if any, to which the personal identifier in question relates".

Note: The identification document to which a personal identifier relates is the document issued to the individual for identification purposes containing the personal identifier concerned, e.g. a passport in relation to a passport number.

The following paragraphs seek to give practical effect to the Personal Data Accuracy Principle (Data Protection Principle 2(1)):

4.4 Subject to paragraph 4.5, paragraph 2.4 applies with the modifications set out in paragraph 4.3 to personal identifiers other than the identity card number in the same way it applies to the identity card number.

4.5 Paragraph 2.4 as modified by paragraph 4.3 does not apply to the collection of a personal identifier pursuant to paragraph 4.2.

The following paragraph seeks to give practical effect to section 26 and to the Personal Data Duration of Retention Principle (Data Protection Principle 2(2)):

4.6 Paragraph 2.5 applies with the modifications set out in paragraph 4.3 to personal identifiers other than the identity card number in the same way as they apply to the identity card number.

The following paragraphs seek to give effect to the Personal Data Use Limitation Principle (Data Protection Principle 3):

4.7 Subject to paragraph 4.8, paragraph 2.6 applies with the modifications set out in paragraph 4.3 to personal identifiers other than the identity card number in the same way as it applies to the identity card number.

4.8 A personal identifier other than the identity card number may be used for the purpose for which it was collected pursuant to paragraph 4.2.

V ALL PERSONAL IDENTIFIERS (INCLUDING THE IDENTITY CARD NUMBER)

The following paragraph seeks to give practical effect to the Personal Data Security Safeguard Principle (Data Protection Principle 4):

5.1 A data user shall take all reasonably practicable steps to ensure the security of any system it controls for assigning a personal identifier to an individual. Such steps shall include all reasonably practicable measures to safeguard against the unauthorised assignment of the personal identifier to an individual and to prevent the unauthorised production of the identification documents, if any, it issues bearing the personal identifier that it assigns to individuals.

VI EXCLUSIONS

For the avoidance of doubt, the following paragraph expressly excludes from the coverage of the Code personal identifiers (including the identity card number) in certain situations.

6.1 The following are not subject to the foregoing sections of the Code:-

6.1.1 any record of a personal identifier or copy of an identity card held by an individual for purposes directly related to the management of the individual's personal, family or household affairs or for the individual's recreational purposes;

6.1.2 a personal identifier assigned to an individual who is deceased; and

6.1.3 a personal identifier being furnished without being recorded.

VII COMMENCEMENT DATE

The following paragraph provides for the date of commencement of operation of the provisions of the Code.

7.1 The provisions of the Code, with the exception of paragraph 2.8, shall commence operation 6 months after the date of approval of the Code, i.e. on 19 June, 1998. Paragraph 2.8 of the Code shall commence operation 12 months after the date of approval of the Code, i.e. on 19 December, 1998.

APPENDIX I

Personal Data (Privacy) Ordinance

Schedule 1

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).

APPENDIX II

Personal Data (Privacy) Ordinance

Sections 26, 57(1) & 58(1)

26. Erasure of personal data no longer required

(1) A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless -

(a) any such erasure is prohibited under any law; or

(b) it is in the public interest (including historical interest) for the data not to be erased.

(2) For the avoidance of doubt, it is hereby declared that -

(a) a data user shall erase personal data in accordance with subsection (1) notwithstanding that any other data user controls (whether in whole or in part) the processing of the data;

(b) the first-mentioned data user shall not be liable in an action for damages at the suit of the second-mentioned data user in respect of any such erasure.

57. Security, etc. in respect of Hong Kong

(1) Personal data held by or on behalf of the Government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to prejudice any of the matters referred to in this subsection.

58. Crime, etc.

(1) Personal data held for the purposes of -

(a) the prevention or detection of crime;

(b) the apprehension, prosecution or detention of offenders;

(c) the assessment or collection of any tax or duty;

(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(e) the prevention or preclusion of significant financial loss arising from-

(i) any imprudent business practices or activities of persons; or

(ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(f) ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on any thing -

(i) to which the discharge of statutory functions by the data user relates; or

(ii) which relates to the discharge of functions to which this paragraph applies by virtue of subsection (3); or

(g) discharging functions to which this paragraph applies by virtue of subsection (3),

are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to -

(i) prejudice any of the matters referred to in this subsection; or

(ii) directly or indirectly identify the person who is the source of the data.