G.N. 2205

PERSONAL DATA (PRIVACY) ORDINANCE (Chapter 486)

(Notice under Section 12(2))

APPROVAL OF REVISED CODE OF PRACTICE

Under sections 12(1) and (2) of the Personal Data (Privacy) Ordinance (hereinafter referred to as "the Ordinance"), the Privacy Commissioner for Personal Data (hereinafter referred to as "the Commissioner") may, for the purpose of providing practical guidance in respect of any requirements under the Ordinance imposed on data users, approve and issue such codes of practice as in his opinion are suitable for that purpose, and by notice in the *Gazette* identify such codes of practice.

On 22 September 2000, the Commissioner issued by notice in the *Gazette* a code of practice entitled 'the Personal Data (Privacy) Ordinance Code of Practice on Human Resource Management'. The said code of practice took effect on 1 April 2001.

Notice is hereby given that consequential amendments are made to the said code of practice under section 12(3) of the Ordinance to effect various amendments made to the Ordinance pursuant to the Personal Data (Privacy) (Amendment) Ordinance 2012, which took effect on 1 October 2012. The revised version of 'the Personal Data (Privacy) Ordinance Code of Practice on Human Resource Management' is issued and approved by me in respect of the requirements of sections 18, 19, 20, 22, 23, 24, 25, 26 and the six data protection principles in Schedule 1 of the Ordinance. The revised code of practice as set out below takes effect on 22 April 2016 and henceforth replaces and supersedes the previous code of practice issued on 22 September 2000.

Code of Practice on Human Resource Management

Office of the Privacy Commissioner for Personal Data, Hong Kong
12/F, Sunlight Tower, 248 Queen's Road East,
Wanchai, Hong Kong

Tel: (852) 2827 2827
Fax: (852) 2877 7026
Website: www.pcpd.org.hk
Email: enquiry @pcpd.org.hk

First published in September 2000 (effective on 1 April 2001)
April 2016 (First Revision)

Table of Contents

Introduction

THIS CODE OF PRACTICE ("the Code") has been issued by the Privacy Commissioner for Personal Data ("the Commissioner") in the exercise of the powers conferred on him by Part III of the Personal Data (Privacy) Ordinance (Cap. 486 "the Ordinance"). Section 12(1) of the Ordinance empowers the Commissioner to issue codes of practice "for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users."

This Code was first notified by Gazette of the Hong Kong SAR Government on 22 September 2000. The related Gazette Notice, as required by section 12(2) of the Ordinance, specified that the Code took effect on 1 April 2001 and was approved in relation to the following requirements of the Ordinance: Sections 18, 19, 20, 22, 23, 24, 25, 26 and the six Data Protection Principles in Schedule 1.

This Code was revised and notified by Gazette in April 2016. The revision was necessitated by the amendments of the Ordinance and to update the provisions of the Code that were spent of effect.

The primary purpose of this Code is to provide practical guidance to employers and their staff on how to properly handle personal data that relate to each phase of the employment process. Failure to abide by the mandatory provisions of this Code will weigh unfavorably against the data user concerned in any case that comes before the Commissioner. Where any data user fails to observe any of the mandatory provisions of this Code, a court, a magistrate, the Administrative Appeals Board or the chairman of the Administrative Appeals Board, is entitled to take that fact into account when deciding whether there has been a contravention of the Ordinance.

♦♦♦

This Code is designed to give practical guidance to data users who handle personal data in performing human resource management functions and activities. It deals with issues concerning collection, holding, accuracy, use and security, and data subject access and correction in relation to the personal data of prospective, current and former employees.

The provisions of the Code apply to data users who are employers of individuals relating to their prospective, current or former employment with the employers concerned.

Interpretation

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

"DPP" means a data protection principle in Schedule 1 to the Ordinance.

"Employer" means any person who has entered into a contract of employment to employ any other person as an employee and the duly authorised agent of such first mentioned person;

"Employment" is deemed to include the engagement of an individual whose service is procured through a contract with a third party which employs such individual, and the terms "employ", "employer" and "employee" are to be construed accordingly.

"Ordinance" means the Personal Data (Privacy) Ordinance.

"Personal Information Collection Statement" ("PICS") means a statement made to an individual in respect of whom personal data is collected by the person providing the statement in compliance with the requirements of DPP1(3).

"Permitted purpose" in relation to personal data means a lawful purpose directly related to an employer's functions or activities for which the data was to be used at the time of their collection; a directly-related purpose for which the data was or is used; the fulfillment of a relevant statutory requirement; or a purpose for which the data was or is used where the data subject has given express consent to that use.

"Practicable" means reasonably practicable.

"Prescribed consent" is the express consent of the person[1] given voluntarily, which has not been withdrawn by notice in writing.

Using this Code

It is recommended that readers begin by carefully reading the Code as a whole to understand all elements of its use as it applies to the personal data of job applicants, employees and former employees. Subsequently, when a specific question needs to be answered in relation to a matter covered by the Code, the reader should first refer to Section 1 which contains general requirements for handling employment-related personal data, and then the particular subsequent section dealing with the specific area of interest. If this approach is used, the reader should acquire a better understanding of the matter.

In this document, the contents of the Code are arranged to indicate which parts of the text are mandatory, and which are illustrative or explanatory as follows:

The mandatory provisions of the Code are printed in normal typeface.

The sections in *italics* give general explanatory notes, examples and specify good practices. These sections amplify the Code to assist the reader in complying with the mandatory provisions of the Code.

The footnotes provide specific references to the provisions of the Ordinance or other sources

[1] Under DPP3(2), a relevant person may give prescribed consent on behalf of a data subject when certain conditions are fulfilled.

that provide the statutory basis e.g. other codes of practice, for the particular requirements of the Code.

1 General Requirements

1.1 Introduction

Section 1 reviews a range of topics relating to the general practices and policies that an employer should give consideration to when collecting, processing and handling employment-related personal data. Other matters relating to specific aspects of human resource management, such as recruitment, current and former employees' matters are dealt with in subsequent sections.

More specifically, this section details the following:

1.1.1 Notification requirements on collection of personal data - PICS.
1.1.2 Issues pertaining to the accuracy and retention of employment-related personal data.
1.1.3 Security measures for protection of employment-related personal data.
1.1.4 Data access and correction requests concerning recruitment-related or employment-related personal data.
1.1.5 Employer's liability pertaining to the wrongful conduct of its staff or an appointed agent in handling personal data.

1.2 Notification Requirements on Collection of Personal Data

Statements to be Made on or before Collecting Employment-related Personal Data

1.2.1 When an employer collects personal data from a job applicant or employee, the employer should take all practicable steps to explicitly inform the individual on or before collecting the data of the following information:[1]

1.2.1.1 the purpose for which the data is to be used;
1.2.1.2 the classes of persons to whom the data may be transferred; and
1.2.1.3 whether it is obligatory or voluntary for the individual to supply the data unless this is obvious from the circumstances.

On or before using the data, an employer should explicitly provide the following information to the individual concerned:

1.2.1.4 the rights of the individual to request access to, and correction of, his personal data and the name or job title, and address, of the person to whom such requests should be made.

[1] DPP1(3)

As a matter of good practice, an employer should comply with the above notification requirements by means of a written PICS. This statement may, for example, be attached to, or be printed as an integral part of standard employment forms used to collect data e.g. a job application form.

The following list provides examples of occasions when it would be appropriate to make such statements.

- *In recruitment advertisements where an employer requests that résumés, or other personal data, be submitted by job applicants.*
- *On an Internet page where an employer invites job applicants to complete a form and submit online.*
- *On an employer's printed job application form or any other data collection forms specified by the employer that requires the provision of personal data.*

Purpose Statement : Purpose for which Personal Data is to be Used

1.2.2 An employer may state the purposes for which employment-related personal data is to be used in general or specific terms.[1]

Many of the purposes for which personal data is to be collected are common to most employers. Examples of common purposes for which personal data is collected from employees include information required: to pay employees and to make compensation, benefits and awards, to contact employees when absent from the office, to make tax returns, to assess employees' training and development needs, to plan promotion and to administer a retirement or provident fund scheme to which employees contribute and from which they may benefit.

The accompanying examples may be used as a starting point from which employers may prepare more specific statements of purposes, adapted to their own needs, to be included in their PICS.

Purpose of Collection – Job Applicants

To assess the suitability of candidates for a vacancy within the organisation, and to negotiate with and make offers of employment to selected applicants.

Purpose of Collection – Employees

For the supervision, management and payment of employees, to develop and maintain the employment relationship between the employer and the individual, and to support the organisation's development.

For any residual employment-related activities of an employer in respect of an employee, including the provision of job references, processing of applications for re-employment and any matter relating to pension or retirement scheme payments.

Transferee Statement : Classes of Transferees

1.2.3 An employer should explicitly inform job applicants or employees of the classes of third parties to which any of their personal data may be transferred. An employer must do this on or before collecting the data.[2]

[1] DPP1(3)(b)(i)(A)
[2] DPP1(3)(b)(i)(B)

Examples of common classes of transferees include the employer's insurers, bankers, medical practitioners providing medical services for employees, staff unions and provident fund managers. Before collecting the relevant personal data it is necessary for an employer to inform staff of such possible transfers. Government departments to which an employer is required by law to transfer relevant personal data, for example the Inland Revenue Department, need not be included in a statement of such third parties.

Classes of Transferee

The data that you have supplied for the purpose of employment may be passed to the employer's insurers, bankers, medical practitioners providing medical services to employees, any relevant staff union and provident fund managers.

It should be noted that an employer should state that any transfer of employment-related personal data to one of the named classes of possible transferees will be for one or other of the purposes stated in the Purpose Statement, or a directly related purpose. Because the transfer notification requirements only apply to transfers to third parties outside the employing organisation, there is no requirement for employers to name other internal departments or employees of the employer to whom personal data may be transferred for the purposes of employment.

Optional or Obligatory Provision of Data

1.2.4 Unless it is obvious from the circumstances, an employer should explicitly inform job applicants or employees, whether it is obligatory or voluntary to supply personal data.[1] The consequences of not providing such data should also be stated explicitly unless this is obvious from the circumstances.[2]

An employer needs not provide a notice of whether it is compulsory to provide personal data if it is obvious from the circumstances that all the employment-related personal data sought in a form used by an employer must be provided and that if any item is not provided the matter concerned will not be processed further.

Omission of Personal Data

The provision of full and complete information in support of a job application is necessary for selection purposes. Failure to provide any of the data may affect the processing and outcome of the application.

For example, on a staff leave application form, it is not necessary for an employer to state that it is compulsory to provide personal data such as the days of intended absence in order for the application to be processed and approved.

Data Access and Correction Rights

1.2.5 An employer, on or before the first use of the employment-related data, should explicitly provide information of an individual's rights of access to, and correction of, his personal data and the contact details of the person to whom any such request may be made.[3]

[1] DPP1(3)(a)(i)
[2] DPP1(3)(a)(ii)
[3] DPP1(3)(b)(ii)(A) and DPP1(3)(b)(ii)(B)

The Ordinance confers upon an individual whose personal data is held by an employer a right to request a copy of such data. Subsequently, the individual concerned is entitled to request correction of any inaccurate data provided in compliance with such a request.

An employer should also include the name or job title and address of a person to whom the request may be made.

Data Access & Correction Rights

You have a right under the Ordinance to make a data access or correction request concerning your personal data. You may make such requests by applying to the Privacy Compliance Officer in the Human Resources Department.

Employment-related Personal Data Collected before the Ordinance came into Effect

1.2.6 An employer may continue to use employment-related personal data collected before 20 December 1996[1] as long as the purposes for which the data is used come within the reasonable scope of the purposes for which the data was originally collected. Any use of such data outside the original scope of collection will require the prescribed consent of the individual concerned.[2]

Employment-related data collected prior to 20 December 1996 may be used for the implicit purpose for which it was collected, which may be inferred from the nature of the transaction involved e.g. recruitment or administering the employment of the individual who provided the data. As a matter of good practice, an employer should consider providing an employee with its PICS at the first opportunity where new data is collected from the employee.

1.3 Accuracy and Retention of Employment-related Personal Data

Accuracy of Employment-related Data

1.3.1 An employer should take all practicable steps to ensure that the employment-related data it holds about employees is:

1.3.1.1 accurate having regard to the purpose for which the data is used;[3] or

1.3.1.2 not used for the purpose where there are reasonable grounds for believing that the data is inaccurate when used for that purpose, unless and until such inaccuracies are rectified.[4]

1.3.2 An employer who discloses or transfers employment-related data to a third party on or after 20 December 1996 should take all practicable steps to ensure that:

[1] The date the relevant provisions of the Ordinance first came into effect.
[2] DPP3
[3] DPP2(1)(a)
[4] DPP2(1)(b)

1.3.2.1 the data thereby disclosed or transferred is accurate having regard to the purpose for which the data is disclosed or transferred; and

1.3.2.2 where it is practicable in all circumstances to know that the data was inaccurate at the time of such disclosure or transfer, the recipient is informed of the inaccuracy and is provided with such particulars as will enable the recipient to rectify the data.[1]

Retention of Employment-related Data

1.3.3 An employer should implement a written data retention policy that specifies a retention period of:

1.3.3.1 no longer than two years in respect of recruitment-related data held about a job applicant from the date of rejecting the applicant;

1.3.3.2 no longer than seven years in respect of employment-related data held about an employee from the date the employee leaves employment;

Unless

1.3.3.3 the individual concerned has given express consent for the data to be retained for a longer period; or

1.3.3.4 there is a subsisting reason that obliges the employer to retain the data for a longer period.

The provisions of the four anti-discrimination ordinances - the Disability Discrimination Ordinance, the Family Discrimination Ordinance, the Sex Discrimination Ordinance and the Race Discrimination Ordinance permit an individual to make a claim to the District Court against another person for an act of discrimination against him before the end of the period of two years beginning (a) when the act complained of was done; or (b) if there is a relevant report in relation to the act, the day on which the report is published or made available for inspection.

Further guidance in respect of the above requirements is given in Section 2 on Recruitment and in Section 4 on Former Employees' Matters.

1.4 Security Measures to Protect Employment-related Data

Measures to Ensure Integrity, Prudence and Competence of Employees

1.4.1 An employer should take reasonably practicable measures to ensure that staff handling employment-related personal data are trained to observe the employer's personal data privacy policies, exercise due diligence in the application of those policies, and are subject to procedures designed to ensure their compliance with those policies.[2]

[1] DPP2(1)(c)
[2] DPP4(1)(d)

Employees play the principal role in implementing an employer's policies on the security of personal data. Security practices are therefore a vital part of any human resources policy with regard to privacy of personal data.

In evaluating internal procedures pertaining to the security of employment-related personal data, employers should determine the extent to which their policies satisfy the following criteria:

- *Policy relating to the security of employment-related personal data is systematically and regularly communicated to staff authorised to access and process that data.*
- *The employer commits to, and provides, on-going training to staff on matters relating to personal data protection.*
- *New recruits to the organisation are provided with training on personal data protection as part of their induction into the organisation.*
- *Employer's policy manuals, training materials, and employee handbook are periodically reviewed to ensure that they are consistent with the requirements under the Ordinance and any codes of practice in force.*
- *In-house policy is to restrict access to, and processing of, personal data on a "need-to-know" and "need-to-use" basis.*
- *As a matter of protocol, staff involved in accessing and processing employment-related personal data are required to sign a secrecy or confidentiality statement that clearly specifies operational expectations in these respects.*
- *Appropriate investigative procedures are engaged should such protocols be breached and action taken against staff found to have violated the terms and conditions of the confidentiality statement.*
- *Random checks are made to ensure that there is compliance with established procedures.*

Security through Controlled Access to Employment-related Personal Data

1.4.2 If an employer makes any employment-related data available internally, it should take appropriate measures to protect the data against unauthorised or accidental access, processing, erasure, loss or use of that data.[1]

As a matter of good practice, employers should ensure that access to personal data held on an automated system is regulated by security features. For example, such features may include the use of account names and passwords; dedicated terminals; an audit trail or installed warning feature that can detect unsuccessful attempts to access data; and automatic log-off after a timed period of inactivity. Further precautions may include prohibiting unauthorised copies of employment-related personal data from being established on distributed computers, such as stand alone PCs, that are not subject to the controls applied to authorised copies.

1.4.3 If an employer engages a third party to perform any of its human resource management functions, it must adopt contractual or other means to ensure that the third party applies appropriate security protection to the employment-related data.[2]

[1] DPP4(1)
[2] DPP4(2)

It should be noted that the Ordinance imposes legal liability on an employer in relation to any wrongful acts or practices done by a third party where the third party is engaged as an agent acting on behalf of the employer.[1] *For example, an employer without suitable storage or disposal facilities may arrange for large volumes of employment-related personal data to be stored or destroyed by a reputable storage or waste disposal company. The employer should include in its agreement with such a company appropriate precautions controlling the handling of the materials including, in particular, conditions that ensure security and confidentiality.*

1.4.4 An employer should ensure that the physical destruction of documents containing employment-related data held on paper or other non-erasable media is undertaken with appropriate security precautions, to avoid their inadvertent disclosure to, or access by, unauthorised parties prior to destruction.

As a matter of good practice, an employer should note that the destruction of personal data that is no longer required will generally necessitate special arrangements to be put in place within the organisation for the collection and consolidation of such data prior to its disposal. For example, waste for secure disposal may be collected in special containers in a controlled area accessible only to staff authorised to handle personal data of the type being disposed of.

Precautions and Other Matters Regarding Internet Usage

1.4.5 An employer should take all practicable steps to implement appropriate data protection measures to ensure the secure transmission of employment-related data on a public network such as the Internet.[2]

Data travelling on the Internet is vulnerable to unauthorised interception or access. Depending on the sensitivity of the data to be transmitted, appropriate security protection software should be installed to enhance the integrity of data. For example, software encryption or digital signature used in email transmission would be an acceptable form of protection to safeguard data integrity and authentication. In addition, security protection measures should also be implemented on computers that are used for sending or receiving email containing personal data. Staff should be reminded to ensure all copies of email are held securely to prevent accidental or unauthorised access.

1.4.6 If an employer provides Internet access facilities, including email, for the use of its employees, it should inform the employees of its written policy on the use of the system.

As a matter of good practice, the policy referred to above should include matters such as:

- *Whether the use of the email system by employees for sending and receiving personal email is permitted and any special arrangements that employees should adopt for segregating personal email from work-related email.*
- *Whether the employer reserves the right to access and read email sent and received by employees using the email system.*

[1] Section 65(2)
[2] DPP4(1)(e)

- *Specific rules that apply to the distribution of incoming or outgoing email and the erasure of unnecessary email that contain personal data or have an attachment that includes such data.*

1.5 Complying with Data Access and Correction Requests

Data Access Requests of Employment-related Data

1.5.1 An individual whose personal data is held by his employer is entitled to request to be given a copy of such data.[1] Unless exempted from doing so under the Ordinance, the employer is required to provide a copy of the requested data within 40 days after receiving a data access request.[2] In the event of an employer being unable to provide the copy within the 40-day limit, the employer must communicate that fact in writing to the person making the request before the expiry of that period and must provide the copy as soon as practicable thereafter.[3]

1.5.2 An employer responding to a data access request from a job applicant, current or former employee must not disclose to the individual seeking access any data identifying any other individual unless that other individual consents.[4]

1.5.3 Where one document contains the personal data of two or more individuals, an employer may not refuse to comply with a data access request from one or more individuals where it is possible not to disclose the identities of the others by the omission of names or other identifying particulars.[5]

For example, an employee who is the subject of a disciplinary proceeding has a right to request a copy of the disciplinary records such as a disciplinary board's minutes of a meeting that is conducted for the purpose of the disciplinary investigation. The employer cannot rely on the fact that the document contains personal data of a third party, other than the employee, to refuse to provide a copy of the minutes. In this circumstance, the employer should edit out the information relating to the third party before providing a copy to the employee if no consent is given by the third party concerned of its disclosure. Similarly, it is not a valid reason for the employer to refuse access to a promotion board report merely because the document contains a comparison of two or more employees where it is possible to conceal the identities of the others by the omission of names or other identifying particulars.

As a matter of good practice employers should implement measures to ensure that they can comply with a data access request made by a job applicant, current or former employee. Those measures should seek to satisfy the following criteria:

- *The employer has established tracking procedures to monitor the progress of compliance with data access requests.*
- *In complying with a data access request the employer should:*

[1] Section 18
[2] Section 19(1)
[3] Section 19(2)
[4] Section 20(1)(b) and 20(2)(a)
[5] Section 20(1)(b) and 20(2)

- *not withhold any personal data of the requestor unless a lawful exemption applies to the circumstances of the case;*
- *reply to the data access request in writing within 40 days of receipt of the request;*
- *clearly specify what fees, if any, will be charged for providing the requestor with a copy of his/her record of personal data;*
- *provide the relevant data in a form that is intelligible to the data subject;*
- *erase from the copy any reference of personal data of a third party individual unless that third party has consented to its disclosure;*
- *erase from the copy all names or other identifying particulars that explicitly identify a third party individual as the source of the personal data relating to the requestor.*

- *Where the employer is unable to comply with the data access request within 40 days he should, before that time has elapsed:*

  - *comply with the data access request in part, so far as it is practicable to do so;*
  - *inform the requestor in writing, explaining why he is unable to comply fully with the request;*
  - *fully comply with the request as soon as practicable thereafter.*

Data Correction Requests of Employment-related Data

1.5.4 An employee who has been provided with a copy of personal data held by his employer in compliance with a data access request is entitled to request the employer to make the necessary correction in respect of any data that the employee considers to be inaccurate.[1] If satisfied that the data is indeed inaccurate, the employer is required to make the necessary correction and provide the employee with a copy of the corrected data within 40 days of receiving the request.[2]

1.5.5 An employer who, pursuant to a permitted circumstance under the Ordinance, refuses to make the necessary correction in relation to a data correction request, should inform the requestor in writing of the refusal and the reasons for such refusal.[3]

For example, if the correction requested relates to data, whether a fact or an expression of opinion and the employer is not satisfied that the data is inaccurate, it may refuse to make the correction. An "expression of opinion" includes an assertion of fact that is unverifiable or, in all circumstances of the case, is not practicable to verify. However, the employer should inform the requestor in writing of the refusal and the reasons for such refusal. In the case of the data being an expression of opinion, the written refusal should be accompanied by a copy of a note containing matters referred to in the correction request. This note should be annexed to the file of the individual concerned so that anyone having access to it may have the contents of the note brought to their attention.

[1] Section 22(1)
[2] Section 23(1)
[3] Sections 24(3) and 25(1)(a)

1.6 Employer's Liability for Wrongful Acts or Practices by its Employees or Agents

1.6.1 An employer is liable in civil proceedings for any act or practice relating to personal data that is undertaken by its employees in the course of their employment that is contrary to the provisions of the Ordinance, even if the employees undertook the act or engaged in the practice without the employer's knowledge or approval.[1]

1.6.2 An employer is liable in civil proceedings for any wrongful acts or practices done by a third party where the third party is engaged as an agent acting with authority (whether express or implied, and whether precedent or subsequent) on behalf of the employer.[2]

1.6.3 The employer may avoid liability only if the employer is able to prove that it took such steps as were reasonably practicable to prevent the wrongful acts undertaken or practices engaged in by its employee who acted on its behalf.[3]

For example, if an employee disclosed employment-related personal data to a third party contrary to DPP3, the employer may be able to avoid liability for the wrongful disclosure if it can prove that the employee had ignored a departmental policy that prohibited disclosure to a third party.

1.7 Other Matters

Statutory Requirements in Relation to Employment-related Data

1.7.1 Where ordinances other than the Ordinance impose upon an employer obligations to keep certain employment-related information, and to disclose such information to the relevant authorities when required, the employer should comply with the obligation as stated.

For example, under the Immigration Ordinance an employer is required to keep a record of the type of identification document held by an employee by virtue of which the employee is lawfully employable, and the number of that identification document. The employer is also required to disclose such information when requested by a labour inspector.

Information about Policies and Practices to be Made Available

1.7.2 An employer should take all practicable steps to ensure that the public at large and its employees can be provided with a copy of its policies and practices in relation to personal data.[4]

---

[1] Section 65(1)
[2] Section 65(2)
[3] Section 65(3)
[4] DPP5

As a matter of good practice, an employer should comply with the above requirement by means of a written Privacy Policy Statement ("PPS") that details its personal data management policies and practices. The PPS should include a list of the kinds of personal data held by the employer as well as the main purposes for which such data is used. The employer should also consider including other data protection policies and practices such as its data retention policy and security protection policy.

Matters Concerning the Hong Kong Identity Card Number in Employee Records

1.7.3 The Code of Practice on the Identity Card Number and Other Personal Identifiers ("the PI code") makes provisions whereby an employer may:

1.7.3.1 collect the Hong Kong Identity Card number of a job applicant when certain criteria are met;[1]

1.7.3.2 collect a copy of the Hong Kong Identity Card of a selected candidate at the time the candidate accepts an offer of employment;

1.7.3.3 collect the Hong Kong Identity Card number and copy of the Hong Kong Identity Card of an employee;[2] or

1.7.3.4 use Hong Kong Identity Card numbers in a computer or manual system to link, retrieve or otherwise process records of employment-related data within the organisation.[3]

1.7.4 An employer must check any copy of the Hong Kong Identity Card against the original card[4] and mark it with the word "COPY" across the entire image of the Hong Kong Identity Card.[5] Such a copy collected before 19 June 1998 needs not be so marked until it is first used after that date.

1.7.5 An employer issuing staff cards, pensioner's cards, employee club cards etc. to its employees or former employees, should not issue any such cards bearing the holder's Hong Kong Identity Card number.[6]

[1] Paragraph 2.3.1 of the PI code
[2] Paragraphs 2.3.1 and 3.2.2.1 of the PI code
[3] Paragraph 2.6.3 of the PI code
[4] Paragraph 3.5 of the PI code
[5] Paragraph 3.9 of the PI code
[6] Paragraph 2.8 of the PI code

2 Recruitment

2.1 Introduction

2.1.1 Employers often commence the recruitment process by specifying a job description or candidate specification. Various means may be employed in the collection of personal data from job applicants. These may include:

2.1.1.1 Requiring job applicants to fill in a job application form.
2.1.1.2 Inviting job applicants to submit an application in response to a job advertisement.
2.1.1.3 Obtaining job applicants' personal data via employment agencies or an executive search company.
2.1.1.4 Relying on job applications that are collected in the course of a previous recruitment exercise.

2.1.2 An employer may have a practice of inviting job applicants to submit applications in response to a job advertisement posted on the employer's website by filling in an online data collection form or by email. In these circumstances, the employer also engages in a practice that amounts to the collection of personal data from applicants.

2.1.3 In addition to the data collected through the original application, an employer may, in the course of the recruitment selection process, compile additional information about job applicants to assess the suitability of candidates for the job. Such information may include:

2.1.3.1 A written assessment of the candidate recorded in a selection interview.
2.1.3.2 An assessment report of any tests that the candidate is required to undertake, such as psychological tests.
2.1.3.3 Personal references obtained from the candidate's current or former employers or other sources.

2.1.4 The Ordinance requires an employer to take all practicable steps to ensure that job applicants are informed, on or before collection, of certain matters relating to the collection of their personal data.[1] This requirement applies to paragraphs 2.1.1.1, 2.1.1.2, 2.1.2 and 2.1.3. The notification requirement can be made in the form of a written PICS, either as a separate statement for recruitment, or as an integral part of a more detailed PICS pertaining to employment.

[1] DPP1(3)

Practical Guidance on Recruitment-related Practices

2.2 Collection of Personal Data from Job Applicants

2.2.1 An employer should not collect personal data from job applicants unless the purpose for which the data is to be used is lawful.[1]

For example, an employer should not use a vacancy notice to solicit the submission of personal data by candidates for the purpose of unlawfully discriminating against them on grounds of gender or marital status with the intention of excluding female employees from supervisory positions.

2.2.2 An employer should not collect personal data from job applicants unless the data is adequate but not excessive in relation to the purpose of recruitment.[2]

In determining which data is regarded as relevant, an employer should be mindful of the need to demonstrate that the prescribed personal data is indeed directly related to the purpose of identifying suitable candidates. Careful selection of relevant data in the job description or candidate specification will minimise the likelihood of personal data being collected from job applicants that is excessive for the recruitment purpose.

For example, the job description or specification should be restricted to the collection of personal data relevant to the recruitment exercise, and for the purpose of identifying suitable candidates for the job. Generally, these may include work experience, job skills, competencies, academic/professional qualifications, good character and other attributes required for the job.

2.2.3 An employer may collect the Hong Kong Identity Card number of a job applicant only if all of the following requirements are satisfied:[3]

2.2.3.1 the employer has a general policy to retain the Hong Kong Identity Card numbers of former employees and unsuccessful job applicants for a certain period;

2.2.3.2 the employer collects Hong Kong Identity Card numbers because it is necessary for the correct identification of individuals or for the correct attribution of records it holds relating to the applicants;

2.2.3.3 the employer conducts checks of whether any particular job applicant has applied for a position with it before, or is a former employee, and a large number of applicants or former employees may be involved; and

2.2.3.4 there is no less privacy-intrusive and practicable alternative of correctly identifying or attributing records to such individuals.

2.2.4 An employer should not collect a copy of the Hong Kong Identity Card of a job applicant during the recruitment process unless and until the individual has accepted an offer of employment.[4]

---

[1] DPP1(1)(a)
[2] DPP1(1)(c)
[3] PI Code
[4] Paragraph 3.3.2 of the PI Code

Paragraph 3.3.2 of the PI Code prohibits a data user from collecting a copy of the Hong Kong Identity Card of an individual merely in anticipation of a prospective relationship between the data user and the individual.

2.2.5 An employer may collect personal data concerning a job applicant's family members, if the personal data:

2.2.5.1 relate to employment circumstances of the applicant's family members only to the extent necessary for assessing whether any conflict of interest might arise should the applicant be offered the job; and

2.2.5.2 are adequate but not excessive in relation to this purpose.

For example, if an employer wishes to know whether a job applicant's family members are currently employed by a competitor, it should confine itself to asking whether this is the case and making further enquiries only in relation to any family members that are so employed. As a matter of good practice, an employer should consider collecting the data no earlier than at the time when the applicant is considered as a potential candidate for appointment.

2.2.6 Where an employer requires job applicants to fill in a job application form, either in a paper format or online on a webpage of the employer's website, it should ensure that the PICS notification requirement mentioned in paragraph 2.1.4 is complied with.[1]

A practical way to comply with the notification requirement is to print the PICS as an integral part of the paper application form or display it as part of the text of the online form. Alternatively, the PICS may be attached as a separate sheet to the paper application form. In the case of the online form, this can be done by displaying the PICS as a linked page to the online form or as a "pop-up" screen when a "confirm" button is pressed prior to the transmission of the online form.

2.3 Advertising of Job Vacancies

2.3.1 An employer who advertises an employment vacancy in a vacancy notice that directly solicits the submission of personal data by interested individuals thereby starts the process of collecting personal data of those individuals. Accordingly, the requirements mentioned in paragraphs 2.2.1 to 2.2.5 would apply for the purpose of this section.

It should be noted that if the vacancy notice merely invites interested individuals to contact an employer, there is no direct solicitation of personal data. An example would be where an employer advertises the job vacancy requirements and invites interested individuals to write in to obtain an application form in relation to the vacancy.

[1] DPP1(3)

2.3.2 Where an employer advertises a vacancy in a vacancy notice that directly solicits the submission of personal data by job applicants, it should ensure that the PICS notification requirement, mentioned in paragraph 2.1.4, is complied with in the advertisement [1] unless:

2.3.2.1 the advertisement invites job applicants to respond by filling in a job application form specified by the employer that prescribes the PICS notification; or

2.3.2.2 the advertisement expressly identifies the contact person from whom applicants may obtain a copy of the PICS.

For example, an employer may state in the vacancy notice the telephone number, name or title of the employer's nominated person from whom a copy of the PICS pertaining to recruitment may be obtained. A statement to the following effect should be included - "Personal data provided by job applicants will be used strictly in accordance with the employer's personal data policies, a copy of which will be provided immediately upon request."

2.3.3 An employer who directly, or through its agent, advertises a vacancy that solicits the submission of personal data by job applicants should provide a means for the applicant to identify either the employer or its agent.[2]

A blind advertisement is one that provides no means of identifying either the employer or the employment agency acting on its behalf. However, the advertisement may or may not directly solicit personal data from job applicants. A blind advertisement is permitted provided that there is no direct solicitation of personal data from job applicants.

For example, an employer should not use a vacancy notice to solicit the submission of personal data by applicants that gives only a Post Office Box Number. However, should an employer not wish to disclose its identity in a vacancy notice, it may request interested individuals to submit a written request to a Post Office Box Number for an application form for the vacancy that identifies the employer. Alternatively, the employer may use a recruitment agency identified in the vacancy notice to receive the personal data solicited from the applicants. In this case, the advertisement is required to identify the agency.

2.3.4 An employer should not solicit the submission of personal data of individuals by means of a job advertisement unless there are one or more positions of employment which are presently, or may become, unfilled.[3]

For example, an employer should not place an advertisement just to test the job market situation or to put pressure on existing staff members and, in that process, solicit the submission of personal data. Obtaining personal data by misrepresenting the purpose of collection may amount to an act of collection by means that are unfair in the circumstances.

[1] DPP1(3)
[2] DPP1(2)
[3] DPP1(2)

2.4 Employment Agencies/Executive Search Company

2.4.1 An employer who engages an employment agency to solicit the provision of personal data by job applicants thereby collects personal data of those applicants. Accordingly, the requirements mentioned in paragraphs 2.2.1 to 2.2.5 would apply for the purpose of this section.

2.4.2 Where an employer receives unsolicited personal data of an individual, whether directly from the individual seeking a job opportunity with the employer or offered by an employment agency about its job-seekers, the employer should:

2.4.2.1 use only such data as may be necessary for, or directly related to, its purpose of assessing the suitability of the individual for employment[1]; and

2.4.2.2 not use the data for a new purpose unless the prescribed consent from the individual is obtained. [2]

It is very common for an employer to receive personal data from an individual who is searching for a job opportunity. An employment agency may also refer its job-seeker's information to an employer. Information received in this manner is often excessive for recruitment purposes by the employer. The employer should disregard any personal data provided which is irrelevant to the recruitment process.

2.4.3 An employer who engages a third party as an agent with express authority to perform specified recruitment functions for, and on behalf of, the employer should take all practicable steps to ensure that the third party will not act in contravention of the requirements under the Ordinance.[3]

The Ordinance imposes legal liability on an employer in relation to any wrongful acts or practices done by a third party where the third party is engaged as an agent on behalf of the employer. For example, an employer could request details of the third party's personal data privacy policies and practices to verify that the appropriate standards have been adopted. Alternatively, an employer may consider having in place an agreement between the parties that incorporates clauses requiring certain procedures to be complied with. For example, the employer should clearly identify the sets of personal data needed to facilitate the selection process undertaken by the agent, and the agent should agree to restrict the collection of personal data to the sets specified.

2.5 Internal Records about Job Applicants

2.5.1 An employer may use personal data of a job applicant whose data is collected during the course of a recruitment exercise for use in a later exercise of this nature, provided that:

[1] DPP1(1)(b)
[2] DPP3(1) and DPP3(4)
[3] Section 65, DPP2(3) and DPP2(4), DPP4(2) and DPP4(3)

2.5.1.1 the employer has a general policy to retain the data for such a purpose;
2.5.1.2 the employer has a stipulated retention period of keeping such data; and
2.5.1.3 the applicant has not otherwise objected to the use of his data for such a purpose.

As a matter of good practice an employer should take steps to inform job applicants about its retention policy of personal data collected in the course of a recruitment exercise. It should also provide an opportunity for unsuccessful applicants to request the destruction of the data if the applicant does not wish it to be used for a subsequent recruitment exercise.

2.5.2 An employer who, pursuant to paragraph 2.5.1, uses personal data collected on a previous occasion for the purpose of identifying suitable candidates should refrain from using the data until such time as the data has been updated should there be reasonable grounds to believe that such data has become inaccurate since it was collected.[1]

2.5.3 An employer who has retained personal data of job applicants that has been collected during the course of a recruitment exercise for use in a later exercise should:

2.5.3.1 only use the data for such purpose or a directly related purpose unless the applicant has given his prescribed consent to the use in some other purposes;[2] and
2.5.3.2 take all practicable steps to ensure that the data is retained securely and is accessible to authorised personnel on a "need-to-know" basis.[3]

It should be noted that the requirements mentioned in paragraphs 2.5.1 to 2.5.3 also apply to an employment agency that holds personal data provided by individuals searching for jobs.

2.6 Receiving and Processing Applications for Employment

2.6.1 An employer should take all practicable steps to ensure that, having regard to their confidential nature, the personal data of job applicants is collected, processed and stored securely, irrespective of whether the data is stored in electronic, photographic or hard copy format.[4]

For example, an employer that asks candidates to supply data in hard copy format should request that candidates place their applications in a sealed envelope marked in some way such as "Confidential. For the attention of the Human Resources Department (or of the relevant employee)". Mailroom and reception staff should be instructed to deliver such letters unopened.

[1] DPP2(1)(b)
[2] DPP3(1) and DPP3(4)
[3] DPP4(1)
[4] DPP4(1)

As a matter of good practice, databases comprising personal data of job applicants should be accessible only to authorised staff using secure passwords on a "need-to-know" basis. Hard copy data should be located in secure areas. Personal data relating to job applicants stored on physical media such as paper or microfilm should be stored in locked cabinets in a secure room. In the event of such information being analysed or reviewed, the contents of that data should not be left unattended by, or out of the control of, the authorised persons.

2.6.2 An employer should take all practicable steps to ensure that staff authorised to access personal data have the appropriate qualities of integrity, prudence and competence.[1]

For example, an employer may implement training programmes to ensure that staff members who have responsibility for recruitment-related matters are made aware of the employer's personal data handling policy and practices, and carry out supervisory checks to ensure compliance with policy requirements.

2.7 Seeking Information for Selection Assessment

2.7.1 An employer may compile information about a job applicant, to supplement other data collected at the time of the original application, to assess the suitability of potential candidates for the job provided that it does not in the process collect personal data that are excessive in relation to the purpose.[2]

Generally, it would not be excessive to collect data to increase an employer's knowledge of a candidate's skills, good character, competencies or abilities, provided this knowledge was relevant in relation to the nature of the job. A common selection technique is by means of a selection interview or by requiring applicants to undertake a written skill test. Depending on the nature of the job, other selection techniques may involve an applicant in psychological tests, security vetting or integrity checking procedures. These selection techniques often entail collection of additional personal data from applicants.

For example, an employer may use a security vetting procedure to establish the security credentials of a potential candidate for a security guard's position if such knowledge is crucial prior to the employer's consideration to offer the job to the candidate. However, recording the details of a candidate's outside activities and interests might be excessive unless the employer can demonstrate that such detail is relevant to the inherent requirements of the job.

To ensure the impartiality of the post holder and to avoid any conflict of interest that may arise in respect of the capacity to which the potential candidate is appointed, integrity checking may be necessary. However, the employer must be able to demonstrate that the collection of personal data, such as the candidate's investments or other financial matters, are relevant items essential for assessing the integrity of the individual concerned.

[1] DPP4(1)(d)
[2] DPP1(1)(c)

2.7.2 An employer who compiles information about a job applicant pursuant to paragraph 2.7.1 should ensure that the selection method so employed does not involve the collection of personal data by means that are unfair.[1]

As a matter of good practice, an employer should inform a job applicant before the selection method is used of its relevance to the selection process and the personal data to be collected by the chosen method.

2.8 Seeking Personal References of Job Applicants

2.8.1 An employer who wishes to obtain references from a potential candidate's current or former employers or other sources should ensure that such references are provided with the consent of the candidate concerned.

The Ordinance requires the candidate's current or former employers to have the candidate's consent in providing references. Such consent may be given orally or in writing. As a matter of good practice, the prospective employer should consider seeking consent from the candidate prior to approaching the candidate's current or past employers or other sources for a reference. If this is the case, the prospective employer should, when requesting for the reference, notify the source that provides the reference that consent of the candidate has been given. If in doubt, the current or past employer should seek evidence of such consent from the requesting party, or verify this with the candidate.

2.9 Acceptance by Candidates

2.9.1 An employer may, no earlier than at the time of making a conditional offer of employment to a selected candidate, collect personal data concerning the health condition of the candidate by means of a pre-employment medical examination, provided that:

2.9.1.1 the personal data directly relates to the inherent requirements of the job;
2.9.1.2 the employment is conditional upon the fulfilment of the medical examination; and
2.9.1.3 the personal data is collected by means that are fair in the circumstances[2] and are not excessive[3] in relation to this purpose.

For example, an employer may have a policy requiring a suitable candidate to undertake a pre-employment medical check by a nominated medical board to confirm whether the candidate is fit for employment. In this circumstance, the employer needs only to be provided with the minimum information about the candidate's health condition that supports the medical practitioner's opinion that he or she is fit for employment. Details of the candidate's medical history and treatment might be relevant for the medical board when conducting the medical check with the candidate, but these details need not be collected by the employer.

[1] DPP1(2)
[2] DPP1(2)
[3] DPP1(1)(c)

2.9.2 An employer may, at the time when a selected candidate accepts an offer of employment, collect additional personal data of the candidate and his family members, provided that the personal data is:

2.9.2.1 necessary for the purpose of employment in relation to the job[1] for which the candidate is appointed; or

2.9.2.2 necessary for a purpose pursuant to a lawful requirement that regulates the affairs of the employer.

For example, after the acceptance of an offer of employment, it would be necessary for the employer to collect personal data relating to the new employee such as bank details for the payment of salary. Other examples are information concerning the candidate's family members that are needed for the administration of any benefits an employer provides for such family members. However, it would be excessive to collect personal data such as the candidate's outside interests unless such information is necessary for, or directly related to, the inherent requirements of the job for which the employee has been appointed.

2.9.3 An employer may, at the time when the selected candidate accepts an offer of employment, collect a copy of the Hong Kong Identity Card of the candidate.[2]

2.9.4 An employer should obtain the prescribed consent of an appointee before publicly disclosing any personal data of the appointee in relation to the appointment unless such public disclosure is required by law or by any statutory authorities.[3]

2.10 Unsuccessful Candidates

2.10.1 An employer who has a general policy of retaining personal data of an unsuccessful job applicant for future recruitment purposes should not retain such data for a period longer than two years from the date of rejecting the applicant unless:

2.10.1.1 there is a subsisting reason that obliges the employer to retain the data for a longer period; or

2.10.1.2 the applicant has given prescribed consent for the data to be retained beyond two years.

As a matter of good practice, an employer wishing to retain personal data relating to an unsuccessful job applicant, for the purpose of future recruitment exercises, should inform the candidate of the period for which the employer will normally retain such data. It is also a good practice to provide unsuccessful job applicants with the opportunity to request the destruction of their data if they do not wish them to be used for this purpose. Generally speaking, actual or potential legal proceedings may constitute a subsisting reason for personal data of unsuccessful applicants being retained for longer than two years.

---

[1] DPP1(1)(b)
[2] Paragraph 3.2.2.1 of the PI Code
[3] DPP3(1), DPP3(4) and section 60B(a)

2.11 Data Access and Correction Requests by Job Applicants

2.11.1 Personal data collected from job applicants in respect of job recruitment and other data compiled about applicants in the course of a recruitment selection process mentioned in paragraphs 2.1.1 - 2.1.3 are subject to access and correction by the applicants. Accordingly, requirements mentioned in Section 1 - Complying with Data Access and Correction Requests, should be complied with for the purpose of this section unless there is an applicable exemption provided for under the Ordinance.

2.11.2 An employer may refuse to comply with a data access request made by a job applicant pursuant to paragraph 2.11.1 if:

2.11.2.1 the employer has received the request prior to it making a decision on filling the vacancy for which the job applicant has applied; and

2.11.2.2 the recruitment is a process whereby the applicant has a right to appeal against the appointment decision.[1]

It should be noted that a recruitment process falls outside the meaning of a "relevant process" under the Ordinance if it is a process where no appeal may be made against any such determination of the process (as most recruitment processes probably are). Furthermore, the exemption in relation to a relevant process is only applicable for the period until the completion of that process. Completion, in relation to a recruitment process that falls within the meaning of a relevant process, means the making of the determination on the suitability of job applicants for employment or appointment to office. The availability of an appeal governs whether the recruitment process amounts to a relevant process and does not mean that the appeal period is part of the recruitment process period. Hence, an employer who receives a data access request by a job applicant after the determination of the recruitment process is completed should comply with the request.

2.11.3 An employer, who holds personal data that consists of a personal reference given by a third party individual other than in the ordinary course of his occupation, may refuse to comply with a data access request made by a job applicant pursuant to paragraph 2.11.1 if:

2.11.3.1 in any case, unless that third party individual has given his consent in writing to the employer for the disclosure of the reference; or

2.11.3.2 in the case of a reference given on or after 20 December 1996, until the applicant concerned has been informed in writing that he has been accepted or rejected for employment in respect of the job he applies.[2]

If the third party gives consent for disclosure of the reference before the applicant is informed of the employer's decision, the employer might consider granting access to the data concerned.

[1] Section 55
[2] Section 56

3 Current Employment

3.1 Introduction

3.1.1 On appointment, an employer may retain personal data of the appointee for the purpose of the employment. Examples of these are the data provided by the appointee at the time of the job application and other data compiled about the appointee in the course of the recruitment process as mentioned in paragraph 2.1.3.

3.1.2 In addition, an employer may collect supplementary personal data from the employee for the purposes of employment and other related human resource management functions. Examples of these data would include, bank details for the payment of salary and information on family members of the employee that are needed for the administration of any benefits an employer provides for family members. A further example would be information that is required by the employer to fulfil certain legal obligations, such as personal data about the spouse of married employees for the purpose of filing returns under the Inland Revenue Ordinance.

3.1.3 In the course of employment of the employee, an employer may further compile information about the employee. Such information may include:

3.1.3.1 Records of remuneration and benefits paid to the employee.
3.1.3.2 Records of job postings, transfer and training.
3.1.3.3 Records of medical checks, sick leave and other medical claims.
3.1.3.4 Written records of disciplinary proceedings involving the employee.
3.1.3.5 Performance appraisal reports of the employee.
3.1.3.6 Written reports of staff planning exercises involving the employee.
3.1.3.7 Written reports of promotion exercises involving the employee.

3.1.4 The Ordinance requires an employer to take all practicable steps to ensure that employees are informed of certain matters in relation to the collection of their personal data.[1] This requirement applies to situations mentioned in paragraphs 3.1.2 to 3.1.3 where the personal data is collected directly from the employee. This notification requirement can be made in the form of a written PICS pertaining to employment. As a practical guidance, an employer should provide the PICS notification at the time when the employee accepts the offer of employment or during induction.

[1] DPP1(3)

3.2 Personal Data in relation to the Terms and Conditions of Employment

3.2.1 An employer may, pursuant to paragraph 3.1.2, collect personal data from an employee and his family members provided that the collection of the data is:

3.2.1.1 necessary for or directly related to a human resource function of the employer[1]; or
3.2.1.2 pursuant to a lawful requirement that regulates the affairs of the employer; and
3.2.1.3 by means that are fair in the circumstances[2] and the data is not excessive in relation to the purpose.[3]

Compensation and Benefits

3.2.2 An employer may collect personal data of an employee and his family members in relation to its provision of compensation and benefits to the employee provided that:

3.2.2.1 the requirements mentioned in paragraph 3.2.1 are complied with; and
3.2.2.2 the data is necessary to ascertain the eligibility of the employee's claim for compensation or benefits.

An employer may provide medical, housing or other benefits to its employees or their family members. In administering the provision of these benefits, the employer may have a policy that aims to prevent the provision of double benefits to employees or their family members. In this circumstance, the employer may require employees to provide evidential proof about claims made in relation to their family members. In processing statutory or contractual claims of compensation, an employer may also require an employee to provide evidential proof to substantiate payment of such claims.

Integrity Checking/Declaration of Conflict of Interest

3.2.3 An employer may collect personal data of an employee to facilitate integrity checking or to determine any conflict of interest by the employee, provided that:

3.2.3.1 the requirements mentioned in paragraph 3.2.1 are complied with;
3.2.3.2 the data is important to the employer in relation to the inherent nature of the job for which the employee is appointed; and
3.2.3.3 the employer has a policy covering such practices, prior notice of which has been brought to the attention of the employee concerned.

[1] DPP1(1)(b)
[2] DPP1(2)
[3] DPP1(1)(c)

An employer may have a policy requiring its employees to disclose their private investments by means of a declaration submitted to the employer. The practice is usually concerned with ensuring the impartiality of the post holder and to avoid any conflict of interest that may arise in respect of the capacity to which the employee is appointed. However, the employer must be able to demonstrate that the personal data collected relating to the employee, his family members, or any third party individual acting on his behalf, are relevant items essential for the said purposes.

Medical Checking and Health Data

3.2.4 An employer may collect personal data relating to the health condition of an employee provided that the collection is for a purpose:

3.2.4.1 directly related to the assessment of the suitability of the employee's continuance in employment; or

3.2.4.2 directly related to the employer's administration of medical or other benefits or compensation provided to the employee.

For example, where the nature of a post requires the maintaining of a certain level of health, an employer may, by contract or statutory requirement, require an employee to undergo regular medical checking for consideration of his suitability for continuance in employment. In this circumstance, the employer needs only be provided with the minimum information necessary to determine whether the employee is fit for further employment. Similarly, an employer may only need the minimum information about a sick leave application of an employee to verify or calculate the entitlement to sick leave and other related benefits but not the details of the treatment prescribed for the medical condition afflicting the employee.

3.2.5 An employer who, pursuant to paragraph 3.2.4, collects personal data of an employee should ensure that:

3.2.5.1 the requirements mentioned in paragraph 3.2.1 are complied with; and

3.2.5.2 the employer has a policy covering medical checking, prior notice of which has been brought to the attention of the employee concerned.

In most cases, details of medical history are not necessary for the purposes concerned unless the collection of these details are required in order to fulfil certain legal requirements on the part of the employer, for example, for the purpose of processing statutory or contractual medical claims.

3.2.6 An employer should take all practicable steps to ensure that personal data collected pursuant to paragraphs 3.2.1 to 3.2.4 is kept secure having regard to the generally sensitive nature of the data concerned.[1]

As a matter of good practice, personal data held in relation to employees on an automated system should be accessible only to authorised staff using appropriate security procedures. Such procedures might include secure terminals, access protocols, audit trail software, logging and compliance checks. If such data is in hard copy form, it should be held in a secure area accessible only to authorised personnel on a "need-to-know" basis.

[1] DPP4(1)

3.3 Disciplinary Proceedings

3.3.1 An employer who conducts a disciplinary investigation against an employee for a breach of the terms and conditions of employment should take all practicable steps to ensure that the personal data compiled about the employee concerned is:

3.3.1.1 accurate for the purpose upon which disciplinary decisions are taken;[1] and

3.3.1.2 held securely and accessible only by authorised personnel on a "need-to-know" basis.[2]

For example, an employer may, in the course of disciplinary proceedings, compile information about an employee who is the subject of allegations of improper behaviour that may be a cause for his removal from employment or office. In this circumstance, the sensitivity of such information requires the employer to take effective measures to ensure that the information is accurate for decision making purposes. Correspondingly effective security measures should also be adopted to prevent the information from being accessed by unauthorised persons.

3.3.2 An employer who holds personal data about an employee obtained in the course of disciplinary proceedings, including information collected from third party sources about the employee concerned, should:

3.3.2.1 only use the data for a purpose directly related to the investigation of suspected wrongdoings; and

3.3.2.2 not disclose or transfer the data to a third party unless the third party has legitimate reasons for gaining access to the data.

Generally, an employer should not publicly disclose any disciplinary findings that lead to the disclosure of the identity of the employee concerned unless such disclosure is in compliance with DPP3. For example, if an employer wishes to make an internal announcement of a disciplinary finding to all staff members, it should take into account the possible harm that might be caused to the employee concerned and consider removing from the announcement any identifiable particulars that relate to the employee.

3.4 Performance Appraisal

3.4.1 An employer who has a policy of conducting performance appraisals may compile personal data about the employee provided that the data is to be used for the purpose of:

3.4.1.1 assessing the employee's performance;
3.4.1.2 assessing the employee's suitability for advancement;
3.4.1.3 determining the employee's continuance in employment; or
3.4.1.4 determining the employee's job posting or training needs.

[1] DPP2(1)
[2] DPP4(1)

3.4.2 An employer who compiles performance appraisal information about an employee should collect personal data that is not excessive in relation to the purpose and by means that are fair in the circumstances.[1]

For example, it would not be fair to record an employee's work-related telephone conversations as part of a performance appraisal process unless there is no other reasonably practicable way of monitoring the employee's performance, and prior notification is given of such a practice. It may not be fair to use electronic surveillance of employees at work, such as the use of a finger-scan system, to monitor staff attendance at work unless there is no other less privacy-intrusive means of doing so. As a matter of good practice, employees should be served notice in writing if specific techniques are to be deployed to monitor their performance.

3.4.3 An employer who holds personal data about an employee compiled in the course of performance appraisal, should:

3.4.3.1 only use the data for a purpose mentioned in paragraph 3.4.1; and
3.4.3.2 not disclose or transfer the data to a third party unless the third party has legitimate reasons for gaining access to the data.

For example, if the performance appraisal report compiled about an employee requires follow-up action by a third party, e.g. by a third party authority, then the report can be referred to the third party for the purpose of completing the appraisal. As a matter of good practice, an employer should invite employees to comment on all assessments that are made and record such comments on the appraisal form.

3.5 Staff Planning

3.5.1 An employer, who holds personal data that consists of information relevant to any staff planning proposal may withhold such data from an employee requesting access.[2] Staff planning proposals consist of plans to fill a series of employment positions, i.e. two or more such positions, or the cessation of the employment of a group of employees.

Examples of activities that would be considered to be staff planning would be restructuring, reorganising, redundancy or succession plans involving a group of employees. Normally, such planning would result in the addition or removal of positions in an organisation. It should be noted that a recruitment process does not fall within the meaning of staff planning. Similarly, a performance appraisal report prepared in the course of a normal human resource management function would not be covered.

Neither promotion planning nor career development planning of employees amount to staff planning under section 53 of the Ordinance as they do not result in the addition or removal of positions in an organisation.

[1] DPP1(1)(c) and DPP1(2)
[2] Section 53

3.6 Promotion Planning

3.6.1 An employer who compiles information about an employee for the purpose of determining an individual's suitability for promotion should collect personal data that is not excessive in relation to the purpose[1] and by means that are fair in the circumstances.[2]

Promotion planning refers to the process of assessing an individual's readiness to assume the duties of a more senior position within the organisation. As a matter of good practice, an employer should restrict the use of psychological tests, assessment role-plays, simulations and other related techniques so that only those skills, abilities and attitudes relevant to the advancement are assessed.

3.6.2 An employer who holds personal data about an employee compiled in the course of promotion planning, including information collected from third party sources about the employee concerned, should:

3.6.2.1 only use the data for a purpose directly related to its promotion planning process; and

3.6.2.2 not disclose or transfer the data to a third party unless the third party has legitimate reasons for gaining access to the data.

For example, an employer may have a policy that requires a third party authority to endorse or confirm recommendations made by a selection board in respect of a promotion planning exercise. In this circumstance, the transfer of the information to the third party concerned is permissible only if the use of the data by the other party directly relates to matters concerning the promotion planning.

3.7 Providing Job References for Employees

3.7.1 An employer should not provide a reference concerning an employee or former employee to a third party without the employee's prescribed consent unless the employer is satisfied that the third party requesting the reference has obtained the prior consent of the employee concerned.[3] Such consent means the express consent of the employee given voluntarily.[4]

The consent may be given by the employee directly to the employer or may be given to the third party seeking the reference. In the latter case, the third party seeking the reference should notify the employer that he has documentary evidence of the consent of the employee to request the reference and is prepared to furnish a copy of that evidence upon request. If in doubt, the employer may verify this with the employee concerned before releasing any reference to the requesting party.

[1] DPP1(1)(c)
[2] DPP1(2)
[3] DPP3(1) and DPP3(4)
[4] Section 2(3)(a)

3.8 Data Access and Correction Requests by Employees

3.8.1 Personal data collected from employees and other data compiled about employees in the course of their employment mentioned in paragraphs 3.2 to 3.7 are subject to access and correction by the employees.[1] Accordingly, requirements mentioned in Section 1 - Complying with Data Access and Correction Requests, should be complied with for the purpose of this section unless there is an applicable exemption provided for under the Ordinance.

Relevant Process Exemption[2]

3.8.2 An employer who holds personal data that is the subject of a relevant process may withhold such data from an employee requesting access for as long as the process is in progress and until a determination has been made regarding the relevant process. A relevant process means an employment-related evaluative process whereby the employee concerned has a right to appeal against any such determination.

For example, disciplinary proceedings conducted against an employee for a breach of the terms and conditions of employment would fall within the meaning of a relevant process if the proceedings consist of a process whereby the employee may appeal against any determination of the disciplinary action taken. Other examples include promotion exercises or evaluative processes concerning an employee's continuance in employment or removal from employment where the employee has a right of appeal against the decision made.

It should be noted that the relevant process exemption is only applicable for the period until the completion of that process. Completion, in relation to a relevant process, means the making of the determination of action taken. The availability of an appeal governs whether a particular process amounts to a relevant process and does not mean that the appeal period is part of the process period. Hence, an employer who receives a data access request by an employee after the determination of the relevant process is completed should comply with the request.

As a matter of good practice, employers should have a written policy that documents the procedures and personal data collected for the purpose of conducting a relevant process. The policy should stipulate any right of appeal against the decision of the process and any conditions pertaining to that right.

Transitional Provision Exemption

3.8.3 [Omitted as spent on 3 August 2002]

[1] Sections 18 and 22
[2] Section 55

3.8.4 An employee who has been provided with a copy of personal data by the employer in compliance with a data access request is entitled to request the employer to make the necessary correction in respect of any data that the employee considers to be inaccurate.[1] If satisfied that the data is indeed inaccurate, the employer is required to comply with the request.[2]

An employer is required to make the necessary correction if it is satisfied that the personal data to which the request relates is inaccurate. This should be made within 40 days upon receiving the request from the employee and the employer should provide the employee with a copy of the corrected data within the same time limit. However, if the correction requested relates to data, whether a fact or an expression of opinion, and the employer is not satisfied that the data is inaccurate, it may refuse to make the correction. An "expression of opinion" includes an assertion of fact that is unverifiable or in all circumstances of the case, is not practicable to verify. Further guidance on handling data correction requests is given in Section 1 - Complying with Data Access and Correction Requests.

3.9 Accuracy and Retention of Employment-related Data

3.9.1 An employer should take all practicable steps to ensure that the employment-related data it holds about employees is accurate having regard to the purpose for which the data is used.[3]

An employer may implement a reminder system to ask employees to report changes of their personal data so that any changes in personal circumstances concerning the employees could be made. As a matter of good practice, an employer may consider providing employees with copies of employment-related data at regular intervals and invite them to report on any changes that need to be made. For example, medical benefit records may require updating to include information on an employee's spouse, if the employee has married during the course of the employment, so that medical benefits may be extended to cover the spouse.

3.9.2 An employer should take all practicable steps to ensure that information about its policies and practices in relation to personal data can be made available to its employees.[4]

[1] Section 22(1)
[2] Section 23(1)
[3] DPP2(1)(a)
[4] DPP5

For example, an employer may comply with this requirement by preparing a written PPS concerning its personal data handling policies and practices. The PPS should include a list of the kinds of employment-related data held by the employer, and the main purposes for which the data is used. As a matter of good practice, the PPS should also include a retention policy covering employment-related data and be circulated to employees at regular intervals.

3.10 Use of Employment-related Data of Existing Employees

3.10.1 An employer should not use or disclose employment-related data of an employee for any purpose other than the purpose directly related to the employment of the employee unless:

3.10.1.1 the employee has given his prescribed consent to such other use or disclosure;[1]
3.10.1.2 the purpose is directly related to the purpose for which the data was collected;[2]
3.10.1.3 such use or disclosure is required by law or by statutory authorities;[3] or
3.10.1.4 there is an applicable exemption provided for under the Ordinance.

For example, an employer may wish to enter into an agreement with a credit card company to offer a credit card with special terms and conditions for its employees. In such a case, the employer should not use the employees' data and pass it to the credit card company for marketing of the card without first obtaining the prescribed consent of the employees. Alternatively, the employer may use the address data of employees, which was collected to facilitate communication with the employer, to notify the employees directly of the service.

However, an employer may transfer documents regarding an employee's medical claim to its insurer who provides employee medical cover to effect the claim. This would be a purpose directly related to the original purpose for which the claim documents are collected. As a matter of good practice, an employer could remind the recipient to confine its use of the data to only those purposes that are directly related to the purpose of the disclosure. In the example of the insurer given above, the employer may include in its instruction to the insurer a statement to the effect that "The employment-related personal data attached should only be used to effect insurance cover under the terms and conditions of our Employee Medical Insurance policies with you."

An example of statutory requirement for disclosure would be the disclosure of employment-related data to public authorities that are authorised by law to require the production of personal data. For example, the reporting of employment-related data of employees in the annual Employer's Return of Remuneration and Pensions to the Inland Revenue Department.

3.10.2 An employer who, pursuant to paragraph 3.10.1, discloses employment-related data to a third party should take all practicable steps to ensure that:

[1] DPP3(1)
[2] DPP3(1) and DPP3(4)
[3] Section 60B(a)

3.10.2.1 the data thereby disclosed is accurate having regard to the purpose for which the data is disclosed;[1] and

3.10.2.2 where it is practicable in all circumstances to know that the data was inaccurate at the time of such disclosure, the recipient is informed of the inaccuracy and is provided with such particulars as will enable the recipient to rectify the data.[2]

As a matter of good practice, an employer should also avoid disclosure of data in excess of that is necessary for the purpose of use by the recipient. For example, employment-related records held on a computer should not be printed in full and passed on to an insurer without consideration of the insurer's needs. Only the information reasonably required to effect the type of insurance policy being written should be transferred to the underwriter or insurance agency.

3.10.3 An employer should take all practicable steps to ensure that the means of transferring employment-related personal data to a third party are secure, having regard to the sensitivity of the data thereby disclosed and the harm that could result if unauthorised or accidental access should occur.[3]

For example, in mailing out documents containing employment-related data, an employer may consider putting the documents in a sealed envelope addressed to the recipient and marked "Private and Confidential" on the envelope. If a window envelope is used, care should be taken not to make visible through the window opening personal data other than that necessary for the purpose of postal delivery. It should be noted that email transmission is insecure unless security protection software is used. Depending on the level of sensitivity of data to be transmitted, an employer may consider implementing appropriate security protection software before employment-related data is allowed to be transferred via email.

3.10.4 An employer may, without the consent of the employee, disclose employment-related data of the employee to a third party provided that:

3.10.4.1 such disclosure concerns data that is necessary for a purpose that falls within the ambit of section 58(1) of the Ordinance; and

3.10.4.2 the employer has reasonable grounds for believing that non-disclosure would be likely to prejudice such purposes.[4]

The purposes referred to in section 58(1) of the Ordinance include, inter alia, purposes used for the prevention or detection of crime, the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, dishonesty or malpractice by individuals. The words "unlawful or seriously improper conduct" extend beyond criminal conduct to include civil wrongs.[5] Hence, an employer may disclose employment-related data of an employee to a third party if it has reasonable grounds for believing that the data thereby disclosed will be used by the third party in civil proceedings and non-disclosure of the data would be likely to prejudice the prevention, preclusion or remedying of a civil wrong by the employee.

---

[1] DPP2(1)(a)
[2] DPP2(1)(c)
[3] DPP4(1)(e)
[4] Section 58(2)
[5] Court of First Instance in case HCPI 828/97

However, it should be noted that the requirement is for the employer to have reasonable grounds for holding the belief referred to above and the Ordinance does not oblige the employer to accede to such a request for disclosure by the third party. For example, if employment-related data of an employee is requested without a warrant by the Police in connection with a criminal investigation, the Police will need to satisfy the employer that investigation would be prejudiced by a failure to disclose the data being sought. If the data is sought pursuant to a warrant, the employer may rely on the warrant as providing sufficient grounds for providing the Police with such information even though such a disclosure was not one of the purposes for which the data was collected.

3.11 Disclosure or Transfer of Employment-related Data

Transfer to Outside Professional Services

3.11.1 An employer who seeks professional services of third parties on matters that involve the disclosure or transfer of employment-related data should ensure that the data is limited to that required for the specific services that they are to provide.

An employer may employ external professional services, such as legal representatives or consultants to advise on human resource management matters. In doing so, the employer should avoid disclosure of data in excess of that is necessary for the purpose of use by the recipient in providing the service. For example, data such as home address or detailed salary payment of individual employees would generally be unnecessary for use by a management consultant who is engaged to devise a career development plan for employees.

An employer may use the services of an external auditor for the purpose of carrying out a financial audit. Such access to employment-related data by the auditor is in accordance with section 412 of the Companies Ordinance (Cap. 622). External auditors' requirements for access will generally be limited to information such as emoluments, taxation and personal expenses, sight or copies of any contract between employer and employee, or employer and contractor, and documents relating to termination of employment where these are required to substantiate the terms of relevant transactions.

Outsourcing of Human Resource Data Processing

3.11.2 An employer who out-sources or contracts out its human resource processing to an external agency should take all practicable steps to ensure that the processing agency protects the employment-related data against unauthorised or accidental access or disclosure.

It should be noted that the Ordinance imposes legal liability on an employer in relation to any wrongful acts or practices done by a third party[1] where the third party is engaged as an agent on behalf of the employer. For example, an agreement may be drawn up controlling how the data are transmitted or processed and requiring the processing agency to take steps to ensure the integrity, prudence and competence of its staff having access to the data[2].

---

[1] Section 65(2)

[2] Reference can be made to the *Information Leaflet : Outsourcing the Processing of Personal Data to Data Processors* issued by the Commissioner.

Sub-contracting out Employees' Service to Other Organisations

3.11.3 An employer may disclose or transfer employment-related data of an employee for a purpose of sub-contracting the service of the employee to a third party organisation provided that:

3.11.3.1 such sub-contracting arrangement relates to a function or activity that the employer engages in; or

3.11.3.2 the use of the employee's data for such a purpose is one of the purposes for which the employee is so employed.

Most sub-contracting arrangements are governed by an agreement between the employer and the third party organisation. The employer is the prime contractor as a party to the agreement and the employees concerned are assigned to work on the job contracted for. For example, the employer has successfully won a project in a tender with the third party and the employee is assigned as one of the project members. In this situation, the employment relationship remains between the employee and his employer although the third party might have supervisory responsibility over the employee in terms of the job.

3.11.4 An employer who, pursuant to paragraph 3.11.3, discloses or transfers employment-related data to a third party organisation should ensure that the personal data disclosed is:

3.11.4.1 relevant to the inherent requirements of the job as specified in the third party's job description;

3.11.4.2 adequate but not excessive in relation to the purpose of the sub-contracting service; and

3.11.4.3 limited to employment-related data of the employee concerned.

In a sub-contracting arrangement, the employer may be required by the other party to provide personal data of its employees for selection purposes. For example, it may be necessary to include in a project proposal information about the employee to demonstrate his qualifications and suitability for the project tendered for. The employee's data, such as his curriculum vitae, is collected primarily for the purpose of employment with the employer. In so far as the data is disclosed for a purpose of inclusion in a project proposal that the employer engages in, the disclosure of such data could be regarded as a purpose directly related to the purpose for which the data is collected. However, the data thereby disclosed should be limited to the skills, competencies, abilities and work experience of the employee that are relevant to the inherent requirements of the job to which the employee may be assigned.

Transfer to a Place outside Hong Kong

3.11.5 Employment-related personal data may be transferred to a related office of the organisation outside Hong Kong provided that such a transfer is for a purpose directly related to the employment of employees and the data is adequate but not excessive in relation to that purpose.

For example, transfer of employment-related personal data outside Hong Kong to an overseas head office may be done for a permitted purpose, such as for a purpose relating to an intended posting of staff to an overseas office. It should be noted that the Ordinance provides for specific controls on the transfer of personal data outside Hong Kong.[1]

Transfer to Other Offices within the Organisation

3.11.6 Employment-related personal data may be transferred within the employing organisation for purposes directly related to the employment of employees provided that the data is adequate but not excessive in relation to the purpose of use by the party to whom it is transferred.

For example, staff of the employer's accounting department need not be provided with data that is irrelevant for its use in calculating salary payment to an employee, such as the employee's performance appraisal report. Similarly, internal auditors of the organisation should not have access to employment-related data that is not necessary in performing an internal audit.

Mergers, Acquisitions, and Associated Due Diligence Exercises[2]

3.11.7 Where an employer transfers employment-related data to an outside party involved in a merger, acquisition or due diligence exercise, such data should be limited to that is reasonably required to make a decision on the quality of personnel employed by the organisation, or other reasonable matters relating to the acquisition or merger[3].

Parties wishing to acquire a substantial share in a company, or organisations contemplating a merger, may request that employment-related personal data of the key officers be transferred to them. Examples of relevant data might be salary, job title, length of service, promotion history, qualifications, achievements and assessment of strengths and weaknesses. It is reasonable for employees to expect that if the organisation for which they work is a target for acquisition by another, or is actively considering a merger, certain employment data might be disclosed or transferred to the other party.

3.11.8 An employer may transfer employment-related data to intermediate parties in any transactions relating in any way to mergers, acquisitions and due diligence including financial advisors, bankers and lawyers provided that they use the data only on behalf of the employer for the purpose of facilitating the merger or acquisition[4].

As a matter of good practice, the employer should obtain an undertaking from such parties that they would keep the data secure and comply with all other relevant provisions of the Ordinance. If it becomes clear that a contemplated merger or acquisition will not take place, the other party, and any agent acting on their behalf, should forthwith destroy or return to the employer concerned any employment-related

---

[1] Section 33. This section of the Ordinance is not currently in force. Reference can be made to the *Guidance on Personal Data Protection in Cross-border Data Transfer* issued by the Commissioner.

[2] Section 63B

[3] Section 63B(1) & (2)(a)

[4] Section 63B(4)(a)

personal data received for the purpose of considering the merger or acquisition[1].

3.11.9 An employer may continue to use the employment-related data of employees for purposes directly related to their employment, notwithstanding any acquisition, in part or whole, of the employing organisation by another party.

For example, where two or more organisations merge, the resulting employer may continue to use employment data of employees in relation to their continued employment. As a matter of good practice, the employer should ensure that a single set of privacy policies and practices are developed for the combined employment-related personal data of the merged organisations.

3.12 Matters Concerning the Engagement of Subcontract Staff

3.12.1 An employer, who engages individuals on a subcontract basis, should not collect personal data about them that is excessive for the purpose of carrying out the employer's functions and activities in employing such individuals.[2]

For the purpose of this section, subcontract staff include staff employed through a third party such as an employment agency, workers employed by one company but who undertake work on behalf of another company, or staff who are self-employed. In these circumstances, the employer does not have a direct employment contract with the individuals concerned.

In general, an employer would need to collect less personal data relating to subcontract staff compared with data collected in respect of employees. For example, the employer would not normally collect personal data in relation to subcontract staff such as details of their bank accounts and family members. However, an employer may need to collect data of next of kin in case there is an emergency at work.

3.12.2 An employer who engages subcontract staff may retain personal data that it holds in respect of such staff only for so long as the data is required:

3.12.2.1 for carrying out the purposes (or any directly related purposes) for which the data was collected;[3] or

3.12.2.2 where there is a reasonable likelihood that such staff may be re-engaged on subsequent work.

For example, the employer may retain personal data relating to subcontract staff where this is necessary for the purpose of dealing with possible work disputes arising from the performance of subcontract staff. In the case where subcontract staff may be re-engaged for subsequent work, the employer may retain the data of subcontract staff for two years after the completion of the current or most recent contract. Once the two-year period has elapsed the data may only be retained if the staff concerned have given prescribed consent to an extension.

3.12.3 An employer who holds employment-related data of subcontract staff should observe the requirements mentioned in paragraph 3.11 in relation to the

[1] Section 63B(4)(b)
[2] DPP1(1)(c)
[3] DPP2(2)

disclosure or transfer of such data.

It is very common for a property management company to act as an agent of the Owners' Incorporation of a building and handle all affairs relating to the management and security of the building. In doing so, the property management company may sub-contract the security management duty to a third party security company who employs security guards or caretakers to work in the building premises.

The subcontracted security company may be asked to provide remuneration details of security guards to the property management company for the purposes of account auditing by the Owners' Incorporation. In this circumstance, the security company who is the employer of the guards should take special care in preparing the information requested as it may involve a disclosure of the data not only to the property management company but also the Owners' Incorporation. Generally, it would be adequate to provide the requested remuneration data without disclosing the identity of the individual guards concerned.

4 Former Employees' Matters

4.1 Introduction

4.1.1 Employees may leave an employer by transferring to another company, resigning, or because of termination of employment as a result of disciplinary action, redundancy, retirement, invalidity, or death.

4.1.2 Relevant personal data pertaining to a former employee may be required by an employer to fulfil its obligations to the former employee and its legal obligations under certain ordinances. The data may be required to:

4.1.2.1 meet statutory requirements – these may relate to the retention of salaries' tax records, business records, and sick leave records;
4.1.2.2 administer any remaining duties in respect of former employees or their family members under a pension, superannuation, or MPF scheme;
4.1.2.3 defend the organisation in any civil suit or criminal prosecution – in cases where legal action may be brought under, for example, legislation such as the Employees Compensation Ordinance;
4.1.2.4 defend the organisation against any claim for damages resulting from a purported medical condition or injury allegedly sustained during, and/or resulting from, the period of employment;
4.1.2.5 re-employ a former employee if there is a reasonable likelihood of the individual re-applying for employment; or
4.1.2.6 provide job references at the request of the employee.

4.1.3 For example, the Employment Ordinance[1] requires an employer to retain wage and employment records of employees covering the period of their employment during the preceding twelve months. Such records should be kept for six months after they cease employment.

4.1.4 Personal data of former employees retained by an employer for purposes mentioned in paragraph 4.1.2 is subject to access and correction by the employee. Accordingly, requirements mentioned in Section 1 - Complying with Data Access and Correction Requests, should be complied with for the purpose of this section unless there is an applicable exemption provided for under the Ordinance. Where relevant, attention should be paid to observing the requirements mentioned in paragraphs 3.10 and 3.11 in relation to Use, Disclosure and Transfer of Employment-related data that may be applicable to former employees.

[1] Section 49A of the Employment Ordinance (Cap. 57) refers.

Practical Guidance on Former Employees' Matters

4.2 Continued Retention of Personal Data of Former Employees

4.2.1 An employer may retain personal data of a former employee for purposes mentioned in paragraph 4.1.2 or other purposes provided that such other purposes are:

4.2.1.1 necessary for the employer to fulfil its contractual or legal obligations;
4.2.1.2 directly related to the purpose of managing the relationship between the employer and the former employee; or
4.2.1.3 those that the former employee has given prescribed consent.

4.2.2 An employer may retain a former employee's Hong Kong Identity Card number for linking, retrieving or processing records held by it concerning the employee.

For example, paragraph 2.6.4 of the PI makes provision for an employee's Hong Kong Identity Card number to be used for linking the employee's records held by different data users under the Mandatory Provident Fund system.

4.2.3 An employer should not retain the personal data of a former employee for a period longer than seven years from the date the former employee ceases employment with the employer unless:

4.2.3.1 there is a subsisting reason that obliges the employer to retain the data for a longer period;[1] or
4.2.3.2 the former employee has given prescribed consent for the data to be retained beyond seven years.

Generally, an employer is permitted to retain personal data where the erasure of the data is prohibited under any law, where there is ongoing litigation, where there are contractual obligations on the part of the employer to retain the data, or where it is in the public interest (including historical interest) for the data not to be erased.

The employer must take all practicable steps at the earliest opportunity upon the departure of an employee to ensure that only relevant information of the employee is retained to satisfy its retention requirements. For example, a summary of service records or testimonial about the service of a former employee can be compiled for the purpose of providing job references or processing applications for re-employment relating to the former employee instead of keeping full details that may otherwise be unnecessary for the purpose.

[1] Section 26(1)(a) and (b)

4.3 Accuracy of Former Employees' Personal Data

4.3.1 An employer should take all practicable steps to maintain the accuracy of personal data retained for purposes that continue after the employee has left employment.[1]

Generally, this requirement could be met by updating the data when the former employee informs the employer of a change, or when data is about to be used where any inaccuracies of the data would have a material effect on the use of the data.

4.3.2 Where an employer has reasonable grounds for believing that personal data of a former employee is inaccurate, having regard to the purpose of its retention, the employer should not use such data unless and until those grounds cease to be applicable.[2]

For example, an employer may need to regularly mail documents relating to a former employee's benefit payments. If the employer repeatedly received return mail, indicating wrong delivery, this would suggest that the contact address of the former employee was inaccurate. In this circumstance, the employer should avoid using the address for further mailing of benefit payments until the former employee's address can be verified.

4.3.3 An employer who engages a third party to administer any post-employment matters that concern former employees, such as a provident fund scheme, should take all practicable steps to ensure that:

4.3.3.1 the data transferred is accurate having regard to the purpose for which the data is used;[3] and

4.3.3.2 where it is practicable in all circumstances to know that the data was inaccurate at the time of such transfer, the recipient is informed of the inaccuracy and is provided with such particulars as will enable the recipient to rectify the data.[4]

4.4 Security of Former Employees' Personal Data

4.4.1 An employer should take all practicable steps to ensure secure protection measures are implemented in locations, either on-site at the employer's premise or off-site on other premises, to prevent unauthorised or accidental access to the retained personal data of former employees.[5]

As a matter of good practice, where the personal data of former employees is retained in computer or paper files, such files should be kept separately from the files of existing staff to enhance their security. If an employer retains former employees' data in a low-cost storage facility, this should be reasonably secure.

[1] DPP2(1)(a)
[2] DPP2(1)(b)
[3] DPP2(1)(a)
[4] DPP2(1)(c)
[5] DPP4(1)

4.5 Providing Job References for Former Employees

4.5.1 An employer should ensure that former employees have given their prescribed consent before giving a reference on them to a third party.[1]

Very often, a third party may request a job reference about a former employee of the employer when the employee applies for a job with the third party. Before doing this, the employer should obtain the consent of the employee concerned or request the third party to provide proof that the consent of the employee has been provided. It should be noted that an individual providing an oral personal reference based upon personal data from written or computer records is disclosing personal data and should therefore have the prescribed consent referred to above of the individual concerned.

4.6 Public Announcements about Former Employees

4.6.1 An employer who finds it necessary to announce publicly that a former employee has left employment, and no longer represents it, should include only the minimum information required to identify the employee concerned.

In any announcement regarding a former employee that may be made public, the employer should take care not to disclose the Hong Kong Identity Card number of the employee. Generally, the individual's full name, former job title and name of the organisation would be sufficient for the purpose. Normally, an employer making an announcement for such purposes need not state the reason for the former employee having left the organisation. If it is necessary to disclose the reason, the employer should consider obtaining prior consent of the individual concerned unless the employer has reasonable grounds to believe that such disclosure to a news organisation would be in the public interest.

4.7 Erasure of Former Employees' Personal Data

4.7.1 An employer who has retained personal data of former employees for purposes mentioned in paragraph 4.2.1 should ensure that, if the data is no longer necessary for such purposes prior to the expiry of the permitted retention period under paragraph 4.2.3, the data is not used for any purposes and is erased at the earliest practicable opportunity.[2]

Very often, records containing personal data of former employees are maintained in a storage medium other than paper files, e.g. microfiche or microfilm. If this is the case, it might not be practicable to delete individual data items from the records when the data needs to be erased. However, where the records are kept on physical paper files, then it would be practicable to destroy records that are no longer necessary for the purpose concerned. Such destruction might take place on the next occasion that the file is accessed for a particular purpose, or at the next scheduled time of the employer's file "weeding programme".

[1] DPP3(1) and DPP3(4)
[2] DPP2(2)

As a matter of good practice, an employer should develop a personal data management policy that will result in the implementation of a data disposal programme to facilitate deletion of those classes of data that are no longer necessary. This policy should also specify scheduled intervals for record destruction and disposal.

4.7.2 The requirement mentioned in paragraph 4.7.1 also applies to personal data of family members of the former employee held by the employer.

4.8 Retirement

4.8.1 An employer may retain relevant personal data of retired employees, or their family members, so long as there is an obligation on the part of the employer to administer any affairs relating to the retirement plan of employees.[1]

Generally, an employer may need to retain the name, contact, and perhaps bank details of those former employees or their dependents entitled to receive any benefits under the retirement plan. To ensure the accuracy of personal data relating to former employees, an employer should require former employees to notify it of any changes in their personal circumstances, or those of their family members (if relevant), that would necessitate updating of the data.

4.9 Death of an Employee

4.9.1 Data relating to a former employee who has died are not subject to the code. However, if an employer retains personal data relating to a living relative of a deceased employee, such data is subject to the code.[2]

For example, an employer may need to retain personal data of the relatives of deceased employees for the purposes of administering a company retirement fund. Such data is subject to the code.

[1] DPP2(2)
[2] Definition of "personal data" in Section 2

Appendix I - Ordinance Definition, principles and key sections

Ordinance Definitions

"data" means any representation of information (including an expression of opinion) in any document, and includes a personal identifier;

"data access request" means a request under section 18;

"data correction request" means a request under section 22(1);

"document" includes, in addition to a document in writing -
(a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and
(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

"employment" means employment under -
(a) a contract of service or of apprenticeship; or
(b) a contract personally to execute any work or labour,
and related expressions shall be construed accordingly;

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

"personal identifier" means an identifier -
(a) that is assigned to an individual by a data user for the purpose of the operations of the 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;

"use" in relation to personal data, includes disclose or transfer the data.

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 is 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 is 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 is or is 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 is 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 it was collected, of -
(A) his rights to request access to and to request the correction of the data; and
(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,,
unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is 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 is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;
(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used -
(i) the data is 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 is 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 is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and
(ii) that data was inaccurate at the time of such disclosure.
that the third party -
(A) is informed that the data is inaccurate; and
(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3) —
data processor means a person who —
(a) processes personal data on behalf of another person; and
(b) does not process the data for any of the person's own purposes.

3 Principle 3 – Use of Personal Data

(1) Personal data shall not, without the prescribed consent of the data subject be used for a new purpose.

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—
(a) the data subject is—
(i) a minor;

(ii) incapable of managing his or her own affairs; or
(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136);
(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and
(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section—

new purpose**,** in relation to the use of personal data, means any purpose other than—
(a) the purpose for which the data was 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

(1) 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 unauthorised or accidental access, processing, erasure, loss or 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 is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is 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.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2)-

data processor has the same meaning given by subsection (4) of data protection principle 2.

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 is or is 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).

Key Sections Referred to in the Text of the Code

2 Interpretation

(1) "relevant person", in relation to an individual (howsoever the individual is described), means –
(a) where the individual is a minor, a person who has parental responsibility for the minor;
(b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;
(c) where the individual is mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap.136) –
(i) a person appointed under section 44A, 59O or 59Q of that Ordinance to be the guardian of that individual; or
(ii) if the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by, the Director of Social Welfare or any other person under section 44B(2A) or (2B) or 59T(1) or (2) of that Ordinance, the Director of Social Welfare or that other person.

(3) Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent -
(a) means the express consent of the person given voluntarily;
(b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).

17A Interpretation of Part 5

Without limiting the definition of ***relevant person*** in section 2(1), in this Part—
relevant person, in relation to an individual, also includes a person authorised in writing by the individual to make, on behalf of the individual-
(a) a data access request; or
(b) a data correction request.

18 Data Access Request

(1) An individual, or a relevant person on behalf of an individual, may make a request -
(a) to be informed by a data user whether the data user holds personal data of which the individual is the data subject;
(b) if the data user holds such data, to be supplied by the data user with a copy of such data.

(2) A data access request under both paragraphs of subsection (1) shall be treated as being a single request, and the provisions of this Ordinance shall be construed accordingly.

(3) A data access request under paragraph (a) of subsection (1) may, in the absence of evidence to the contrary, be treated as being a data access request under both paragraphs of that subsection, and the provisions of this Ordinance (including subsection (2)) shall be construed accordingly.

(4) A data user who, in relation to personal data -
(a) does not hold the data; but
(b) controls the use of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with a data access request which relates to the data,
shall be deemed to hold the data, and the provisions of this Ordinance (including this section)

shall be construed accordingly.

(5) A person commits an offence if the person, in a data access request, supplies any information which is false or misleading in a material particular for the purposes of having the data user—
(a) inform the person whether the data user holds any personal data which is the subject of the request; and
(b) if applicable, supply a copy of the data.

(6) A person who commits an offence under subsection (5) is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

19 Compliance with Data Access Request

(1) Subject to subsection (2) and sections 20 and 28(5), a data user must comply with a data access request within 40 days after receiving the request by—
(a) if the data user holds any personal data which is the subject of the request—
(i) informing the requestor in writing that the data user holds the data; and
(ii) supplying a copy of the data; or
(b) if the data user does not hold any personal data which is the subject of the request, informing the requestor in writing that the data user does not hold the data.

(1A) Despite subsection (1)*(b)*, if—
(a) a data access request is made to the Hong Kong Police Force as to whether it holds any record of criminal conviction of an individual; and
(b) it does not hold such record,
it must comply with the request by informing the requestor orally, within 40 days after receiving the request, that it does not hold such record.

(2) A data user who is unable to comply with a data access request within the period specified in subsection (1) or (1A) shall -
(a) before the expiration of that period -
(i) by notice in writing inform the requester that the data user is so unable and of the reasons why the data user is so unable; and
(ii) comply with the request to the extent, if any, that the data user is able to comply with the request; and
(b) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with the request.

20 Circumstances in which Data User shall or may Refuse to Comply with Data Access Request

(1) A data user shall refuse to comply with a data access request -
(a) if the data user is not supplied with such information as the data user may reasonably require -
(i) in order to satisfy the data user as to the identity of the requester;
(ii) where the requester purports to be a relevant person, in order to satisfy the data user-
(A) as to the identity of the individual in relation to whom the requester purports to be such a person; and
(B) that the requester is such a person in relation to that individual;
(b) subject to subsection (2), if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the data user is satisfied that the other individual has consented to the disclosure of the data to the requester; or
(c) in any other case, if compliance with the request is for the time being prohibited under this or any other Ordinance.

(2) Subsection (1)*(b)* shall not operate -
(a) so that the reference in that subsection to personal data of which any other individual is the data subject includes a reference to information identifying that individual as the source of the personal data to which the data access request concerned relates unless that

information names or otherwise explicitly identifies that individual;

(b) so as to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise.

22 Data Correction Request

(1) Subject to subsections (1A) and (2), where -

(a) a copy of personal data has been supplied by a data user in compliance with a data access request; and

(b) the individual, or a relevant person on behalf of the individual, who is the data subject considers that the data is inaccurate,

then that individual or relevant person, as the case may be, may make a request that the data user make the necessary correction to the data.

(1A) If a person is a relevant person in relation to an individual only because the person has been authorised in writing by the individual to make a data access request on behalf of the individual, the person is not entitled to make a data correction request.

(2) A data user who, in relation to personal data -

(a) does not hold the data; but

(b) controls the processing of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with section 23(1) in relation to a data correction request which relates to the data,

shall be deemed to be a data user to whom such a request may be made, and the provisions of this Ordinance (including subsection (1)) shall be construed accordingly.

(3) Without prejudice to the generality of sections 23(1)*(c)* and 25(2), if a data user, subsequent to the receipt of a data correction request but before complying with the request pursuant to section 24 or refusing to comply with the request pursuant to section 25, discloses to a third party the personal data to which the request relates, then the user shall take all practicable steps to advise the third party that the data is the subject of a data correction request still under consideration by the user (or words to the like effect).

23 Compliance with Data Correction Request

(1) Subject to subsection (2) and section 24, a data user who is satisfied that personal data to which a data correction request relates is inaccurate shall, not later than 40 days after receiving the request—

(*a*) make the necessary correction to the data;

(*b*) supply the requestor with a copy of the data as so corrected; and

(*c*) subject to subsection (3), if—

(i) the data has been disclosed to a third party during the 12 months immediately preceding the day on which the correction is made; and

(ii) the data user has no reason to believe that the third party has ceased using the data for the purpose (including any directly related purpose) for which the data was disclosed to the third party,

take all practicable steps to supply the third party with a copy of the data as so corrected accompanied by a notice in writing stating the reasons for the correction.

(2) A data user who is unable to comply with subsection (1) in relation to a data correction request within the period specified in that subsection shall—

(*a*) before the expiration of that period—

(i) by notice in writing inform the requestor that the data user is so unable and of the reasons why the data user is so unable; and

(ii) comply with that subsection to the extent, if any, that the data user is able to comply with that subsection; and

(*b*) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with that subsection.

24 Circumstances in which Data User shall or may Refuse to Comply with Data Correction Request

(3) A data user may refuse to comply with section 23(1) in relation to a data correction request if -

(a) the request is not in writing in the Chinese or English language;

(b) the data user is not satisfied that the personal data to which the request relates is inaccurate;

(c) the data user is not supplied with such information as the data user may reasonably require to ascertain in what way the personal data to which the request relates is inaccurate;

(d) the data user is not satisfied that the correction which is the subject of the request is accurate; or

(e) subject to subsection (4), any other data user controls the processing of the personal data to which the request relates in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with that section.

25 Notification of Refusal to Comply with Data Correction Request, etc.

(1) A data user who pursuant to section 24 refuses to comply with section 23(1) in relation to a data correction request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor -

(a) of the refusal and the reasons for the refusal; and

(b) where section 24(3)*(e)* is applicable, of the name and address of the other data user concerned.

(2) Without prejudice to the generality of subsection (1), where -

(a) the personal data to which a data correction request relates is an expression of opinion; and

(b) the data user concerned is not satisfied that the opinion is inaccurate, then the data user shall -

(i) make a note, whether annexed to that data or elsewhere -

(A) of the matters in respect of which the opinion is considered by the requester to be inaccurate; and

(B) in such a way that that data cannot be used by a person (including the data user and a third party) without the note being drawn to the attention of, and being available for inspection by, that person; and

(ii) attach a copy of the note to the notice referred to in subsection (1) which relates to that request.

(3) In this section, "expression of opinion" includes an assertion of fact which -

(a) is unverifiable; or

(b) in all the circumstances of the case, is not practicable to verify.

26 Erasure of Personal Data no Longer Required

(1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was 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 must take all practicable steps to 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.

53 Employment-staff Planning

(1) Personal data which consists of information relevant to any staff planning proposal to -

(a) fill any series of positions of employment which are presently, or may become unfilled; or

(b) cease any group of individuals' employment, is exempt from the provisions of data protection principle 6 and section 18(1)*(b)*.

55 Relevant Process

(1) Personal data the subject of a relevant process is exempt from the provisions of data protection principle 6 and section 18(1)*(b)* until completion of that process.

(2) In this section –

"completion", in relation to a relevant process, means the making of the determination concerned referred to in paragraph *(a)* of the definition of "relevant process"; "relevant process" -

(a) subject to paragraph *(b)*, means any process whereby personal data is considered by one or more persons for the purpose of determining, or enabling there to be determined -

(i) the suitability, eligibility or qualifications of the data subject for -

(A) employment or appointment to office;

(B) promotion in employment or office or continuance in employment or office;

(C) removal from employment or office; or

(D) the awarding of contracts, awards (including academic and professional qualifications), scholarships, honours or other benefits;

(ii) whether any contract, award (including academic and professional qualifications), scholarship, honour or benefit relating to the data subject should be continued, modified or cancelled; or

(iii) whether any disciplinary action should be taken against the data subject for a breach of the terms of his employment or appointment to office;

(b) does not include any such process where no appeal, whether under an Ordinance or otherwise, may be made against any such determination.

56 Personal References

Personal data held by a data user which consists of a personal reference—

(*a*) given by an individual other than in the ordinary course of his occupation; and

(*b*) relevant to another individual's suitability or otherwise to fill any position of employment or office which is presently, or may become, unfilled,

is exempt from the provisions of data protection principle 6 and section 18(1)(*b*)—

(i) in any case, unless the individual referred to in paragraph (*a*) has informed the data user in writing that he has no objection to the reference being seen by the individual referred to in paragraph (*b*) (or words to the like effect); or

(ii) in the case of a reference given on or after the day on which this section comes into operation, until the individual referred to in paragraph (*b*) has been informed in writing that he has been accepted or rejected to fill that position or office (or words to the like effect),

whichever first occurs.

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),

is 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.

(1A) In subsection (1)*(c)*, "tax" includes any tax of a territory outside Hong Kong if –
(a) arrangements having effect under section 49(1A) of the Inland Revenue Ordinance (Cap. 112) are made with the government of that territory; and
(b) that tax is the subject of a provision of the arrangements that requires disclosure of information concerning tax of that territory.

(2) Personal data is exempt from the provisions of data protection principle 3 in any case in which-
(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data is held for any of those purposes); and
(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of those matters.

(6) In this section —
crime means—
(a) an offence under the laws of Hong Kong; or
(b) if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place;
offender means a person who commits a crime**.**

60A Self Incrimination

(1) If, as a result of complying with a request under a provision of data protection principle 6 or section 18(1)*(b)* in relation to any personal data, a data user might be incriminated in any proceedings for any offence other than an offence under this Ordinance, the data is exempt from that provision or section.

60B Legal Proceedings etc

Personal data is exempt from the provisions of data protection principle 3 if the use of the data is –
(a) required or authorised by or under any enactment, by any rule of law or by an order of a court in Hong Kong;
(b) required in connection with any legal proceedings in Hong Kong; or
(c) required for establishing, exercising or defending legal rights in Hong Kong.

63B Due Diligence Exercise

(1) Personal data transferred or disclosed by a data user for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction that involves—

(a) a transfer of the business or property of, or any shares in, the data user;
(b) a change in the shareholdings of the data user; or
(c) an amalgamation of the data user with another body,
is exempt from the provisions of data protection principle 3 if each of the conditions specified in subsection (2) is satisfied.

(2) The conditions are—
(a) the personal data transferred or disclosed is not more than necessary for the purpose of the due diligence exercise;
(b) goods, facilities or services which are the same as or similar to those provided by the data user to the data subject are to be provided to the data subject, on completion of the proposed business transaction, by a party to the transaction or a new body formed as a result of the transaction;
(c) it is not practicable to obtain the prescribed consent of the data subject for the transfer or disclosure.

(3) Subsection (1) does not apply if the primary purpose of the proposed business transaction is the transfer, disclosure or provision for gain of the personal data.

(4) If a data user transfers or discloses personal data to a person for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction described in subsection (1), the person—
(a) must only use the data for that purpose; and
(b) must, as soon as practicable after the completion of the due diligence exercise—
(i) return the personal data to the data user; and
(ii) destroy any record of the personal data that is kept by the person.

(5) A person who contravenes subsection (4) commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years.

(6) In this section—
due diligence exercise, in relation to a proposed business transaction, means the examination of the subject matter of the transaction to enable a party to decide whether to proceed with the transaction;
provision for gain, in relation to personal data, means provision of the data in return for money or other property, irrespective of whether-
(a) the return is contingent on any condition; or
(b) the person who provides the data retains any control over the use of the data.

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.

22 *April 2016*
Stephen Kai-yi WONG
Privacy Commissioner for Personal Data