



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

# **Inspection Report**

**(published under Section 48(1) of the Personal Data (Privacy)  
Ordinance, Chapter 486, Laws of Hong Kong)**

## **Personal Data System of a Data User in the Food and Beverage Industry**

**Report Number : R20 - 18950**

**Date Issued: 26 August 2020**

## Table of Contents

Executive Summary .....	1
I. Introduction .....	5
II. Inspection .....	6
III. Methodology .....	7
IV. Personal Data System and Data Flow .....	9
V. Findings and Recommendations .....	11
VI. Conclusion .....	24
VII. Salient points of the Code of Practice on Human Resource..... Management in Handling of the Personal Data of Prospective, Current and Former Employees	25
Annex A – Code of Practice on Human Resource Management	
Annex B – Data Protection Principles	
Annex C – A copy of the questionnaire	
Annex D – The assessment results of the compliance with the requirements of the Code of Practice on Human Resource Management	

## **Report on the Inspection of the Personal Data System of an Employer in the Food and Beverage Industry**

---

This report is relevant to an inspection carried out by the Privacy Commissioner for Personal Data, Hong Kong, pursuant to section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong in relation to the personal data system of an employer as a data user in the food and beverage industry and is published pursuant to section 48 of the Ordinance.

**Section 36** of the Ordinance provides that:-

*“Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

- (a) any personal data system used by a data user; or*
- (b) any personal data system used by a data user belonging to a class of data users,*

*for the purposes of ascertaining information to assist the Commissioner in making recommendations-*

- (i) to-*
  - (A) where paragraph (a) is applicable, the relevant data user;*
  - (B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and*
- (ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be.”*

The term “**personal data system**” is defined in **section 2(1)** of the Ordinance to mean “*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.*”

**Section 48** of the Ordinance provides that:-

*“(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

- (a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*
- (b) in such manner as he thinks fit.*

.....

*(3) Subject to subsection (4), a report published under subsection (1)... shall be so framed as to prevent the identity of any individual being ascertained from it.*

*(4) Subsection (3) shall not apply to any individual who is-*

- (a) the Commissioner or a prescribed officer;*
- (b) the relevant data user.”*

**Tony Chik-ting LAM**

**Acting Privacy Commissioner for Personal Data, Hong Kong**

**26 August 2020**

# **Inspection Report**

(published under Section 48(1) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

## **Personal Data System of An Employer in the Food and Beverage Industry**

### **Executive Summary**

#### **Background**

Raising data users' awareness of the importance of personal data privacy and promoting compliance with the Personal Data (Privacy) Ordinance (**Ordinance**), Chapter 486 of the Laws of Hong Kong, is one of the pivotal statutory duties of the Privacy Commissioner for Personal Data, Hong Kong (**Commissioner**).

Given that a massive volume and a broad range of personal data were collected and handled by employers in Hong Kong and more than 220,000 persons were employed by the food and beverage industry according to the recent employment statistics published by the Census and Statistics Department, the Commissioner considered that it would be in the public interest to carry out an inspection (**Inspection**) to review the employment-related personal data system of one of the leading companies in the food and beverage industry (**Employer**) pursuant to section 36 of the Ordinance.

With a view to identifying good practices and inadequacies from the perspective of data privacy protection, the entire life cycle of the employment-related data involved in the Employer's personal data system, including its privacy policy, forms and training materials were examined. The Commissioner considered that the findings and recommendations made after the Inspection would also serve as a guide to the industry and all employers in Hong Kong as a whole in ensuring compliance with the requirements under the Ordinance, in particular the Data Protection Principles (**DPPs**) of Schedule 1 to the Ordinance and the Code of Practice on Human Resource Management (**Code**).

## **Findings and Recommendations**

In the Inspection, the Commissioner noted that the Employer had strived to devote its efforts in privacy management in accordance with its business nature and operation mode. No material deficiencies were found on the part of the Employer in privacy protection matters although some room for improvement was identified.

The Commissioner was pleased to find that the Employer had complied with most of the requirements of the Code and was appreciative of some good practices of the Employers when handling personal data of job applicants and employees as shown below:-

- Notifying job applicants of the data retention period;
- Providing sample questions to interviewers to avoid collecting excessive personal data;
- No input of unsuccessful job applicants' personal data into the Human Resources system; and
- Security measures to protect employment-related data, including the following:
  - (a) certification of ISO/IEC 27001 on its information management system;
  - (b) robust password management; and
  - (c) rigorous access right control.

The Commissioner also identified some areas of improvement on the part of the Employer that were generally applicable to the industry and all employers in Hong Kong and thus made the following major recommendations:-

- To cease the practice of collecting partial Hong Kong Identity (**HKID**) Card number of job applicants and to completely obliterate such data previously collected;
- To ensure that each HKID Card copy of employees collected and held is marked with the word "COPY" across the entire image of the HKID Card;
- To ensure that all job applicants are provided with (a) Personal Information Collection Statement (**PICS**) if a job advertisement placed by an employer directly solicits personal data from job applicants, or (b) in the job

advertisements the identity of the contact person from whom the job applicants may obtain a copy of the PICS;

- To conduct timely erasure of job applicants' personal data collected through instant messaging applications;
- To ensure consistency of the retention period of employees' personal data as stated in the online privacy policy and the employment application form;
- To conduct regular data protection training for all employees and to regularly update related training materials; and
- To incorporate restrictive clauses in the agreement with paper disposal contractor and other contractors handling employees' personal data.

### **Salient points of the Code for Employers to follow in handling of the personal data of prospective, current and former employees**

The protection of privacy in relation to employment-related personal data is the concern of every member of staff in any company and the duty of every employer in Hong Kong. The Commissioner therefore issued the Code to provide practical guidance to employers and their staff on how to properly handle personal data of prospective, current and former employees during each phase of the employment process. The main salient points of the Code which all employers in Hong Kong should follow are set out below:-

#### *Prospective Employees*

- When an employer places a job advertisement that directly solicits personal data from job applicants, it should ensure that the PICS notification requirement is complied with in the advertisement. (paragraph 2.3.2 of the Code)
- An employer should not collect a copy of the HKID Card of a job applicant during the recruitment process unless and until the individual has accepted an offer of employment. (paragraph 2.2.4 of the Code)
- An employer should not retain personal data of unsuccessful applicants longer than two years from the date of rejecting the job applicant, unless the applicants have given their consent for the data to be retained longer. (paragraph 1.3.3.1 of the Code)

### *Current employees*

- An employer may collect personal data relating to the health condition of an employee if the collection is for a purpose directly related to (a) the assessment of the suitability of the employee's continuance in employment; or (b) the employer's administration of medical or other benefits or compensation provided to the employee. (paragraph 3.2.4 of the Code)
- 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 accurate and held securely and accessible only by authorised personnel on a "need-to-know" basis. (paragraph 3.3.1 of the Code)
- When employment-related data is transferred or disclosed to a third party, an employer should avoid transfer or disclosure of data in excess of what is necessary for the purpose of use by the third party. (paragraphs 3.11.1 and 3.11.4 of the Code)

### *Former employees*

- An employer must take all practicable steps to ensure that only relevant and necessary information of the former employee is retained after the employment ceases. (paragraph 4.2.1 of the Code)
- Personal data of a former employee should not be retained for more than seven years from the date the former employee ceases to be employed unless there is a subsisting reason that obliges the employer to retain the data for a longer period, or the former employee has given prescribed consent for the data to be retained beyond seven years. (paragraph 4.2.3 of the Code)
- An employer should not provide a reference concerning a former employee to a third party without first obtaining the employee's prescribed consent. (paragraph 4.5.1 of the Code)



# **Personal Data System of An Employer in the Food and Beverage Industry**

## **The Report**

### **(I) Introduction**

- 1.1 According to the statistics published by the Census and Statistics Department, the size of the total labour force in Hong Kong in 2019 was 3.97 million, which represented approximately 61% of the total population aged 15 and over<sup>1</sup>. Hence, employment-related personal data of these 3.97 million individuals would be / have been collected, processed, held and handled by employers or their agents / service providers. Employment-related personal data on job applicants, serving staff and former employees would generally include records of personal and family particulars (such as name, HKID Card number and copy, date of birth, address, contact information, etc.), education and qualifications, employment history, salary and allowances, bank account details, housing, medical records, leave and passages and retirement pension, etc.
- 1.2 The protection of privacy in relation to employment-related personal data is the concern of every member of staff in any company and the duty of every employer in Hong Kong. To provide practical guidance to employers and their staff on how to properly handle personal data during each phase of the employment process, the Commissioner exercised the powers conferred on him under section 12(1) of the Ordinance and issued the Code in September 2000 which took effect in April 2001. Necessitated by the amendments to the Ordinance and the need to update the provisions of the Code, the Code was revised once in April 2016.
- 1.3 The primary purpose of the Code is to provide practical guidance to data users who are employers and their staff on how to properly 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.
- 1.4 Failure to abide by the mandatory provisions of the 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 the Code,

---

<sup>1</sup> Source: <https://www.censtatd.gov.hk/hkstat/sub/sp200.jsp?tableID=008&ID=0&productType=8>

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.

- 1.5 According to the “Employment and Vacancies Statistics for March 2020”<sup>2</sup> released by the Census and Statistics Department in June 2020, the food and beverage industry employed more than 220,000 employees. Given the massive volume and broad range of personal data handled by the employers in this industry, the Commissioner considered that it would be in the public interest to carry out the Inspection on the employment-related personal data system of an employer of the food and beverage industry under section 36 of the Ordinance.
- 1.6 The Commissioner considered that the Inspection could assist him in identifying good practices and areas of inadequacies/ areas of improvement, and making corresponding recommendations on the compliance with the requirements under the Ordinance and the Code.
- 1.7 The employer selected (**Employer**) is a publicly listed restaurant and catering group operating in Hong Kong and other regions. The Inspection is only confined to the collection, handling, processing and use of employment-related personal data of the Employer’s flagship restaurant in Hong Kong, which operates about 160 outlets and hires more than 6,000 employees in Hong Kong.

## (II) Inspection

- 2.1 The Inspection Team (**Team**) examined the handling of employment-related personal data of the Employer from data collection to data disposal with a view to identifying good practices and areas of improvements from the perspective of data privacy protection. Due reference to the promotion of compliance with the requirements under the Ordinance, in particular the six DPPs of Schedule 1 to the Ordinance and the Code was made. The six DPPs cover the collection, accuracy, retention, use, security, transparency and access to personal data.
- 2.2 The Code and the six DPPs are respectively reproduced at **Annexes A and B** for easy reference.

---

<sup>2</sup> Source: <https://www.statistics.gov.hk/pub/B10500032020QQ01B0100.pdf>

### **(III) Methodology**

3.1 The Inspection comprised six major types of review work:

#### *Mystery visits*

3.2 The Team conducted mystery visits at job fairs and restaurants of the Employer for the purpose of gaining a thorough understanding on the workflow of processing job applications and the actual performance of individual staff to whom the task of handling of employment-related personal data was entrusted to, e.g. staff of the Human Resources Department and branch managers. The Team made job enquiries by means of instant messaging applications specified by the Employer.

#### *Policy review*

3.3 The Team examined the personal data privacy policies documented in policies, forms (e.g. employment application forms), job advertisements and training materials, and agreements with service providers (e.g. paper shredding service provider). The Team also made reference to its online privacy policy.

#### *Site inspections*

3.4 Site inspections at the two offices hosting the Human Resources Department, selected branches, central food processing centre and a warehouse were conducted for the purpose of (i) understanding the physical layout and security measures of the premises where employment-related personal data was collected, processed and stored; (ii) examining the equipment and systems used for collection, processing and storage of employment-related personal data; and (iii) examining papers and electronic records retained in the premises and computer systems with a view to identifying any irregularities/ inadequacies in terms of data protection.

#### *Walkthrough demonstration*

3.5 During site inspection, the Employer demonstrated to the Team their working procedures including access right restriction to the Human Resources system (**HR System**) and retrieval of personnel files, thereby enabling the Team to have a better understanding on how they collected, used and safeguarded personal data.

### *Interviews and enquiries*

- 3.6 The Team made verbal and written enquiries with the Employer before, during and after site inspection. Verbal enquiries were made through interviews with staff members ranking from management to operational levels at head office, selected branches and central food processing centre. These enabled the Team to understand how the staff members of the Employer handled personal data, their familiarity with internal policies relating to personal data privacy and the training they provided and received, as well as to what extent they complied with the internal policies and the requirements of the Code. Interviews and enquiries also enabled the Team to verify the observations.
- 3.7 The information sought through written enquiries assisted the Team in understanding the operation of the employment-related personal data system, reinforcing the documentary information obtained with observations at site inspection and identifying any cause for concern.

### *Questionnaire*

- 3.8 During site inspection, 26 staff members<sup>3</sup> who were granted access to employment-related personal data were invited to complete a questionnaire in relation to the Employer's internal policies and the requirements of the Code. The questionnaires formed part of the Inspection. A copy of the questionnaire is at **Annex C**.
- 3.9 Out of a total of 20 questions, six were related to the internal policies of the Employer whereas the remaining 14 questions focused on the requirements of the Code, e.g. collection of job applicants' personal data, accuracy of employment-related personal data, retention, use, security, and access of employment-related personal data.
- 3.10 All questionnaires were given to the respondents at the beginning of site inspection and collected before the completion of the site inspection.

---

<sup>3</sup> 26 staff members comprised 23 HR staff and 3 selected branch managers.

#### (IV) Personal Data System and Data Flow

##### *The Personal Data System*

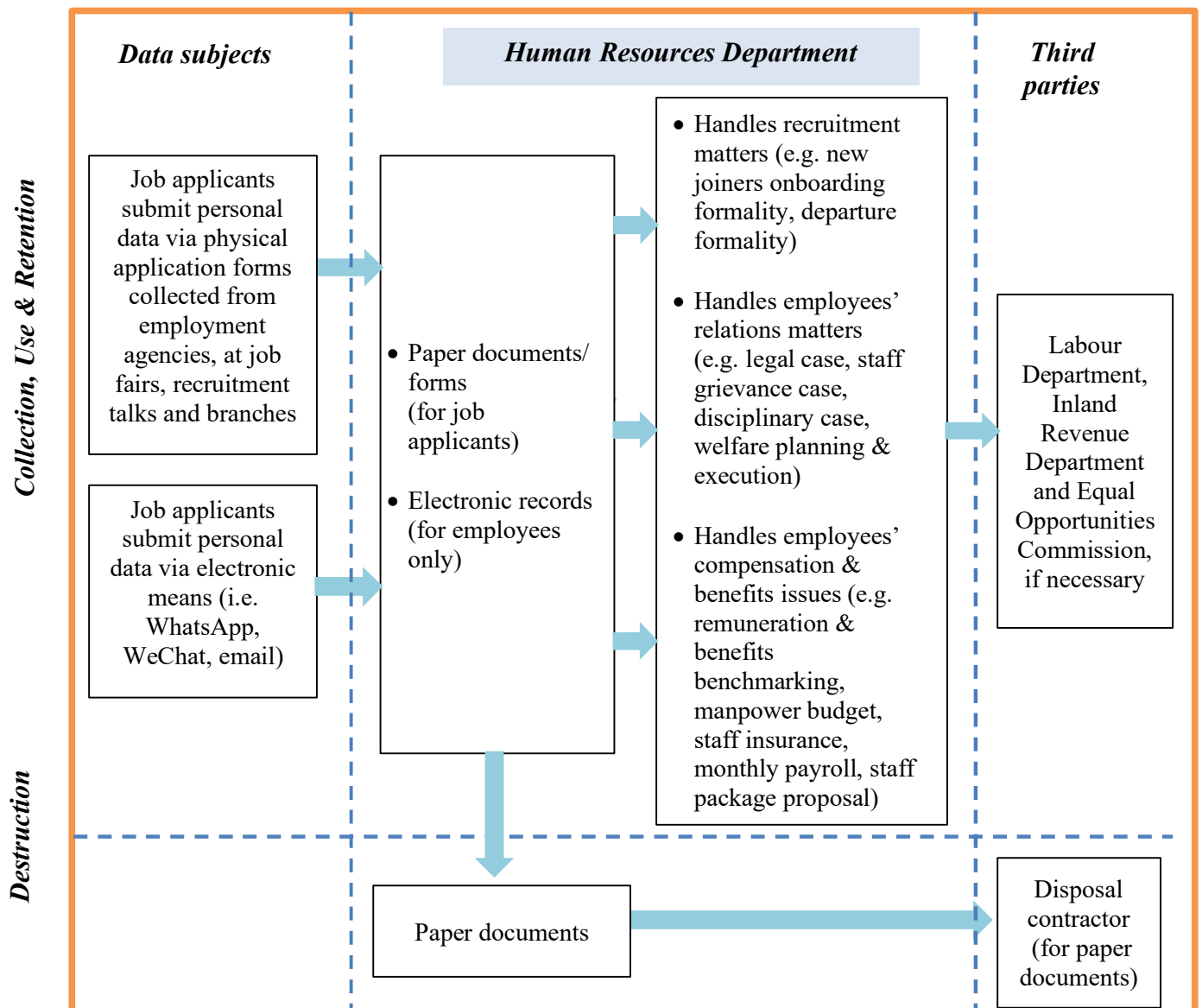
4.1 The personal data system that the Team inspected covered the HR System used to process personal data and the operation of the Human Resources Department, selected branches and central food processing centre in the collection, holding, processing or use of employment-related personal data. The types of personal data of job applicants, current and former employees of the Employer are tabulated below:

<b>Type of personal data</b>	<b>Job applicants</b>	<b>Current employees</b>	<b>Former employees</b>
Name	✓	✓	✓
Date of birth	Only year of birth	✓	✓
HKID Card number	Only first letter and first three digits	✓	✓
Correspondence address	✓	✓	✓
Residential and mobile phone numbers	✓	✓	✓
Email address	✓	✓	✓
Education and training background	✓	✓	✓
Professional qualification	✓	✓	✓
Employment history	✓	✓	✓
Place of birth	✗	✓	✓
Nationality	✗	✓	✓
Marital status	✗	✓	✓

Information of spouse/ emergency contact person	x	✓	✓
Bank account details	x	✓	✓
Community service/ public service history	x	✓	✓

## Personal Data Flow

4.2 The flow of personal data of job applicants, current employees and former employees is illustrated as follows:



## (V) Findings and Recommendations

- 5.1 Findings and recommendations made in this Report are based on the information provided by the Employer and the Team’s on-site observations, which may not be exhaustive. They should be regarded only as a reflection of the compliance level of the matters at the Inspection.
- 5.2 Our findings are derived from comparing the actual operation of the Employer in handling employment-related data with the requirements of the Code. The Code is divided into four sections:
- Section 1 – General requirements;  
Section 2 – Recruitment;  
Section 3 – Current employment; and  
Section 4 – Former employees’ matters
- 5.3 Our assessment findings took the forms of (i) conformity, (ii) non-conformity, and (iii) not applicable when comparing with the requirements of the Code. Remarks were made in each instance of non-conformity. The detailed findings are at **Annex D**.
- 5.4 The Team found that the Employer had fully complied with the requirements of Sections 3 and 4 of the Code. However, two non-conformity instances were noted in Sections 1 and 2 respectively.

<b>Section</b>	<b>Non-conformity</b>	<b>Details of non-conformity</b>
Section 1 (General requirements)  a. Paragraph 1.7.3 b. Paragraph 1.7.4	Two out of 28 items	a. Excessive collection of partial HKID Card number of job applicants.  b. Failure to mark the word “COPY” on a copy of an employee’s Hong Kong Identity Card.
Section 2 (Recruitment) a. Paragraph 2.2.3 b. Paragraph 2.3.2	Two out of 29 items	a. Collection of partial HKID Card number of job applicants did not meet the requirements of paragraph 2.2.3.  b. Some advertisements on recruitment platforms invited job applicants to submit resume to the Human Resources Department but the

		advertisements did not expressly identify the contact person from whom applicants might obtain a copy of the PICS.
Section 3 (Current employment)	None	Not applicable
Section 4 (Former employees' matters)	None	Not applicable

### **Good practices of the Employer in Handling Employment-Related Personal Data**

5.5 Among those conformities are praiseworthy practices that could serve as good examples for other employers. These good practices are tabulated below:-

***1. Notifying job applicants of the retention period of personal data (paragraphs 1.2 and 1.3.3 of the Code)***

5.6 Paragraph 1.2 of the Code sets out the notification requirements on collection of personal data of job applicants. The Employer fully informed the job applicants of the notification requirements in the Notes for Applicants in the Employment Application Form, which stated the following:-

- (i) personal data collected will be used by the Employer or its subsidiaries or associated companies to assess the job applicant's suitability to assume the job duties of the position and to determine preliminary remuneration, bonus payment and benefits package;
- (ii) which data is regarded as mandatory for selection purposes and that failure to provide these data may influence the processing and outcome of the application;
- (iii) when there are vacancies in the group of companies during the period, the application may be transferred to them;
- (iv) the right to request access to and correction of personal data; and
- (v) email address and fax number of the Human Resources Department to which the job applicants shall contact in their exercise of the right to request access to and correction of personal data.

5.7 On top of the information mentioned above, the Employer also notified job applicants that personal data of unsuccessful applicants would be retained for a year. This piece of additional information reflected high transparency in terms of



personal data protection, which would in turn give job applicants assurance and peace of mind when submitting their data.

**2. *Providing sample questions to interviewers to avoid collecting excessive personal data at job interviews (paragraph 2.2.2 of the Code)***

5.8 Paragraph 2.2.2 of the Code states that 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.

5.9 To ensure that its employees would comply with the above collection requirements, the Employer explicitly stated in its HR policy that “*During interview, only questions relating to job nature and the applicant’s ability could be asked. The applicant’s sensitive personal data, such as marital status and family conditions should not be asked to avoid contravening the regulations governing privacy and discrimination.*”

5.10 Besides, the Employer’s training materials provide sample interview questions to the staff who would perform job interviews for reference. The Commissioner reviewed the sample questions and noted that they were all job-related and no questions would request collection of excessive personal data from job applicants.

**3. *No input of unsuccessful job applicants’ personal data into the HR system (paragraph 2.2 of the Code)***

5.11 The Employer would only enter personal data of employees into the HR System. Personal data of successful job applicants who did not show up for work and unsuccessful job applicants would not be entered and stored in the HR System. This practice is commendable as it would minimize the inherent risk of retaining data longer than necessary.

**4. *Security measures to protect employment-related data (paragraph 1.4 of the Code)***

**(a) *Certification of ISO/IEC 27001 (paragraph 1.4 of the Code)***

5.12 The Employer’s information management system has been certified as being compliant with ISO/IEC 27001 since 2015. ISO/IEC 27001 is a standard primarily concerning the requirements for establishing, implementing, maintaining and improving an information security management system. According to the Sustainability Report 2018/19 of the Employer, the certification

of ISO/IEC 27001 included its corporate policy on personal data privacy, data access control mechanism, ongoing communication and training, internal control review, improving cyber-attack protection, third-party reviews.

***(b) Robust and rigorous password management (paragraph 1.4.2 of the Code)***

5.13 The Information Technology Policy of the Employer stipulated that a password must be changed once every three months and its setup must comply with specific length and combination requirements (e.g. 8-character password including either capital letters, numbers or symbols (at least 2 out of 3 required)). It also stated that users must not share passwords among themselves. This requirement also applied to the HR System.

5.14 Furthermore, it is a company-wide policy of the Employer that repeatedly entering wrong passwords for 5 times to access an account would result in suspension of the account until unlock procedures are performed by its IT personnel.

***(c) Access right control on need-to-know basis (paragraph 1.4.1 of the Code)***

5.15 Although the entire Human Resources Department would come in contact with employment-related data, the access right to the HR System was granted and linked to the job role / grade among Human Resources team on a need-to-know basis.

5.16 Furthermore, the Employer would conduct a review on the access right at a regular interval of six months.

***5. Proactive measures in upholding personal data protection (paragraphs 1.4.1 and 1.3 of the Code)***

5.17 Each employee of the Employer is required to sign a document entitled 「個人資料(私隱)保障守則」 which listed out non-exhaustive prohibited acts that might lead to contravention of the Ordinance, such as copying, downloading and videotaping other employees' employment terms and conditions, attendance records, and failure to lock up restricted documents such as job application forms, sick leave certificates, etc. By signing the document, the employees agreed to comply with the requirements of the document and the Employer's Privacy Policy.

5.18 The Employer acknowledged the importance of accuracy of the employment-related data held by it and had put in place strict initiatives such as cross checking of data entries by Human Resources staff and reminding its employees of updating any change of personal data on an annual basis, e.g. address or bank account details.

### **Areas for Improvement and Recommendations**

5.19 Despite the above good practices adopted by the Employer, the Team noted the following inadequacies that called for improvements. As pointed out in paragraph 5.4 above, there were four non-conformity instances noted during our Inspection. Given that each instance of non-conformity might have impact on data protection, the Employer is advised to take on board our recommendations and take necessary actions set out in the ensuing paragraphs, depending on the impact level and potential harm to the Employer and/ or its employees and/ or job applicants.

#### ***Non-compliance with the Code***

##### ***1. Excessive collection of first letter and three digits of HKID Card number of job applicants (paragraphs 1.7.3.1 and 2.2.3 of the Code)***

5.20 Among the non-conformity instances noted with regard to Sections 1 and 2 of the Code, collection of excessive personal data of job applicants was amongst the greatest privacy concern that the Employer faced.

5.21 From our previous cases and observations, we noted that it has been a long-established practice for employers in Hong Kong to collect job applicants' HKID Card number indiscriminately. The Employer required job applicants to provide the first letter and three digits of HKID Card number in the job application form. In response to our enquiry, the Employer merely explained that the collection of the partial HKID Card number of job applicants was for verification purpose without further elaboration.

5.22 According to paragraph 1.7.3.1 of the Code, an employer may collect the HKID Card number of a job applicant if the prescribed criteria set out in paragraph 2.2.3 of the Code are met. Under paragraph 2.2.3, a data user including the Employer should not collect the HKID Card number of an individual except all of the prescribed situations thereof are satisfied. The prescribed situations under paragraph 2.2.3 of the Code are tabulated below:-

- 2.2.3.1 The employer has a general policy to retain the HKID Card numbers of former employees and unsuccessful job applicants for a certain period;
  - 2.2.3.2 The employer collects HKID 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.
- 5.23 As pointed out in paragraph 5.21 above, the Employer explained that the collection of the first letter and first three digits of HKID Card number of job applicants was for identity verification. Whilst the Employer, like other employers in Hong Kong, should inspect prospective employees' identity documents before employing him/ her to fulfil statutory requirements, the Commissioner considered that requiring job applicants to present their identity documents before the job interview could serve the purpose of identity verification, taking into account in particular that the Employer had yet to decide to employ the job applicants.
- 5.24 Besides, one member of the Team conducted mystery visits to two of the branch restaurants of the Employer in the capacity of a job applicant. Despite the fact that he did not provide the first letter and first three digits of his HKID Card number in the job application forms or present his HKID Card for verifying the personal information provided on the job application forms, he was interviewed. Furthermore, as the partial HKID Card number of unsuccessful job applicants would not be inputted into the HR System, it would not be reasonably practicable for the Employer to check whether the job applicants had applied for the post before. The Team also noted that the Employer requested job applicants to declare whether they had ever been employed by the Employer or its subsidiaries. If "yes", the job applicant concerned would be required to state the position, the department and branch, employment period and last salary. The Commissioner considered that the declaration made by the job applicants would suffice.

5.25 In view of the above, the Commissioner found that the collection of the partial HKID Card number of job applicants was excessive and unnecessary, serving no purpose at all.

**Recommendation:**

1. The Employer should cease the practice of collecting partial HKID Card number of job applicants and to completely obliterate such data previously collected.

**2. *Failure to mark the word “COPY” on a copy of employee’s HKID Card (paragraph 1.7.4 of the Code)***

5.26 Under paragraph 1.7.4 of the Code, an employer must check any copy of the HKID Card against the original card and mark it with the word “COPY” across the entire image of the HKID Card. When the Team performed a random check in the Inspection, the Team discovered that the Employer had failed to stamp “COPY” across a copy of HKID of its employee.

**Recommendation:**

2. The Employer should ensure that each HKID Card copy of employees collected and held is marked with the word “COPY” across the entire image of the HKID Card.

**3. *Failure to expressly identify the contact person from whom job applicants might obtain a copy of the Personal Information Collection Statement in the job advertisements (paragraph 2.3.2 of the Code)***

5.27 According to paragraph 2.3.2 of the Code, where an employer advertises a vacancy in a job advertisement that directly solicits personal data from job applicants, it should ensure that the PICS notification requirement is complied with in the advertisement, unless (1) the advertisement invites job applicants to respond by filling in a job application form that prescribes the PICS notification; or (2) the advertisement expressly identifies the contact person from whom applicants may obtain a copy of the PICS.

5.28 The Commissioner noted that while most of the recruitment channels adopted by the Employer invited job applicants to respond by filling in the Employment Application Form that prescribed the PICS notification, he noted that some recruitment channels such as online advertisements and instant messaging applications adopted by the Employer neither provided PICS nor identified the contact person from whom the job applicants may obtain a copy of the PICS, as set out in the table below:-

<b>Recruitment channels</b>	<b>Any PICS or identity of the contact person from whom the job applicants may obtain a copy of the PICS</b>
Labour Department <sup>4</sup>	Yes
Onsite recruitment at restaurants	Yes
Online advertisements	No
Instant messaging applications	No
Agency (for relatively senior posts)	Yes

**Recommendation:**

3. The Employer should ensure that all job applicants are provided with PICS at the time of collection of personal data or the identity of the contact person in the job advertisements from whom the job applicants may obtain a copy of the PICS.

***Other inadequacies noted***

5.29 The Commissioner also noted the following inadequacies on the part of Employer, which called for improvements.

<sup>4</sup> Labour Department provides free recruitment services to employers by allowing them to post vacancies online with its Interactive Employment Service.

***Failure to conduct timely erasure of job applicants' personal data collected through instant messaging applications***

- 5.30 Apart from the traditional recruitment channels, the Employer leveraged instant messaging applications including WhatsApp and WeChat to recruit talents. In order to expedite the recruitment process, the Employer invited job applicants for the posts of cleaner, cashier, kitchen worker, chef, etc. to contact them via this channel for job interviews. As a result, job applicants would make use of these instant messaging applications to communicate with the Employer and provide at least their basic personal information, such as name, contact number and work experience for the purpose of arranging job interviews.
- 5.31 However, the Team found that the personal data of job applicants so collected through the instant messaging applications were not erased regularly. The Employer's data retention policy did not cover the erasure of the personal data collected through this channel. It highlighted the lack of personal data inventory as a result of which the Employer did not know what kind of personal data it held, where it was held and when it would be erased.
- 5.32 Though only minimal personal data e.g. name, phone number, preferred working location would be collected, the Employer is duty bound to ensure that the personal data stored in the instant messaging applications should be erased regularly so as to avoid retention of job applicants' personal data longer than necessary.

**Recommendation:**

4. DPP2(2) requires data users to take all practicable steps to ensure that personal data is not kept longer than is necessary and section 26 of the Ordinance requires data users to take all practicable steps to erase personal data no longer required. The Employer should incorporate in its internal policy the requirement for erasure of personal data collected through instant messaging applications and conduct periodic checking to ensure that its staff comply with such policy. The Employer is also advised to prepare a personal data inventory such that it could ascertain what kinds of personal data it holds, where they are held and when they are to be erased.

***Discrepancy of retention period of personal data stated in the Employer’s online privacy policy and the Employment Application Form***

5.33 The Employer had a data retention policy in place, specifying that unsuccessful job applicants’ personal data would only be held for one year. However, according to the Privacy Policy posted on its website, the Employer shall retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years from the day on which the recruitment period ends as opposed to one year as set out in the Employment Application Form. This may cause confusion to job applicants.

**Recommendation:**

5. To avoid any confusion over the retention period of unsuccessful job applicants’ personal data, the Employer should rectify the discrepancy of the retention period by amending its online privacy policy accordingly.

***Lack of data protection training and tailor-made training materials***

5.34 Data protection training is vital and should be given to all employees who would handle personal data, including those who are tasked with handling employment-related personal data, such as branch managers who are frequently involved in onsite recruitment, on a regular basis.

5.35 The Team noted that the Employer merely organised one seminar on “Introduction to PDPO” to its staff members during year 2017 to 2019. Furthermore, the training materials provided by the Employer merely covered the background of the Ordinance, six DPPs, direct marketing without any case sharing on handling employment-related data. All in all, the frequency and the comprehensiveness of the training were far from satisfactory.

***Non-familiarity with the Code by Relevant Staff Members***

5.36 As pointed out in paragraph 3.8 above, the Team handed out and received 26 questionnaires. The purpose of the questionnaire was to ascertain the level of awareness among the staff in relation to the internal HR policies of the Employer, how these policies were applied in the discharge of their day-to-day duties and to what extent they were familiar with the requirements of the Code.



- 5.37 The questionnaire comprised two parts. The first six questions focused on the internal policies of the Employer while the remaining 14 questions concerned the requirements of the Code.
- 5.38 The results of the first six questions, which focused on the internal policies of the Employer, were largely satisfactory. Specifically, more than 80% of respondents were aware of the rule on the integrity checking on job applicants and the collection of the details of job applicants'/ employees' medical history. Nevertheless, the performance of the respondents in answering the remaining 14 questions revealed that the staff were rather unfamiliar with the requirements of the Code. Although all respondents could answer correctly that HKID Card number should not appear on staff card and more than 90% of respondents realised that disclosure of the identity of an employee involved in a disciplinary finding to all staff was not allowed, around 60% of the respondents failed to discern properly the requisite content of a PICS and the obligations regarding the compliance with a DAR as required by the Code.
- 5.39 The remaining 14 questions were related to the requirements of the Code. Whilst all respondents provided correct answers to Question 11 and 13, less than half respondents provided correct answers to the Questions 8, 18, 19 and 20. This reflected inadequacies of knowledge in the areas of general understanding on the definition of "personal data" under the Ordinance, PICS and handling of data access request.
- 5.40 When it came to the performance of each individual respondent group (i.e. staff of Human Resources Department and the branch managers), the result of the HR staff stood in stark contrast with that of the branch managers. HR staff scored 13.8 on average in the questionnaire<sup>5</sup> whereas the branch staff could merely obtain a mean score of 6.7, far below the par. Despite the sample size of the branch managers being smaller than that of the HR staff, the stark disparity in the performance of the questionnaire as reflected by the mean scores between these two groups highlighted the lack of training on data protection and internal policies provided to the branch managers. It would come as no surprise to us that the core duties of branch managers are not mainly related to human resources, but they are heavily involved in recruitment process, i.e. onsite recruitment.
- 5.41 All in all, the unfamiliarity with the requirements of the Code and the internal policies necessitated the need for the Employer to re-design the training materials.

---

<sup>5</sup> Each question (20 in total) of the questionnaire carried equal mark.

**Recommendation:**

6. In view of the size of the workforce of the Employer and the massive employment-related data being handled, the Employer is strongly advised to re-design its training materials by including case studies in addition to data governance and Privacy Management Programme elements. The training for personal data protection and internal policies should not be limited to introduction courses or workshops, but also relevant information provided regularly through emails or internal circulars, etc.

***Lack of restrictive clauses on the service agreement with the paper disposal contractor***

- 5.42 Pursuant to DPP4, data users including the Employer are required to take all reasonably practicable steps to safeguard personal data held by them against unauthorised or accidental access, processing, erasure, loss or use. This responsibility covers the entire data life cycle from data collection to final disposal.
- 5.43 Personal data leakage incidents may occur as a result of insufficient steps being taken by the data processors<sup>6</sup> to protect the personal data entrusted to them. By virtue of section 65(2) of the Ordinance, any act done or practice engaged in by an agent for another person with the latter's authority shall be treated as done or engaged in by both that other person and the agent.
- 5.44 The Employer as a data user remains accountable for any unauthorised or accidental access of personal data to be shredded by the contractor. Hence, it is imperative for the Employer to use contractual or other means and auditing mechanism to monitor the paper disposal contractor's compliance with the data protection requirements.
- 5.45 The Team noted that the service agreement between the Employer and the paper disposal contractor had explicitly indicated that all materials collected would be treated in the strict confidence and security. The staff of the service provider shall not in any way make use of, extract, copy, transfer, disclose or leak any contextual or pictorial contents of any documents. The service provider would destroy the

---

<sup>6</sup> Under section 2(1) of the Ordinance, a data user means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. Under section 2(12) of the Ordinance, a person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, the data for any of his own purposes.

personal data within the next working day after their collection of the documents from the Employer's premises.

5.46 However, there is no clause in the service agreement which (1) prohibits the paper disposal contractor from subcontracting the paper shredding service to any third parties, (2) sets out the consequences of violation of the service agreement on the part of the paper disposal contractor. Furthermore, the Employer was not vested with a right to audit and inspect how the paper disposal contractor handled the personal data collected from the Employer. More importantly, the service agreement lacked any clause governing the report of data breach or irregularity on the part of the paper disposal contractor.

5.47 The said measures are not exhaustive and the Employer may take other steps to comply with requirements of the Code and the Ordinance.

**Recommendation:**

7. The Employer is advised to incorporate more stringent control measures in the service agreement with the paper disposal contractor, for example:-
  - (i) The paper disposal contractor is prohibited from sub-contracting the paper shredding service to any third party unless with the consent of the Employer;
  - (ii) The paper disposal contractor should report any data breach incidents to the Employer immediately;
  - (iii) The consequences for breach of the contract; and
  - (iv) The Employer should be given a right to audit and inspect how the paper disposal contractor handles personal data.

## **(VI) Conclusion**

- 6.1 The Commissioner is pleased to note that the Employer has committed to upholding data protection of employment-related personal data as eagerly as it has committed to ensuring provision of high standards in food quality and service to their customers. There being room for improvement on the part of the Employer, the Inspection also serves as a good opportunity for the Commissioner to assess the personal data system of the Employer and make recommendations as set out above to the Employer for enhancing and strengthening its privacy management, which would definitely be of useful reference to other employers in the same industry and all employers in Hong Kong for the purpose of ensuring compliance with the requirements under the Ordinance and the Code.
- 6.2 The Commissioner always advocates the use and benefits of a Privacy Management Programme and strongly encourages all data users to adopt the programme not only to effectively manage their employees and customers' personal data, but also to facilitate their compliance with the requirements under the Ordinance, build trust with the employees and customers and enhance their reputation as well as goodwill.
- 6.3 The Commissioner is thankful for the cooperation of the Employer and its staff, which is pivotal to the Team's understanding of the data flow in the Employer and the operation of its personal data system. He fully appreciates all the assistance rendered by them beyond their normal duties.
- 6.4 The Commissioner sincerely hopes that this Report will be of value to the Employer and other employers in the same industry and all employers in Hong Kong, as well as to nurturing a culture of protecting and respecting personal data privacy.
- 6.5 Last but not least, employers as data users should understand that there is a high expectation from the general public for employers to hold a higher ethical standard and to meet the requirements of laws and regulations. Data users are expected to implement data ethics in their daily operations, and to fully reap the benefits of the data-driven economy while protecting and respecting the fundamental human rights (including the right to privacy), interests and freedoms of individuals.

## **(VII) Salient points of the Code for Employers to follow in handling personal data of prospective, current and former employees**

- 7.1 According to the 2019 statistics released by the Companies Registry, the number of local companies and non-Hong Kong companies remained registered in Hong Kong was 1,380,185<sup>7</sup> and 12,494<sup>8</sup> respectively. Among which, over 340,000<sup>9</sup> registered companies are small and medium enterprises (SMEs). SMEs constitute over 98% of our business establishments in Hong Kong and employ about 45% of our workforce in the private sector. As pointed out in paragraph 1.1 above, the total labour force in 2019 was 3.97 million.
- 7.2 The Commissioner is mindful that it is a challenge for employers to apply the provisions of and requirements under the Ordinance in the course of performing human resource management functions and activities. It is particularly the case with SMEs as they generally lack resources and some of them may not even have a specialised human resources management department.
- 7.3 Against this background and in view that the protection of privacy in relation to employment-related personal data is the concern of every member of staff in any companies and the duty of every employer in Hong Kong, the Commissioner issued the Code to provide practical guidance to employers and their staff on how to properly handle personal data of prospective, current and former employees during each phase of the employment process. Salient points of the Code which all employers in Hong Kong should follow are set out below:-

### *Prospective Employees*

- When an employer places a job advertisement that directly solicits personal data from job applicants, it should ensure that the PICS notification requirement is complied with in the advertisement. (paragraph 2.3.2 of the Code)
- An employer should not solicit personal data from job applicants in a job advertisement that provides no identification of either the employer or its agent. (paragraph 2.3.3 of the Code)

---

<sup>7</sup> Source: <https://www.cr.gov.hk/en/publication/fact-stat/statistics/local-companies-registered/since-2014.htm>

<sup>8</sup> Source: <https://www.cr.gov.hk/en/publication/fact-stat/statistics/registered-non-hk-companies.htm>

<sup>9</sup> Source: [https://www.tid.gov.hk/english/smes\\_industry/smes/smes\\_content.html](https://www.tid.gov.hk/english/smes_industry/smes/smes_content.html)

- An employer should not collect a copy of the HKID Card of a job applicant during the recruitment process unless and until the individual has accepted an offer of employment. (paragraph 2.2.4 of the Code)
- Personal data concerning the health condition of a selected candidate may be collected by means of a pre-employment medical examination if the data directly relates to the inherent requirements of the job, and employment is conditional upon the fulfilment of the medical examination. However, such data should only be collected after the employer has made a conditional offer of employment to the selected candidate. (paragraph 2.9.1 of the Code)
- An employer should not retain personal data of unsuccessful applicants longer than two years from the date of rejecting the job applicant, unless the applicants have given their consent for the data to be retained for a longer period. (paragraph 1.3.3.1 of the Code)

#### *Current employees*

- An employer may collect personal data from an employee and his family members for the purpose of employment, or to fulfil the lawful requirements that regulates the affairs of the employer. (paragraph 3.2.1 of the Code)
- An employer may collect personal data relating to the health condition of an employee if the collection is for a purpose directly related to (a) the assessment of the suitability of the employee's continuance in employment; or (b) the employer's administration of medical or other benefits or compensation provided to the employee. (paragraph 3.2.4 of the Code)
- 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 accurate and held securely and accessible only by authorised personnel on a "need-to-know" basis. (paragraph 3.3.1 of the Code)
- Information compiled about an employee in the process of disciplinary proceedings, performance appraisal or promotion planning should only be used for purposes directly related to the process concerned. The information should not be disclosed to a third party unless such party has legitimate reasons to have access to the data. (paragraphs 3.3.2, 3.4.3 and 3.6.2 of the Code)

- When employment-related data is transferred or disclosed to a third party, an employer should avoid transfer or disclosure of data in excess of what is necessary for the purpose of use by the third party. (paragraphs 3.11.1 and 3.11.4 of the Code)
- An employer who engages a third-party organisation to perform its employment-related functions must use contractual or other means to ensure that the data transferred to the third-party organisation is protected against unauthorised or accidental access, processing, erasure, loss or use. (paragraph 3.11.2 of the Code)

### *Former employees*

- An employer must take all practicable steps to ensure that only relevant and necessary information of the former employee is retained after the employment relationship ends. (paragraph 4.2.1 of the Code)
- Personal data of a former employee should not be retained for seven years from the date the former employee ceases to be employed, unless there is a subsisting reason that obliges the employer to retain the data for a longer period; or the former employee has given prescribed consent for the data to be retained beyond seven years. (paragraph 4.2.3 of the Code)
- An employer should not provide a reference concerning a former employee to a third party without first obtaining the employee's prescribed consent. (paragraph 4.5.1 of the Code)
- An employer who finds it necessary to announce publicly that a former employee has left appointment, and no longer represents it, should include only the minimum information required to identify the employee concerned. (paragraph 4.6.1 of the Code)

**Annex A**

**For the details of “Code of Practice on Human Resource Management”, please visit:**

[https://www.pcpd.org.hk/english/data\\_privacy\\_law/code\\_of\\_practices/files/PCPD\\_HR\\_Booklet\\_Eng\\_AW07\\_Web.pdf](https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf)



**Annex B**

**For the details of the six “Data Protection Principles”,  
please visit:**

[https://www.elegislation.gov.hk/hk/cap486!en?INDEX\\_CS  
=N](https://www.elegislation.gov.hk/hk/cap486!en?INDEX_CS=N)

PCPD use only: Headquarters staff / Branch staff

**Office of the Privacy Commissioner for Personal Data, Hong Kong  
Questionnaire**

The Privacy Commissioner for Personal Data, Hong Kong is now carrying out an inspection of the employment-related personal data system of your company under section 36 of the Personal Data (Privacy) Ordinance. This questionnaire is one part of the inspection and would be filled out anonymously. All information collected would be used for integrated analysis.

There are 20 questions in this questionnaire. Questions 1 to 6 pertain to the internal policy of your company while questions 7 to 20 are related to the Code of Practice on Human Resource Management issued by this office. Please read the questions carefully and choose the appropriate answer. Thank you for your assistance.

If you have any questions about the questionnaire, please contact PCPD staff.

**The internal policy of your company**

1. If a job demands a pre-employment medical examination, the job applicant has to submit a complete medical check report to the human resources department. Simply providing a “fit-for-employment” proof issued by a medical practitioner is insufficient for ascertaining whether the job applicant’s health condition is suitable for the job.
  - (a) True
  - (b) False
  - (c) Depending on circumstances
  
2. During an interview, job applicants should be asked about questions of their family status (including number of children).
  - (a) True
  - (b) False
  - (c) Depending on circumstances

3. The branch has to destroy unsuccessful job applicants' personal data monthly by itself.
  - (a) True
  - (b) False
  - (c) Depending on circumstances
  
4. If an employee would like to make a data access request, to whom should he contact?
  - (a) Direct supervisor
  - (b) Head of department
  - (c) Human resources manager
  
5. Your company would carry out integrity check on all job applicants.
  - (a) True
  - (b) False
  
6. After obtaining the approval of the general manager, the district manager can request the human resources department to email the personnel file of a subordinate for the purpose of performance assessment.
  - (a) True
  - (b) False
  - (c) Depending on circumstances

**Code of Practice on Human Resource Management (Code)**

7. If an employer posts a job advertisement to solicit job applicants' personal data directly, which of the following information must be provided in the advertisement?
  - (a) Identity of employer
  - (b) Contact number of employer
  - (c) Application deadline
  
8. On or before the collection of personal data, the employer is not required to inform the job applicants of which of the following information?
  - (a) The purpose of the collection of data
  - (b) Class of transferees of the data
  - (c) Retention period of the data

9. During interview, an employer can collect job applicants' Hong Kong Identity Card copies for record-keeping.
- (a) True
  - (b) False
10. Without any subsisting reason or job applicants' prescribed consent, an employer cannot retain unsuccessful job applicants' personal data for more than two years (from the date of rejecting the applicant).
- (a) True
  - (b) False
11. Staff card should bear the holder's Hong Kong Identity Card number.
- (a) True
  - (b) False
12. If an employee applies for a sick leave, the employer is not required to know the details of treatment prescribed for the employee.
- (a) True
  - (b) False
13. When an employer issues an internal announcement regarding a disciplinary action against any employee, he can disclose the identity of the employee for reminding purpose.
- (a) True
  - (b) False
14. Under which of the following circumstances can an employer transfer employees' personal data to other organisations?
- (a) Outsourcing human resources processing work
  - (b) Promoting business products to partnering companies
  - (c) Assisting a human resources system service provider to carry out a user acceptance test
15. Without any subsisting reason or former employees' prescribed consent, an employer cannot retain former employees' personal data for more than five years (from the date of ceasing employment).
- (a) True
  - (b) False

16. An employer is not required to take all practicable steps to maintain the accuracy of personal data of those employees who have left employment.
- (a) True
  - (b) False
17. Under which of the following circumstances can an employer provide a job reference of a former employee to a third party? Please choose all the answer(s) which comply with the Code.
- i. Obtained the former employee's consent
  - ii. Obtained the former employee's consent from the third party
  - iii. Obtained the third party's employment proof of the former employee
- (a) (i)
  - (b) (i) & (ii)
  - (c) All of the above
18. Personal data of a deceased former employee is not covered by the Code.
- (a) True
  - (b) False
19. An employer has to provide a copy of the requested personal data within \_\_\_\_\_ after the receipt of a data access request.
- (a) 20 days
  - (b) 1 month
  - (c) 40 days
20. An employer can refuse to comply with a data access request if the document contains personal data of more than one individual.
- (a) True
  - (b) False

- End-

1 General Requirements

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>1.2 Notification Requirements on Collection of Personal Data</b>				
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:	1.2.1.1 the purpose for which the data is to be used;	✓	This information was provided in the Personal Information Collection Statement of the job application form.
		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.		
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.		✓	This information was provided in the Personal Information Collection Statement of the job application form.

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
<b>Transferee Statement : Classes of Transferees</b>				
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.	✓		
		This information was provided in the Personal Information Collection Statement of the job application form.		
<b>Optional or Obligatory Provision of Data</b>				
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. The consequences of not providing such data should also be stated explicitly unless this is obvious from the circumstances.	✓		
		This information was provided in the Personal Information Collection Statement of the job application form.		
<b>Data Access and Correction Rights</b>				
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.	✓		
		This information was provided in the Personal Information Collection Statement of the job application form.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
<b>Employment-related Personal Data Collected before the Ordinance came into Effect</b>				
1.2.6	An employer may continue to use employment-related personal data collected before 20 December 1996 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.	✓		
		The handling of personal data collected before 20 December 1996 was no different from that collected thereafter.		
<b>1.3 Accuracy and Retention of Employment-related Personal Data</b>				
<b>Accuracy of Employment-related Data</b>				
1.3.1	An employer should take all practicable steps to ensure that the employment-related data it holds about employees is:	✓		
		Personal data inputted into the HR system was cross-checked by staff members.		
		HR Department issued notice annually reminding staff members to inform HR any changes of personal data by completing Change of Personal Data Form.		
	1.3.1.1 accurate having regard to the purpose for which the data is used; 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.			



		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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:	1.3.2.1 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.	The handling of personal data collected before 20 December 1996 was no different from that collected thereafter.	
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;	Unsuccessful job applicants' application forms were destroyed within a year from the date of rejecting the candidates. Personnel files of former employees were destroyed after 7 years. These requirements were mentioned in the Human Resource Policy.	

		Assessment Findings		
		Conformity	Non-conformity	N/A
	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.		
<b>1.4 Security Measures to Protect Employment-related Data</b>				
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.		✓	
		Trainings in relation to personal data privacy and security were arranged to staff members in 2017 and 2019.		
<b>Security through Controlled Access to Employment-related Personal Data</b>				
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.		✓	
		Files containing personal data were password-protected when they were sent via email or shared in a common drive.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.	✓		
		Contractual agreements were signed with third parties performing human resources activities to ensure the third parties applied security protection to personal data.		
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.	✓		
		Document disposal contractor was appointed to carry out document destruction process. Contractual agreement was signed with it to ensure it applied security protection to personal data.		
<b>Precautions and Other Matters Regarding Internet Usage</b>				
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.	✓		
		IT team was responsible for checking patches, server update, software update and daily monitoring the anti-virus program.		
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.	✓		
		IT policy was in place.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>1.5 Complying with Data Access and Correction Requests</b>				
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. 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. 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.			✓
		No formal data access request was received.		
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.			✓
		No formal data access request was received.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.			✓
		No formal data access request was received.		
<b>Data Correction Requests of Employment-related Data</b>				
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. 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.			✓
		No formal data correction request was received.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
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.			✓
		No formal data correction request was received.		
<b>1.6 Employer's Liability for Wrongful Acts or Practices by its Employees or Agents</b>				
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.			✓
		No civil proceedings for act or practice relating to personal data were encountered before.		
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.			✓
		No civil proceedings for act or practice relating to personal data were encountered before.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.			✓
		No civil proceedings for act or practice relating to personal data were encountered before.		
<b>1.7 Other Matters</b>				
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.	✓		
		Confirmation of compliance was obtained.		
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.	✓		
		Privacy Policy Statement was made available on the Employer's website.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
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;	✓	
		1.7.3.2 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; 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.		
		<p>First letter and 3 digits of Hong Kong Identity Card (HKID) number of job applicants were collected on the job application form. The Employer explained that they were collected for verification purpose.</p> <p>It was noted that these partial HKID numbers of job applicants were not input into the HR system and the application forms of unsuccessful job applicants were not retained for later recruitment exercise.</p> <p>Inspection Team members conducted several mystery visits to branch restaurants of the Employer in the capacity of job applicants. During two mystery visits, the Team found that job applicants were not required to provide their HKID number in the job application form and present their HKID for verifying the information completed on the job application forms.</p>		



		Assessment Findings		
		Conformity	Non-conformity	N/A
1.7.4	An employer must check any copy of the Hong Kong Identity Card against the original card and mark it with the word "COPY" across the entire image of the Hong Kong Identity Card. Such a copy collected before 19 June 1998 needs not be so marked until it is first used after that date.		✓	
		In a random check carried out by the inspection team, a copy of Hong Kong Identity Card was found not stamping with the word "COPY".		
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.		✓	
		No Hong Kong Identity Card number was shown on staff cards.		

## 2 Recruitment

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>Practical Guidance on Recruitment-related Practices</b>				
<b>2.2 Collection of Personal Data from Job Applicants</b>				
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.		✓	
		Personal data collected from job applicants was used for recruitment purpose.		
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.		✓	
		Except the first letter and 3 digits of Hong Kong Identity Card number, other personal data collected from job applicants was adequate but not excessive.		
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:	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;	First letter and 3 digits of Hong Kong Identity Card number of job applicants were collected on the job application form. The Employer explained that they were collected for verification purpose.	
			It was noted that these partial Hong Kong Identity Card numbers of job applicants were not input into the HR system and the application forms of unsuccessful job applicants were not retained for later recruitment exercise.	
			Inspection Team members conducted several mystery visits to branch restaurants of the Employer in the capacity of job applicants. During two mystery visits, the Team found that job applicants were not required to provide their HKID number in the job application form and present their HKID for verifying the information completed on the job application forms.	

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
		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.		✓	
			No Hong Kong Identity Card copy was collected during recruitment process.	
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.	Only name, relationship and job position of job applicants' relative(s) working in the Employer were collected.	

		Assessment Findings		
		Conformity	Non-conformity	N/A
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 web page of the employer's website, it should ensure that the PICS notification requirement mentioned in paragraph 2.1.4 is complied with.	✓		
		Personal Information Collection Statement was provided in the job application form.		
<b>2.3 Advertising of Job Vacancies</b>				
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.			✓
		Same observations as mentioned in paragraphs 2.2.1 to 2.2.5 above.		
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 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.		
		Some advertisements on recruitment platforms invited job applicants to submit full resume to HR Department. The advertisements did not expressly identify the contact person from whom applicants might obtain a copy of the PICS.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.	✓		
		The name of the Employer was shown on the job advertisements.		
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.	✓		
		Job advertisements were used to solicit personal data for recruitment purpose.		
<b>2.4 Employment Agencies/Executive Search Company</b>				
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.			✓
		No employment agency was engaged for recruitment.		
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; and	✓	
		When an individual went to a branch seeking a job opportunity, he would be requested to complete a job application form only.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
		2.4.2.2 not use the data for a new purpose unless the prescribed consent from the individual is obtained.		
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.			✓
		No employment agency was engaged for recruitment.		
<b>2.5 Internal Records about Job Applicants</b>				
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:	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	Application forms of unsuccessful job applicants were destroyed annually and would not be used in a later recruitment exercise.	
		2.5.1.3 the applicant has not otherwise objected to the use of his data for such a purpose.		
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.			✓
		Application forms of unsuccessful job applicants were destroyed annually and would not be used in a later recruitment exercise.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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; 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.	Application forms of unsuccessful job applicants were destroyed annually and would not be used in a later recruitment exercise.	
<b>2.6 Receiving and Processing Applications for Employment</b>				
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.		✓	
			Hard copies of job application forms were stored in locked cabinets at Headquarters and branches. Personal data was input into HR system only when the job applicants were appointed.	
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.		✓	
			Only authorised HR staff and branch managers could access personal data of job applicants. Trainings were provided to both of them.	

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>2.7 Seeking Information for Selection Assessment</b>				
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.	✓		
		No other supplementary information was collected from job applicants, except sexual conviction record was checked for some helpers who carried out school catering services.		
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.	✓		
		Personal data of job applicants was collected by means of job application form with PICS.		
<b>2.8 Seeking Personal References of Job Applicants</b>				
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.	✓		
		A "Declaration of Consent & Authorization on Reference Check" was signed by job applicants giving their consents to the Employer for conducting reference check.		



		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>2.9 Acceptance by Candidates</b>				
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	No pre-employment medical check was carried out for job applicants.	
		2.9.1.3 the personal data is collected by means that are fair in the circumstances and are not excessive in relation to this purpose.		
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 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.	Additional information, such as bank account information and emergency contact, was collected only when the job applicant was 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.		✓	
		A copy of Hong Kong Identity Card was collected only when the job applicant was appointed.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
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.	✓		
		Appointee's consent was sought before publicly disclosing his personal data in relation to his appointment.		
<b>2.10 Unsuccessful Candidates</b>				
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.	
		✓		
		Application forms of unsuccessful job applicants were destroyed annually by the Headquarters.		
<b>2.11 Data Access and Correction Requests by Job Applicants</b>				
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.			✓
		No formal data access request was received.		

			<b>Assessment Findings</b>		
			<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.	No formal data access request was received.		
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.	No formal data access request was received.		

### 3 Current Employment

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>3.2 Personal Data in relation to the Terms and Conditions of Employment</b>				
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; or	✓	
		3.2.1.2 pursuant to a lawful requirement that regulates the affairs of the employer; and	Only contact information of spouse or emergency contact person was collected.	
		3.2.1.3 by means that are fair in the circumstances and the data is not excessive in relation to the purpose.		
<b>Compensation and Benefits</b>				
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.	Only contact information of spouse or emergency contact person was collected.	
<b>Integrity Checking/Declaration of Conflict of Interest</b>				
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	No integrity check was carried out for employees. Only a declaration of conflict of interest was collected from employees.	

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
		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.		
<b>Medical Checking and Health Data</b>				
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.		Medical check was carried out on employees to ensure they were fit for employment after retirement or for renewal of particular job, e.g. driver.
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.		Health report only showed whether the employee was fit for employment but not the details of the medical check results. HR Policy was in place specifying this requirement.
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.		✓	
				Documents containing personal data were locked in cabinets.

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
<b>3.3 Disciplinary Proceedings</b>				
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 accurate for the purpose upon which disciplinary decisions are taken; and	✓	
		3.3.2 held securely and accessible only by authorised personnel on a “need-to-know” basis.	A policy specifying the procedures of handling disciplinary cases was in place. Only authorised persons could make disciplinary decisions.	
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.	There was a disciplinary committee in the company. Only members of this committee could access the data related to the disciplinary cases and handle the cases in accordance with the established procedures.	
<b>3.4 Performance Appraisal</b>				
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;	A policy specifying the requirements of the performance appraisal system was in place.	
		3.4.1.3 determining the employee's continuance in employment; or		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
		3.4.1.4 determining the employee's job posting or training needs.		
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.		✓	
			A performance appraisal was examined. No excessive personal data was collected.	
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.	A policy specifying the requirements of the performance appraisal system was in place.	
<b>3.5 Staff Planning</b>				
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. 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.			✓
			No such circumstance occurred.	

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
<b>3.6 Promotion Planning</b>				
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 and by means that are fair in the circumstances.		✓	
				Staff movement form only listed out the promoted staff's basic information and the movement reason/ detail. Only the department head/ division head of promoted staff and payroll team members could access the data of staff movement form.
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.		Staff movement form only listed out the promoted staff's basic information and the movement reason/ detail. Only the department head/ division head of promoted staff and payroll team members could access the data of staff movement form.
<b>3.7 Providing Job References for Employees</b>				
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. Such consent means the express consent of the employee given voluntarily.		✓	
				When a third party requested a job reference of a former employee, a letter of consent signed by the former employee was required.



		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>3.8 Data Access and Correction Requests by Employees</b>				✓
3.8.1	<p>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. 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.</p>		No formal data access request was received.	
<b>Relevant Process Exemption</b>				✓
3.8.2	<p>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.</p>		No formal data access request was received.	

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
<b>Transitional Provision Exemption</b>				✓
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. If satisfied that the data is indeed inaccurate, the employer is required to comply with the request.		No formal data correction request was received.	
<b>3.9 Accuracy and Retention of Employment-related Data</b>				
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.	✓		
		HR Department issued notice annually reminding staff members to inform HR any changes of personal data by completing Change of Personal Data Form		
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.	✓		
		Policies and practices were uploaded to the Intranet and relayed to employees in briefing sessions.		
<b>3.10 Use of Employment-related Data of Existing Employees</b>				
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;	Personal data of employees were used for purposes that were directly related to the collection purposes that specified on the Personal Data Form.		
	3.10.1.2 the purpose is directly related to the purpose for which the data was collected;			

		<b>Assessment Findings</b>			
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>	
		3.10.1.3 such use or disclosure is required by law or by statutory authorities; or			
		3.10.1.4 there is an applicable exemption provided for under the Ordinance			
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:	3.10.2.1 the data thereby disclosed is accurate having regard to the purpose for which the data is disclosed; 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.	HR Department issued notice annually reminding staff members to inform HR any changes of personal data by completing Change of Personal Data Form		
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.		✓		
			Files containing personal data were password-protected when they were sent via email.		

		<b>Assessment Findings</b>		
		<b>Conformity</b>	<b>Non-conformity</b>	<b>N/A</b>
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.	No such circumstance occurred.	
<b>3.11 Disclosure or Transfer of Employment-related Data</b>				
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.		✓	
			Personal data of employees was transferred to MPF trustee, clinic for medical checkup, Inland Revenue Department and Group insurance company for employment related purposes.	
<b>Outsourcing of Human Resource Data Processing</b>				
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.			✓
			No such circumstance occurred.	

		Assessment Findings		
		Conformity	Non-conformity	N/A
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.	No such circumstance occurred.	
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	No such circumstance occurred.	
		3.11.4.3 limited to employment-related data of the employee concerned.		
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.		✓	
		Personal data of an employee who was transferred to China office was used for the preparation of working visa and China taxation issue only.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
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.	✓		
		Staff movement form only listed out the transferred staff's basic information and the movement reason/ detail.		
Mergers, Acquisitions, and Associated Due Diligence Exercises				
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.			✓
		No such circumstance occurred.		
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.			✓
		No such circumstance occurred.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
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.			✓
		No such circumstance occurred.		
<b>3.12 Matters Concerning the Engagement of Subcontract Staff</b>				
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.			✓
		No such circumstance occurred.		
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; or		✓
		3.12.2.2 where there is a reasonable likelihood that such staff may be re-engaged on subsequent work.	No such circumstance occurred.	
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 disclosure or transfer of such data.			✓
		No such circumstance occurred.		

#### 4 Former Employees' Matters

			Assessment Findings		
			Conformity	Non-conformity	N/A
<b>Practical Guidance on Former Employees' Matters</b>					
<b>4.2 Continued Retention of Personal Data of Former Employees</b>					
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	Personal files of former employees were not retained for more than seven years for Headquarters staff and not more than two years for branch staff.		
		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.		✓		
			Personal files of former employees were not retained for more than seven years for Headquarters staff and not more than two years for branch staff.		
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; or	✓		
		4.2.3.2 the former employee has given prescribed consent for the data to be retained beyond seven years.	Personal files of former employees were not retained for more than seven years for Headquarters staff and not more than two years for branch staff.		



		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>4.3 Accuracy of Former Employees' Personal Data</b>				
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.	✓		
		There was established procedure in updating former employees' personal 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.	✓		
		In case any document was failed to send to a former employee, HR Department would contact and ask the former employee to update his personal data in the HR records.		
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:	✓		
		There was established procedure in updating former employees' personal data.		
		4.3.3.1 the data transferred is accurate having regard to the purpose for which the data is used; 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.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>4.4 Security of Former Employees' Personal Data</b>				
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.	✓		
		Personal files of former employees were stored in an off-site premise. Only authorised staff members could enter into the premise.		
<b>4.5 Providing Job References for Former Employees</b>				
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.	✓		
		When a third party requested a job reference of a former employee, a letter of consent signed by the former employee was required.		
<b>4.6 Public Announcements about Former Employees</b>				
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.			✓
		No such circumstance occurred.		

		Assessment Findings		
		Conformity	Non-conformity	N/A
<b>4.7 Erasure of Former Employees' Personal Data</b>				
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.	✓		
		During site inspection, it was noted that the earliest record of personal files retained for former employees were in 2016 (i.e. the retention period was not more than three years).		
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.	✓		
		Same observation as mentioned in paragraph 4.7.1 above.		
<b>4.8 Retirement</b>				
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.			✓
		There was no retirement plan of employees available.		
<b>4.9 Death of an Employee</b>				
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.			✓
		No such circumstance occurred.		