Published under Section 48(1) of the
Personal Data (Privacy) Ordinance (Cap. 486)

Inspection Report :
Personal Data System of the Labour Department in Providing Employment Services to Job Seekers

Report Number: R14-3849

Date issued: 20 November 2014

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

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data System of the Labour Department in Providing Employment Services to Job Seekers

This report of an inspection carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 36 of the Personal Data (Privacy) Ordinance, Cap. 486 (the "**Ordinance**") in relation to the personal data system used by the Labour Department is published pursuant to section 48 of the Ordinance.

Section 36 of the Ordinance provides:-

"*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.*"

The relevant parts in **section 48** of the Ordinance provide:-

"*(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."

Allan CHIANG
Privacy Commissioner for Personal Data

Table of Contents

Executive Summary

Introduction

1. The Labour Department provides free employment services through a network of 12 Job Centres, two industry-based Recruitment Centres, a Telephone Employment Service Centre, an Interactive Employment Service website and a mobile phone application. The average number of registered job seekers and job referrals made each year exceeds 96,000 and 172,000 respectively for the three calendar years from 2011 to 2013. The Labour Department collects, holds, processes and uses a wide range of personal data of job seekers including name, Hong Kong Identity Card ("**HKID Card**") number, contact details, education background, work experience and skills, etc.

2. In view of the vast number of data subjects, the extent of personal data involved, the disclosure of personal data to employers, an online system allowing uploading of resumes, a mobile phone application with job vacancy searching function, as well as the continual role of the Labour Department in the provision of employment services, the Privacy Commissioner for Personal Data (the "**Commissioner**") considers that it is in the public interest to carry out an inspection of the personal data system used by the Labour Department (the "**Inspection**") pursuant to section 36 of the Personal Data (Privacy) Ordinance (the "**Ordinance**").

3. The Inspection focuses efforts on the personal data system that handles employment services, which allow registered job seekers to subscribe to job-alert functions, build and upload resumes, search for job vacancies online or through mobile phone application, arrange job interviews, seek employment advice, be notified of suitable recruitment activities, etc. The collection of personal data from members of the public for provision of public services by the Labour Department is typical of many other government departments and public organisations. This means that the Commissioner's recommendations for the Labour Department's personal data system for handling employment

services should be useful reference to this class of data users for the purpose of ensuring compliance with the requirements under the Ordinance.

The Inspection

4. The personal data system of the Labour Department in relation to the provision of employment services was inspected. Specifically, the collection, retention, use, security of personal data and the provision of policies and practices were reviewed against the requirements under Data Protection Principles ("**DPPs**") 1 to 5 in Schedule 1 to the Ordinance and Part VIA of the Ordinance regarding direct marketing activities.

5. The Inspection comprised review of the Labour Department's relevant policies and procedures, enquiries with its staff, site inspection, attending demonstrations by the Labour Department of data handling procedure and interviews with the relevant staff of the Labour Department in the period from 11 March 2014 to 29 July 2014.

Findings and Recommendations

6. The Commissioner found no serious or major deficiencies during the Inspection and is reasonably satisfied with the data protection measures in the personal data system of the Labour Department. Nevertheless, the Commissioner has identified 14 issues which need to be addressed and his recommendations on follow-up and/or improvement actions are summarised below:-

Data collection

(1) The Labour Department collects from the employers, after job interviews have been conducted, the interview results, position recruited, date of employment and salary offered. The Commissioner observes that it is not made clear to the job seekers

as to what types of their personal data the Labour Department may collect from the employers, since collection of such data can only be inferred from reading a reply slip which is primarily intended for completion by the employer. The Commissioner recommends the Labour Department to state clearly in the Personal Information Collection Statement provided to job seekers both the types of personal data to be collected from the employers and the purposes of collecting such personal data.

Data accuracy

(2) Before using the employment services of the Labour Department, job seekers have to complete registration forms provided by the Labour Department ("**Registration Form**"). The staff will input the personal data of job seekers into a computer system called Labour Department Employment Service System (the "**Internal Computer System**"). Job seekers may subsequently request to amend their personal data by completing the amendment forms. A practice of random checking of the accuracy of data input has been introduced since March 2014 to check 5% of the Registration Forms (but not the amendment forms) received in the previous month. However, no guidelines have been drawn up as regards how the results of the random check should be followed up to enhance overall data accuracy. The Commissioner recommends that the Job Centres' managers should monitor and improve on the error rate of data input proactively and systematically. He also recommends extending the accuracy check to cover any subsequent data amendments.

Data retention

(3) Registration Forms will be destroyed two years after the completion of data input according to the Labour Department's

internal guideline, but Registration Forms dating back in 2008 were found during the site inspection. The Commissioner recommends introducing management control to ensure Registration Forms and other forms containing personal data are destroyed according to schedule.

(4) The Internal Guideline on Destruction of Records was last revised in 2003 and since then there has been no formal review of the retention policies. The Commissioner observes that the retention period for data amendment forms held by Job Centres under the Employment Services Division, which is not specified in the guideline, is two years. However, similar forms held by the Telephone Employment Services Centre under another Division are kept for three months only. The Commissioner therefore recommends reviewing file retention policies on a regular basis and across different divisions in the Labour Department to ensure comprehensive coverage and consistency in practice.

(5) The Labour Department engages a contractor for sending job fair promotional messages by SMS. Contractual obligations are imposed on the contractor to delete the file containing phone numbers of job seekers for sending SMS within 12 months after receiving such file. The Commissioner recommends the Labour Department to review the appropriateness of this retention policy and shorten the retention period where appropriate.

Data use

(6) The Labour Department may ask a job seeker to send his resume to the employer directly. The Commissioner was informed that the Labour Department would disclose the employer's identity and contact means to the job seeker during the referral process and no irregularity was detected during the Inspection. However, there is no written guideline stating clearly the requirement to

disclose employer's identity to the job seeker before provision of his resume. The job seeker may not know the employer's identity when he sends his resume. To ensure fair collection of personal data by the employer, the Commissioner recommends devising clear guidelines to disclose the employer's identity for the situation where a job seeker is requested by an employer to provide his resume. In case the employer does not wish to disclose his identity, the Labour Department should provide the employer's contact phone number to the job seeker so that the job seeker can enquire directly with the employer before providing any personal data to the employer.

Data security

(7) The service booths where the placement officers meet the job seekers for provision of employment services are located inside the office area. In the circumstances, the Commissioner is concerned about the risk of trespass by unauthorised persons into restricted areas where personal data is stored or processed. As a stop-gap remedial measure to address this unsatisfactory office layout, he recommends introducing means to prevent trespass by unauthorised persons inside the office area such as by the installation of electronic locks at the entrance to internal office areas, escorting job seekers when they enter internal office areas to meet with placement officers, and the posting of prominent signs to clearly demarcate the service booth area and the internal office area.

(8) A job seeker's Interactive Employment Service Website ("**iES**") account will be locked in the event of repeated incorrect login. The job seeker is required to send an email to the Labour Department providing his personal data including English name, date of birth, contact phone number, the first four digits of his HKID Card number and his account login name to unlock the

account (though this requirement was reduced to supply of account login name and registered contact phone number only from June 2014 after the inspection team alerted the Labour Department of the risk of unsecured transmission of email communication). The Commissioner recommends enhancing the system of iES Website to allow job seekers to apply for account re-activation via the website itself to avoid transmitting personal data via the unsecured means of sending email without encryption.

(9) When a new staff comes on board, the same default password, which is known by IT staff members, will be assigned to him for creation of a new account in the Internal Computer System. After first login, an e-mail reminding him to change the password will be sent. However, the system does not force the user to change the default password after the first login. The Commissioner is concerned about the potential risk that a third party could impersonate another user to access the Internal Computer System, and recommends mandating new staff, by technical means, to change the default password of the Internal Computer System on first login.

(10) There is no departmental-wide guideline, procedure or control on the disposal of equipment including computers and storage devices to ensure that personal data is erased properly before disposal. The Commissioner recommends formulating guidelines or procedures on the disposal of equipment that may store personal data to ensure all such data is erased before disposal.

(11) The Labour Department has devised a high-level department-specific IT security policy, but there is no department-specific IT security guideline. Labour Department advised that reference could be made to the IT security guidelines issued by the Office

of the Government Chief Information Officer available on the government's intranet. The Commissioner recommends the Labour Department to make due assessment on whether devising its own guideline on IT security is required, and clearly inform the staff of which IT security guidelines to follow and where to locate such guidelines. Besides, detailed guidance on data breach handling is also lacking. The Commissioner therefore recommends devising guideline on data breach handling to include clear procedures for staff to follow.

(12) Files containing the personal data of job seekers will be saved in shared computer drives temporarily, e.g. when preparing the contact information list of selected job seekers for promotion of job fairs. A designated staff is assigned in each office to conduct regular checking on shared drives to ensure files containing personal data are deleted after use. However, no written procedure can be found in this regard. To ensure files containing the personal data of job seekers will not be kept in the shared drives for a period longer than is necessary, the Commissioner recommends devising procedures and monitoring mechanism for erasure of records in shared drives for staff to follow.

CCTV

(13) The Labour Department has installed for security purpose closed-circuit television ("**CCTV**") cameras in the public areas of the Job Centres, but there are insufficient measures to prevent unauthorised access to the CCTV systems and there are no specific written instructions or guideline on the use of CCTV issued by the department. The Commissioner recommends devising and implementing CCTV policies and/or procedures specifying who are authorised to access the captured CCTV images, measures to safeguard the security of the CCTV systems and the retention period of the captured CCTV images, and

including in the CCTV notices the contact phone number of Labour Department staff for public enquiry.

Training

(14) All personnel involved in the handling of personal data should be made aware of the importance of respecting the data privacy rights of individuals and the legal requirements of the Ordinance. However, there is no training plan on personal data protection. The Commissioner recommends devising a training plan to ensure staff members who handle personal data are provided with regular training on personal data protection.

Conclusion

7. Notwithstanding the issues identified in paragraph 6, the personal data system inspected is generally in compliance with the requirements of the Ordinance. The Commissioner is pleased to see the following data protection measures in place:

(a) allowing job seekers to choose if they wish to receive information of the relevant job vacancies, recruitment activities and employment services, and stating the ways (by contacting the manager of the Job Centres or sending an email to the Labour Department) by which job seekers may inform the Labour Department if they decide not to receive such information;

(b) allowing job seekers to disclose selected information such as education background, skills, language proficiency, work experience and job preference on an anonymous basis for employers to conduct online potential candidate selection;

(c) assigning different staff privilege rights according to rank for accessing job seekers' personal data in its internal computer system; and

(d) implementing appropriate data privacy measures for the use of public sharing computers at Job Centres to protect job seekers' personal data from being viewed by others such as the use of privacy screen filters and erasure of all settings and data used by the previous user.

8. Of the 14 recommendations outlined above, the Commissioner considers that the following five areas call for the Labour Department's prompt attention:

(a) to notify the job seeker the types of personal data that will be collected from the employer and the purposes of collecting such data (paragraph 6(1) above);

(b) to introduce management control to ensure Registration Forms and other forms containing personal data are destroyed according to schedule (paragraph 6(3) above);

(c) to devise clear guidelines to disclose the employer's identity to the job seeker if a job seeker is requested to send his resume to the employer directly (paragraph 6(6) above);

(d) to introduce means to prevent trespass by unauthorised persons in the office area (paragraph 6(7) above); and

(e) to devise and implement CCTV policies and/or procedures (paragraph 6(13) above).

9. The Commissioner hopes that this report will be of value to the Labour Department. Other government departments and public organisations which

collect personal data from members of the public for providing public service in a similar way are encouraged to take reference from this report.

10. More generally, recalling the pledge made by government bureaux and departments to implement Privacy Management Programmes ("**PMP**"), the Commissioner hopes that bold and decisive steps will be taken by them in this regard. PMP will build a robust privacy infrastructure supported by an effective ongoing review and monitoring process to facilitate compliance with the requirements under the Ordinance. It will also demonstrate the government's commitment to good corporate governance and building trust with the citizens that it serves. More details about PMP are found in "Privacy Management Programme – A Best Practice Guide" (www.pcpd.org.hk/pmp/).

Chapter One

Introduction

1.1 The Labour Department aims to provide comprehensive employment services, foster harmonious labour relations, promote and safeguard employees' rights and benefits as well as occupational safety and health. With regard to employment services, the Labour Department provides free and comprehensive services through its network of 12 Job Centres[1], two industry-based Recruitment Centres[2], the Telephone Employment Service Centre[3], the Interactive Employment Service website ("**iES Website**[4]") and mobile phone application ("**iES Mobile App**[5]").

1.2 On average, the number of registered job seekers and job referrals made per year exceeds 96,000 and 172,000 respectively for the three calendar years from 2011 to 2013. The Labour Department collects, holds, processes and uses a wide range of personal data of job seekers. The kinds of personal data held by the Labour Department include the name, Hong Kong Identity Card ("**HKID Card**") number, date of birth, contact information, education background, work experience, skills, etc. of job seekers.

1.3 Given the vast number of data subjects, the extent of personal data involved, the disclosure of personal data to employers, an online system

[1] Job Centres provide employment services to job seekers such as offering job vacancy information, arranging job referrals, organising district-based job fairs, administering employment programmes and providing employment advisory services, etc.

[2] Recruitment Centres invite employers from retail and catering industries to stage recruitment activities in the centres to interview job seekers on the spot.

[3] Telephone Employment Service Centre provides employment hotline services to job seekers such as arranging job referral via phone and answering enquiries on employment services etc.

[4] iES Website provides online employment services to job seekers such as searching for suitable job vacancies from the Labour Department's database and allowing job seekers to build or upload resumes for online job application etc.

[5] iES Mobile App offers job searching function to job seekers to find suitable job vacancies from the Labour Department's database via smartphone operating in either iOS or Android systems.

allowing uploading of resumes, a mobile phone application with job vacancy searching function, as well as the continual role of the Labour Department in the provision of employment services, the Privacy Commissioner for Personal Data (the "**Commissioner**") considers that it is in the public interest to carry out an inspection of the personal data system used by the Labour Department (the "**Inspection**") pursuant to section 36 of the Personal Data (Privacy) Ordinance (the "**Ordinance**").

1.4 Job seekers' personal data are handled by the following divisions and units for the provision of employment services:

(1) Employment Services Division, including;
    (a) Divisional Headquarters[6];
    (b) 12 Job Centres;
    (c) Two Industry-based Recruitment Centres;
    (d) Information Systems Office[7];
(2) Employment Information and Promotion Division, including:
    (a) Telephone Employment Service Centre;
    (b) Employment Information and Promotion Programme Office[8]; and
(3) Information Technology Management Division[9]

1.5 The Inspection focuses on the personal data system of the Labour Department's employment services which allow registered job seekers to

[6] Divisional Headquarters is responsible for overseeing the operation of the Labour Department's employment services.

[7] Information Systems Office is responsible for the administration and management of the computer systems which support Job Centres, Recruitment Centres and Telephone Employment Service Centre in providing employment services to job seekers.

[8] Employment Information and Promotion Programme Office is responsible for launching promotion programmes to disseminate employment information and promote the employment services of Labour Department, such as large-scale job fairs.

[9] Information Technology Management Division is responsible for providing technical support and maintenance services to the computer systems which support Job Centres, Recruitment Centres and Telephone Employment Service Centre in providing employment services to job seekers.

subscribe to job-alert functions, build and upload resumes, search for job vacancies online or through mobile phone application, arrange job interviews, seek employment advice, and be notified of suitable recruitment activities, etc. During job referral process, the personal data of job seekers is disclosed to employers, making it appropriate for us to take a closer look. The collection of personal data from members of the public for provision of public services by the Labour Department is typical of many other government departments and public organisations. This means that the Commissioner's recommendations for Labour Department's personal data system for handling employment services should be useful reference to this class of data users for the purpose of ensuring compliance with the requirements under the Ordinance.

1.6 The vast volume and broad range of personal data handled by the various Job Centres, Recruitment Centres, Telephone Employment Service Centre and iES Website in the course of providing employment services give rise to a multi-faceted and complex data flow involving processes such as collection, use, transfer, disclosure, retention, security and destruction of such data.

1.7 The Employment Information and Promotion Programme Office (paragraph 1.4(2)(b)) was not our focus as its main function is to launch promotion programmes such as large-scale job fairs, in which it does not normally handle personal data of job seekers, and it shares the same data flow and computer system as other Job Centres and the Telephone Employment Service Centre. However, we have looked at its use of job seekers' personal data to promote the employment services of Labour Department, such as sending job fairs information to job seekers who have registered for receiving such information.

1.8 It is hoped that the recommendations in this report would be of assistance to the Labour Department. Other government departments and public organisations that collect personal data from members of the public in a similar way are encouraged to make reference to this report.

Chapter Two

The Inspection

Commencement of the Inspection

2.1 In accordance with section 41 of the Ordinance, on 11 March 2014 the Commissioner informed the Labour Department in writing of his intention to carry out the Inspection with a view to making recommendations to promote compliance with the Ordinance.

The Inspection Team

2.2 An inspection team (the "**Team**") consisting of six officers[10] from the Office of the Privacy Commissioner for Personal Data ("**PCPD**") was formed to carry out the Inspection.

Pre-Inspection Meeting

2.3 The Team held a pre-inspection meeting with representatives of the Labour Department on 30 April 2014 to explain the nature, purpose, scope and methodology of the Inspection. The Team also answered the Labour Department's queries and addressed its concerns, and gained a better understanding of the operation and work flow of the personal data system of the Labour Department.

Scope of the Inspection

2.4 The personal data system was examined against the requirements under Data Protection Principles ("**DPPs**") 1 to 5 in Schedule 1 to the

[10] The Team consisted of one Chief Personal Data Officer, the Information Technology Advisor, one Senior Personal Data Officer, one Personal Data Officer and two Assistant Personal Data Officers.

Ordinance in respect of the collection, accuracy, retention, use, and security of personal data and the provision of policies and practices in relation to personal data, and Part VIA of the Ordinance regarding the use of personal data in direct marketing activities. The five DPPs and Part VIA of the Ordinance are reproduced in Annex 1. DPP6, concerning access to personal data, is not covered in this Inspection.

Methodology

2.5 The Team performed the following procedures during the Inspection under section 36 of the Ordinance:-

Policy review

2.6 A detailed and comprehensive policy on how to properly handle job seekers' personal data is essential for ensuring good and uniform practice. In the Inspection, the Team examined the relevant policies, procedural manuals and training material which the Labour Department follows in the handling of personal data.

Enquiries

2.7 The Team made written and verbal enquiries with the Labour Department. The information obtained through enquiries assisted the Team in understanding the operation of the personal data system, reconciling the documentary evidence obtained with our observations at site inspection and identifying any cause for concern. The Labour Department was also able to supplement the evidence in question to avoid misunderstanding or misinterpretation.

Site inspections

2.8 Between 4 June 2014 and 13 June 2014, the Team inspected the following premises of the Labour Department:

(1) Three Job Centres located in Shatin, Kowloon West and Hong Kong East respectively and two Recruitment Centres (Catering and Retail Industries) in Wan Chai;
(2) Telephone Employment Service Centre in Quarry Bay;
(3) Information Technology Management Division in North Point;
(4) Divisional Headquarters in Central; and
(5) Server room in Tsuen Wan.

2.9 The Team was able to inspect in person the equipment used for collecting, processing and storing the personal data and physical security measures, sample check file records, review the general data flow throughout the job referral process and identify any issues that might not have been apparent from documents or representations.

Walkthrough demonstration

2.10 Representatives of the Labour Department walked through with the Team the data flow of the collection, use and retention of job seeker's personal data. The Inspection focused on observation of the following :

(1) As regards the Job Centres, Recruitment Centres and Telephone Employment Service Centre, the registration procedures, retention and destruction policies, use and disclosure of personal data, physical and digital security, transparency and call handling protocols;
(2) As regards the Information Technology Management Division and Information Systems Office (for the purpose of this report, the term 'IT Unit' will be used henceforth to refer to them

collectively) , the technical operations of the Labour Department Employment Service System [11] (the "**Internal Computer System**"), including network diagrams, the data flow and back up, roles and responsibility of relevant staff, IT security policy and procedures, IT training and the management of the server and equipment rooms; and

(3) As regards the Divisional Headquarters, the storage and security aspects, specifically in relation to physical security, password control, access right and records retention.

Interviews

2.11 The Team interviewed 32 staff, from management to operational levels, of different teams under the Employment Services Division, the Employment Information and Promotion Programme Office and the Information Technology Management Division of the Labour Department to understand their handling of personal data, their familiarity with the policies, guidelines and procedures relating to their work, and the training they provided and received.

[11] Labour Department Employment Service System is the internal computer system used by Job Centres, Recruitment Centres and the Telephone Employment Service Centre in providing employment services to job seekers.

Chapter Three

Personal Data System and Data Flow

The Personal Data System

3.1 In the provision of employment services (including job referral and counselling services) to job seekers, the Labour Department handles personal data of job seekers through different channels, namely, Job Centres, Recruitment Centres, Telephone Employment Service Centre and iES Website. The relevant personal data system includes the Internal Computer System which is used for storing and processing personal data, and the internal procedural manuals and orders of the relevant centres and units in relation to the collection, retention and processing of personal data.

3.2 The table below lists the major kinds of personal data of job seekers involved (Please refer to Annex 2 for the full list of personal data of job seekers collected):-

Kinds of personal data	**Examples**
Name and personal identifier	• Name in Chinese and English • HKID Card number
Personal particulars	• Date of birth • HKSAR resident status • Number of years of staying in Hong Kong • Ethnic origin • Present employment status
Contact information	• Correspondence address • Daytime contact telephone numbers • Email address • Fax number

Education and skills	• Highest education level attained • Public examination results • Skills • Language
Work Experience	• Name of employer • Position • Average monthly salary of most recent job • Employment period
Job Preference	• Preferred job nature • Preferred work hours • Preferred work district

The Data Flow

An overview of the data flow

3.3 For the purpose of the Inspection, the data flow of the personal data system of employment services was broadly divided into the following five stages:

A. Collection;
B. Use[12];
C. Amendment / Withdrawal;
D. Retention; and
E. Destruction.

3.4 A brief introduction of the data flow is set out in the following paragraphs.

[12] Under section 2(1) of the Ordinance, the term "Use" includes the disclosure or transfer of the personal data.

A. Collection of personal data of job seekers

3.5 A job seeker who would like to use the employment services of the Labour Department, including applying for vacancies in which employers' contact information is not disclosed, on-the-spot interview with employers in a job fair organised by Job Centres or Recruitment Centres, or vacancies in iES Website, must register with the Labour Department. During the registration, job seeker's personal data is collected, input and stored in the Internal Computer System.

3.6 If a job seeker wants to apply for vacancies for which employers' contact information is disclosed, he[13] can directly contact the employer and send his resume by using facilities provided in Job Centres or Recruitment Centres, without using employment services of the Labour Department. In this case, no registration with the Labour Department is required and the Labour Department does not collect the job seeker's personal data.

3.7 A job seeker may download the iES Mobile App, which provides job searching functions, onto his smartphone. Provision of personal data is not required by the Labour Department for the download and use of the application. The Labour Department confirmed that no personal data of job seekers is collected through the application.

A1. Job Centres

3.8 When a job seeker arrives at a Job Centre for employment services, a counter staff will request his HKID Card to check whether he has registered with the Labour Department before. The staff will input the HKID Card number into the Internal Computer System to check whether any records can be retrieved. The HKID Card will then be returned to the job seeker immediately. If there is a record showing that the job seeker has already registered, he can use employment services by meeting a placement officer; otherwise, the staff

[13] Words and expressions importing the masculine gender include the feminine gender in this report.

will give a registration form for the Labour Department's employment services ("**Registration Form**"), containing a Personal Information Collection Statement ("**PICS**"), to the job seeker for his completion. The staff will then arrange a time slot for the job seeker to meet a placement officer.

Reception counters of various Labour Department Job Centres.

3.9 The job seeker can fill in the Registration Form in the lobby area of a Job Centre. There are seven mandatory fields, as indicated on the Registration Form, as follows:

(1) HKID Card number;
(2) Name;
(3) Date of birth;
(4) Correspondence address;
(5) Daytime contact telephone numbers;
(6) Whether the job seeker is a permanent resident in Hong Kong; and
(7) Highest education level.

3.10 There are questions seeking consent from the job seeker for using his personal data for sending promotional information about the Labour Department's employment services in the Registration Form as follows:

(1) Whether the job seeker consents to receive information on job vacancies, recruitment activities and employment services; and
(2) Whether the job seeker consents to receive Short Message Service ("**SMS**") relating to information of recruitment activities.

3.11 There is a question seeking consent from the job seeker for publishing his selected information anonymously through the Internet or other publication means to allow employers to view for choosing suitable candidates, such as education background, skills, language proficiency, work experience and job preference. Identifiable personal particulars such as name, HKID Card number, telephone number, correspondence address and email address will not be published. Employers can then approach the Labour Department to arrange suitable candidates for interview.

3.12 The job seeker will then be called to enter the office area to meet the assigned placement officer and submit the completed Registration Form. The placement officer will ask the job seeker to present his HKID Card for checking his identity again.

Interviewing booths inside the office area of Job Centres.

3.13 The placement officer will create a record for the job seeker in the Internal Computer System with the input of five mandatory fields including

Chinese and English names, HKID Card number, telephone number and correspondence address, which are the minimum fields required for creating a new registrant's computer record.

3.14 The placement officer will confirm with the job seeker whether he consents to receive promotional information from the Labour Department and to publish his selected information for job referral purpose, if he has not answered the questions on the Registration Form mentioned in paragraphs 3.10 - 3.11.

3.15 After creating the job seeker's computer record, the placement officer can provide employment services (explained in paragraphs 3.30 - 3.34) to the job seeker. Before the job seeker leaves the Job Centre, the placement officer will give him a "Notice for Job Seeker" which includes the details of employment services and the PICS.

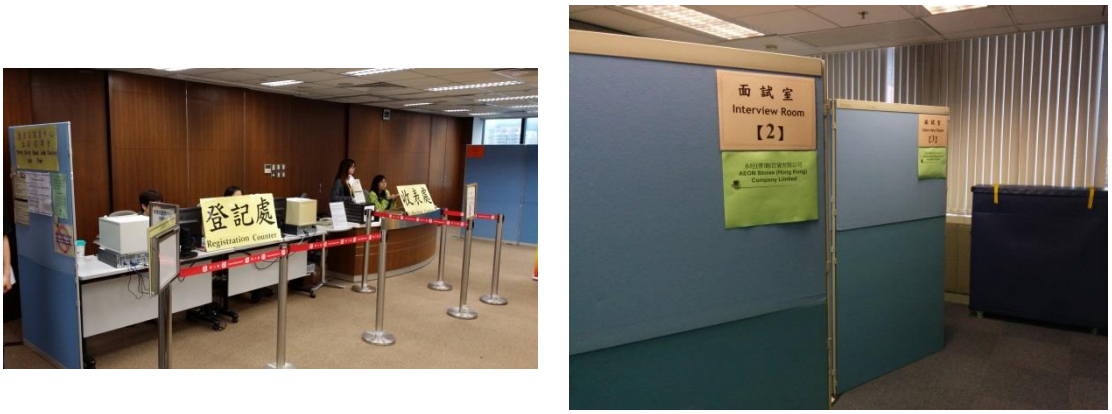
3.16 Other personal data in addition to the five minimum fields will be input into the Internal Computer System at the end of the day.

3.17 After completion of data input, the Registration Forms will be passed to the clerk-in-charge for recording the number of new registrants and storing temporarily in his locked cabinet. At the beginning of each month, five percent of Registration Forms received last month will be randomly retrieved and check will be performed to verify the accuracy of the data input of the Registration Forms collected in the previous month.

Locked cabinets containing miscellaneous forms.

A2. Job fairs organised by Job Centres or Recruitment Centres

3.18 A job seeker can participate in on-the-spot interview with the employer during a job fair organised by a Job Centre or Recruitment Centre. For some vacancies which have interview quota, a job seeker needs to contact the Job Centre or Recruitment Centre via telephone beforehand and provide his name and telephone number for making the appointment. When a job seeker arrives at Job Centre or Recruitment Centre to attend the interview, he needs to approach the counter to inform the Labour Department staff of the vacancy he applies for and present his HKID Card. The staff will then check whether the job seeker has registered before with the Labour Department by inputting his HKID Card number into the Internal Computer System. If the job seeker has not registered with the Labour Department yet, the staff will give him a Registration Form, together with an application form of the concerned vacancy. The staff will record the job seeker's name and the post to be applied for in a log sheet.



On-the-spot interviews at Job Centres: counter (Left) and interview booths (Right).

3.19 The job seeker needs to return the completed forms to the counter. The staff will ask him to present the HKID Card for double checking of his identity and check whether the Registration Form is correctly completed. The HKID Card will be returned to the job seeker immediately after checking. A "Notice for Job Seeker" which includes the details of employment services and the PICS will be given to the job seeker.

3.20 The staff will confirm with the job seeker whether he consents to receive promotional information from the Labour Department and to publish his selected information for job referral purpose if he has not answered the questions on the Registration Form mentioned in paragraphs 3.10 - 3.11.

3.21 The staff will then arrange a time slot for the interview and mark a serial number separately on the Registration Form and the vacancy application form to facilitate retrieval and follow up. The Registration Form will be kept in a restricted folder by the staff himself, while the application form will be passed to the corresponding employer in a restricted folder for interview purpose and kept by the employer after the interview.

3.22 All the Registration Forms collected in the job fair will be passed to the assigned staff for data input into the Internal Computer System by batches during the day in order to complete the registration. After completing the data input, the Registration Forms will be stored in accordance with the procedure mentioned in paragraph 3.17.

A3. iES Website

3.23 Apart from registering with the Labour Department's employment services in person at Job Centre or Recruitment Centre, a job seeker can register via iES Website. The registration interface starts by showing the statement of purposes stating the purpose of data collection, classes of transferees of data and rights of access to personal data. The job seeker can click the "Next" button to proceed to registration after reading the statement.

3.24 The job seeker will then be asked to enter certain personal data. There are 22 fields[14] marked as mandatory on the screen (as shown in Annex 3).

3.25 There are questions seeking consent from the job seeker for using his personal data for sending promotional information about the Labour

[14] The number of mandatory fields has been reduced to 14 since 7 August 2014.

Department's employment services and letting employers view his information as follows:

(1) Whether to receive information on job vacancies, recruitment activities and employment services from Labour Department;
(2) Whether to let employers view his information including education background, skills, language proficiency, work experience and job preference when they select candidates; and
(3) Whether to receive SMS for recruitment activities.

3.26 After the job seeker has completed all the entries, his profile will be created in the iES Website system and it will be copied to the Internal Computer system automatically.

3.27 A job seeker can create on and upload to iES Website his resume to apply for a vacancy which accepts online application through the website. He can either use the web interface to build resume from his registered data, or upload his resume in PDF format onto the website system. The resume will be stored in the website system for future use.

A4. Collection from the employers

3.28 The Labour Department will check placement results of the referred job seekers by collecting from employers information including interview result, position recruited, date of employment and salary. An employer is requested to provide such information by returning a reply slip attached to an introduction letter issued by Job Centres or Telephone Employment Service Centre (the "**Introduction Letter**") after the employer has interviewed the referred job seeker; or by returning an interview result list after the employer has interviewed the job seekers at a job fair.

B. Use of personal data collected from job seekers

3.29 The Labour Department will use the personal data of job seekers for job referral purposes, including job interview arrangement with employers; job

matching to identify suitable job vacancies for job seekers; employment advisory services to enhance job seekers' interview skills and confidence; and sending promotional information of the job fairs organised by the Labour Department.

B1. Job Centres

3.30 If a job seeker is interested in job vacancies which do not disclose the employers' contact details[15], he can request a placement officer to contact the concerned employers to arrange for job interviews. A maximum of three vacancies can be referred in each request. He can provide the job order numbers of the vacancies posted at the Job Centre or iES Website to the officer who will then retrieve the job seeker's record and the vacancies details from the Internal Computer System to check whether the job seeker meets the job requirements of the vacancies. If the job seeker appears to be a suitable candidate, the officer will contact the concerned employers to arrange interviews. The officer will not disclose the job seeker's name and contact information to the employer at this moment. As to other personal data such as education background or work experience, it will only be disclosed after the job seeker has given consent.

3.31 If an interview is successfully arranged, the officer will generate an Introduction Letter from the Internal Computer System for the job seeker to bring to the interview. The letter bears the job seeker's name in Chinese and English and interview details such as the name, address and contact person of the employer, the post applied, interview time and location. The Labour Department will not retain a copy of the letter but a job referral record will be kept in the Internal Computer System.

3.32 If the employer requests the job seeker to send his resume first, the officer will provide the employer's fax number or email address to the job

[15] A separate unit of the Labour Department called Job Vacancy Processing Centre has checked the identity and contact information of employers when they place job vacancy orders.

seeker for sending the resume. He can use the facilities such as fax machines and computers provided at the Job Centre.

Self-service fax machines available to job seekers at Job Centres.

3.33 A job seeker can request the placement officer to provide job matching service. The officer will check his personal data such as education background, work experience, job preference and expected salary with the vacancies available in the Internal Computer System to introduce suitable vacancies to him. If he is interested in the vacancies, the officer will go through the same procedure mentioned in paragraphs 3.30 - 3.32 to follow up.

3.34 A job seeker can request the placement officer to offer employment advisory services. The officer may check the job seeker's background from the Internal Computer system to facilitate appropriate advice to the job seeker.

B2. Job fairs organised by Job Centres or Recruitment Centres

3.35 When a job seeker applies for on-the-spot interview with the employers in a job fair arranged by Job Centres or Recruitment Centres, the Labour Department staff will retrieve his computer record to check the validity of his registration and provide a job application form of the vacancy concerned after checking. The job seeker should then return the completed job application form to the staff for arranging interview. The staff will pass the completed job application form to the employer before interview begins. No copy of the same will be kept by the Labour Department.

3.36 For the promotion of job fairs, Job Centres or Recruitment Centres may send promotional materials by mail, or arrange a contractor to send promotional messages by SMS to those job seekers who have consented to receive such information.

3.37 The staff who is authorised to generate job seekers' information from the Internal Computer System will prepare a list of targeted job seekers with contact information including address or telephone number for sending the promotional materials by mail or SMS messages.

3.38 The Labour Department has engaged a contractor for sending promotional messages by SMS. For the promotion of job fairs, a file with only the phone numbers of job seekers will be passed to the contractor for sending SMS messages. The contract requires the contractor to delete the file within 12 months after receiving such file.

B3. Telephone Employment Service Centre

3.39 A job seeker may use the service of Telephone Employment Service Centre after he has registered for employment services via Job Centres, Recruitment Centres or iES Website.

3.40 When a job seeker calls Telephone Employment Service hotline, he will be asked to enter the phone number registered as a key for searching his computer record. If the phone number entered is correct, the Internal Computer System will retrieve his record for the placement officer to view.

3.41 In case the phone number entered is incorrect or more than one job seeker is registered with the same phone number, the placement officer will ask the job seeker to provide his personal data for searching the correct record. The personal data to be asked are as follows:

(1) Telephone number;
(2) Name in Chinese or English;
(3) Date of birth; and
(4) iES Website username.

3.42 After the job seeker's record is retrieved, and before any services can be provided, the placement officer needs to verify his identity by asking:

(1) Name in Chinese or English; and
(2) Date of birth.

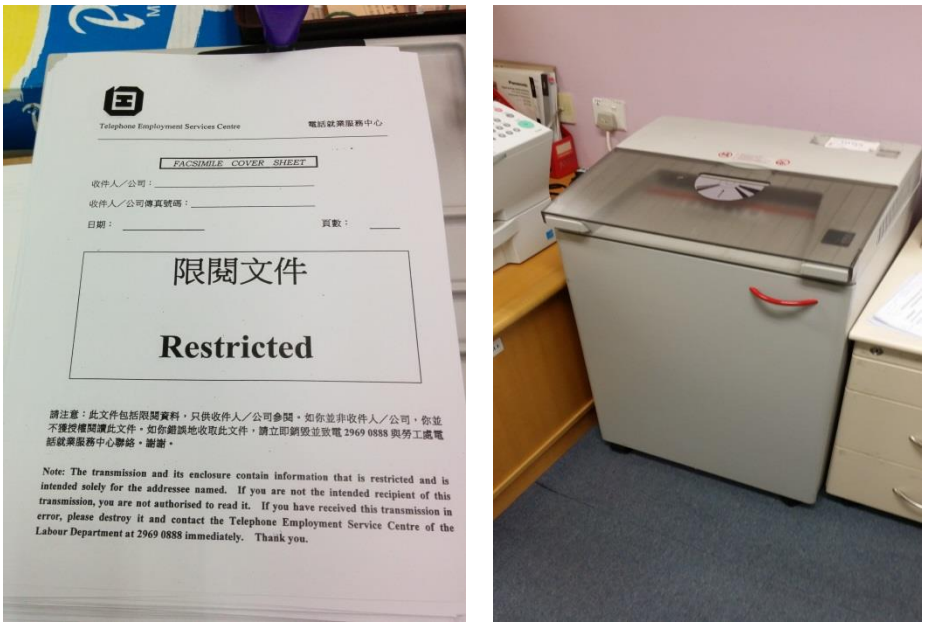
3.43 If the placement officer is in doubt of the job seeker's identity, he can further ask for the following personal data:

(1) Correspondence address;
(2) iES Website username; and
(3) Email address.

3.44 The job seeker whose identity is successfully verified can request the placement officer to refer a maximum of three vacancies of which the employers' contact details were not disclosed. He needs to provide the job order number of the vacancies to the placement officer, who will then retrieve the job seeker's record and the vacancies details from the Internal Computer System to check the job seeker's suitability for the vacancies. The placement officer will then contact the concerned employers to arrange interviews if the job seeker appears to be a suitable candidate. The placement officer will not disclose his name or contact information to the employer at this moment. As to other personal data such as education background or work experience, it will not be disclosed unless the job seeker has given consent.

3.45 If an interview is successfully arranged, the officer will inform the job seeker about the name, address and contact person of the employer and interview details such as the post applied, interview time and location over the phone. An Introduction Letter is also generated from the Internal Computer

System to be sent to the employer by fax or by post. The letter bears the job seeker's name in Chinese and English and interview details only. The letter will be faxed with a facsimile cover sheet marked "Restricted" to prevent the content being exposed.



Facsimile cover sheet marked 'Restricted'(Left) and paper shredder(Right).

3.46 Before sending the Introduction Letter by fax, the placement officer will double check the fax number with the employer over the phone and inform that the letter will be faxed to him immediately. After sending the letter, he will call the employer again to confirm receipt of the letter. Upon confirmation, he will shred the letter immediately.

3.47 The job seeker can request the placement officer to provide job matching service. The placement officer will check his personal data such as education background, work experience, job preference and expected salary against the vacancies available in the Internal Computer System to introduce suitable job vacancies to him. If he is interested in the vacancies, the placement officer will go through the process as mentioned in paragraphs 3.44 - 3.46 to follow up.

B4. iES Website

3.48 A job seeker can apply for a vacancy which accepts online application through iES Website by submitting his resume previously stored in his account to the concerned employer whose identity is disclosed on iES Website. After the job seeker has submitted the resume, a notification email will be generated and sent to the employer with a link for the employer to access his iES Website account. The employer can then login to view the job seeker's resume.

Main page of iES Website (Left) and the registration page for new job seekers (Right).

3.49 The job seeker can request to receive a copy of the notification email (without the link accessing the employer's iES Website account) by choosing the relevant function in his account.

3.50 In case the job seeker has consented to let employers view his selected information including education background, skills, language proficiency, work experience and job preference via the iES Website when choosing suitable candidates (as mentioned in paragraph 3.25), his information can then be searched and viewed anonymously by the employers who have registered in the iES Website and posted job vacancies through the Labour Department.

3.51 The employer can search for suitable job seekers by entering selection criteria into the iES Website such as work experience and skills, etc. After

searching, the matched job seekers' reference number, relevant work experience, expected salary and education level will be displayed. He may click on the job seeker's reference number to further view the job preference, education attainment, skills possessed, language proficiency and work experience of the corresponding job seeker.

3.52 When the employer has selected the job seekers who are suitable for the vacancy, he may approach the Labour Department to seek assistance in arranging the job seekers for interview. Alternatively, the employer may select the suitable job seekers online and the relevant Job Centre (in the same district where the employer locates) will be informed of the employer's selection through the Internal Computer System. The concerned Job Centre will then notify the selected job seekers and provide the vacancy information for their consideration. Interested job seekers can reach the employer directly through the contact means shown on the vacancy information, if any, or contact the placement officers for arranging job interview.

C. Amendment and withdrawal of the personal data of job seekers

C1. Job Centres

3.53 A job seeker can request to amend his registered personal data by submitting a completed personal data amendment form to any Job Centre in person. The staff of Job Centre will check the job seeker's HKID Card to verify his identity before updating his record. The processed form will then be passed to a clerk in-charge for storage.

3.54 On occasion, Job Centre may also allow a job seeker to amend his registered personal data via telephone. The staff will request the job seeker to provide his name, HKID Card number and one of his registered personal data including date of birth, telephone number, correspondence address, email address, nationality or date of arrival to Hong Kong for verifying his identity. The personal data to be amended cannot be the same as the personal data which is used for the verification of the job seeker's identity. For instance, if a job

seeker would like to update his telephone number, he is required to provide his name, HKID Card number and any one of his personal data mentioned above except his telephone number for verification. The staff will record and update the details in an amendment record form, which will then be passed to a clerk-in-charge for storage.

3.55 As mentioned in paragraph 3.10, the Labour Department will ask for the job seeker's consent to use his personal data for sending promotional information about the Labour Department's employment services. If a job seeker verbally requests to change the status from "not consent" to "consent", the staff will record his request and issue a confirmation letter to him. If the verbal request is to change the status from "consent" to "not consent", such request will be recorded but a confirmation letter will not be issued to the job seeker.

3.56 A job seeker can withdraw his registration by submitting an application form for withdrawal to any Job Centre in person or by fax. The staff of Job Centre will verify the job seeker's identity in accordance with the procedure mentioned in paragraph 3.53 (if submitting the form in person) or 3.54 (if submitting the form by fax). After verification, the staff will mark "withdrawal" in his record in the Internal Computer System and pass the form to the staff whose rank is clerical in-charge or above for confirmation.

3.57 The concerned Job Centre will then fax the form to Information Systems Office which will send a request to the Information Technology Management Division for erasing the record of the concerned job seeker in the Internal Computer System within one working day. The form will be faxed with a facsimile cover sheet marked "Restricted" to prevent the content from being exposed.

C2. Telephone Employment Service Centre

3.58 A job seeker can amend his registered personal data via Telephone Employment Service Centre. However, only correspondence address, telephone number, fax number, email address and information including education background, skills, language proficiency, work experience and job preference, can be amended.

3.59 A placement officer will first verify the job seeker's identity in accordance with the procedure mentioned in paragraphs 3.42 - 3.43.

3.60 The officer will then ask the job seeker to provide the original personal data he wants to amend for verification. The officer will record the details in an amendment record form and inform the job seeker a staff will later call him to verify the amendment.

3.61 The form will then be passed to a clerical officer for follow up. He will call the job seeker to verify the details within three working days. After verification, the form will be passed back to the placement officer for computer record updating.

C3. iES Website

3.62 A job seeker can login his account of iES Website to amend his personal data by himself. Once the updating is completed, the updated record will be copied to the Internal Computer System.

D. Retention of personal data of job seekers

3.63 Registration for the Labour Department's employment services is valid for three months, while the retention period of records containing job seekers' personal data vary according to the types of records.

D1. Paper records

3.64 The Labour Department files paper records containing personal data of job seekers in a restricted folder and store them in a locked steel cabinet or a locked record room before destruction. The clerks-in-charge are responsible for safe custody of the keys to the cabinets and record rooms.

Paper records are kept in store room / record room; the clerks-in-charge hold the room keys.

3.65 For most job seekers, the paper records kept in the Labour Department that contain their personal data are their Registration Forms. These forms will be retained in respective Job Centres for two years. The forms will be sorted by month after random checking of data input of the forms mentioned in paragraph 3.17 has been conducted.

Locked steel cabinets (Left) and retained data awaiting destruction (Right).

3.66 For other forms containing the personal data of job seekers, their respective retention periods are as follows:

Types of forms	***Relevant department***	***Retention period***
Personal data amendment form (submitted by job seeker to Job Centre in person - paragraph 3.53)	Job Centre	2 years
Amendment record form (record the personal data amendment via telephone to Job Centre – paragraph 3.54)	Job Centre	2 years
Amendment record form (record the personal data amendment via Telephone Employment Service Centre – paragraph 3.60)	Telephone Employment Service Centre	3 months
Application form for withdrawal (submitted by job seeker to Job Centre – paragraph 3.56)	Job Centre and IT Unit	2 years

D.2 Electronic records

3.67 Records of job seekers kept in the Internal Computer System will be retained for two years. The IT Unit is responsible for the housekeeping of these records.

3.68 Some working files containing the personal data of job seekers are stored in the individual computer of the staff or network drive to which he has access, such as the contact information of job seekers generated from the Internal Computer System for promoting job fairs. The Labour Department confirmed that these working files will not be kept longer than is necessary for the purpose of rendering employment services and will be deleted after use. During site inspection, the Team had checked the network drive and did not find such working files.

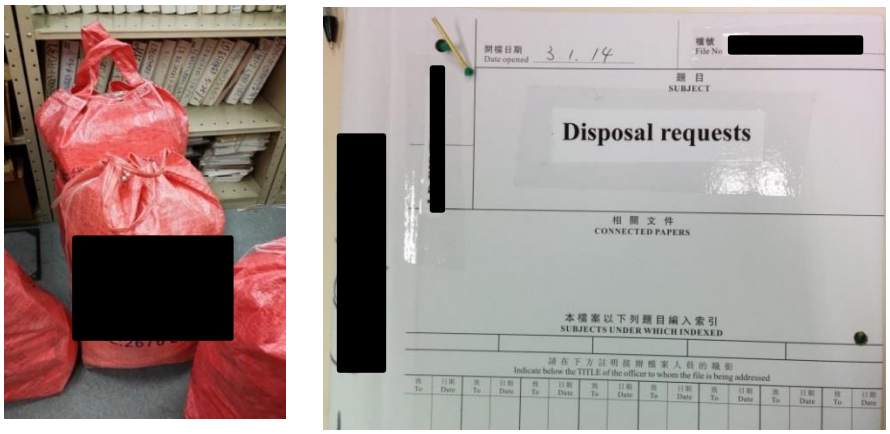
E. Destruction of personal data of job seekers

E.1 Paper records

3.69 The records are disposed of according to the disposal schedules approved by the Government Records Service. A checking exercise for destruction of obsolete records is conducted annually, by following the checklists provided by the Divisional Headquarters for handling disposal of various types of records. By the end of January each year, the clerks in-charge will bundle up all records to be destroyed and submit a memo to the Divisional Headquarters giving details of the nature, title, date coverage and quantity of the records to be destroyed.

3.70 The Divisional Headquarters will consolidate returns from all offices and seek authorisation from the Government Records Service to dispose of the relevant paper records in accordance with the disposal schedules via General Registry of the Labour Department. Once approval from the Government Records Service is obtained, the Divisional Headquarters will inform the

corresponding clerks-in-charge to arrange with the contractor engaged for file disposal for the physical destruction of the records. A staff will be assigned to accompany the delivery of files to the contractor's site and monitor the contractor throughout the destruction process.



(Left) Paper records ready for destruction are sealed in designated bags specified by the contractors. (Right) Approval for records destruction is sought from the Government Records Service.

E.2 Electronic records

3.71 The job seekers' records in the Internal Computer System will be removed to a temporary storage inaccessible to the users of the system upon the expiry of the retention periods. When the approval from the Government Records Service is obtained, the IT Unit will purge the records manually.

Chapter Four

Findings and Recommendations

Preliminaries

4.1 Findings and recommendations made in this Report were based on the information provided by the Labour Department and the Team's on-site observations at the material time. They are not intended to be exhaustive to cover every aspect of the operation of the personal data system inspected, and may be regarded only as verification of the compliance level of the matters in question at the time when the Inspection was carried out.

4.2 The findings are divided into two categories. The first category consists of "specific findings" regarding the level of compliance with DPP1 to DPP5 and Part VIA of the Ordinance. The second category consists of "other findings" in relation to the general measures adopted by the Labour Department in personal data protection.

Specific Findings

DPP1 – Purpose and Manner of Collection of Personal Data

Requirements under the Ordinance

4.3 DPP1 regulates the collection of personal data in respect of (a) the purposes for which the personal data is collected and whether it is necessary to collect such personal data; (b) the means for collecting the personal data; and (c) the duty of the data user to inform the data subject details of such collection (including the purpose of collection and classes of possible transferees of the data).

4.4 As the Labour Department collects HKID Card number, analysis has been made in accordance with the "Code of Practice on the Identity Card Number and other Personal Identifiers" (the "**Code**") issued by the Commissioner. Extracts of the relevant paragraphs of the Code are reproduced in Annex 4.

The Team's findings

4.5 A job seeker who wishes to use employment service, participate in job fairs, use telephone employment service and certain functions such as uploading resume to iES Website is required to register with the Labour Department. The Labour Department collects job seekers' personal data, such as name, HKID Card number, education level, skills, etc. from job seekers via Registration Form and registration interface at iES Website.

4.6 In addition, information of the interview result, position recruited, date of employment and salary offered are collected from employers' replies after making job referrals and organising job fairs.

4.7 A PICS is included in the Registration Form, the first page of iES registration interface, and posted at Job Center's service booths where the Labour Department staff meet the job seekers. The PICS in the Registration Form and registration interface, among others, covers (a) the purpose of data collection, (b) whether it is obligatory or voluntary for the job seeker to supply the data and the consequences of not supplying the data, (c) transfer of data, (d) data access and correction rights and the contact details of the individual who handles such request. The PICS also advises the job seekers that he can at any time refuse to receive information on job vacancies and employment services even if he chooses to receive such information at the time of registration.

4.8 It is stated in the PICS that data collected from the Registration Form/registration interface and employer's reply after job referral is used for the purpose of providing job referral or related employment services.

4.9 The Team reviewed the personal data collected through the Registration Form and registration interface and considered that the data collected serves the purpose of providing employment services to the job seekers. However, the Team noted that the personal data collected from the employer as mentioned in paragraph 4.6 above mainly served to verify whether the post and salary offered tally with the vacancy posted, to confirm whether the salary will not be lower than that stated in the vacancy posted, and for the department's statistical purpose. The Team was advised that the Labour Department will follow up with the employer if the salary offered is lower than that stated in the vacancy posted to understand the reasons behind. The date of employment information also serves to facilitate monitoring of employment subsidy programmes with a limited duration.

4.10 After a Job Centre has arranged an interview between the employer and the job seeker, the Job Centre will provide the job seeker with an Introduction Letter to be presented to the employer. The Introduction Letter advises the employer about the interview arrangement. It bears the job seeker's name, post applied, interview date and time, and contains a reply slip from employer ("**Reply Slip**"), which lists the types of personal data that the Labour Department requests the employer to provide. If the interview is arranged by the Telephone Employment Service Centre, the Labour Department will fax the Introduction Letter to the employer without providing a copy to the job seeker. A job seeker may therefore not be aware of the types of personal data that may be disclosed to the Labour Department by the employer if the job referral is made by the Telephone Employment Service Centre.

4.11 The Labour Department will not use the Introduction Letter in a job fair. It will provide a list for the employer to complete and return to the Labour Department after the job fair to collect the personal data of interviewed job seekers as mentioned in paragraph 4.6 above. Hence, a job seeker who attends a job fair may not be aware of the types of personal data that may be disclosed to the Labour Department by the employer.

4.12 The Team noted that job seekers are not explicitly informed what types of personal data will be collected from employers after job referrals or job fairs. The Labour Department explained that job seekers should have been made aware of such collection as the types of personal data to be collected are shown in the Reply Slip at the bottom of the Introduction Letter.

Commissioner's comments and recommendations

4.13 The Commissioner opines that the personal data collected from the job seekers through the Registration Form and registration interface is for a lawful purpose directly related to the Labour Department's functions and the data collected is in general adequate but not excessive.

4.14 The Commissioner also concludes that the collection of HKID Card number is justified under Paragraph 2.3.1 of the Code which allows the collection of HKID Card number if a statutory provision confers on the data user the power to collect the HKID Card number. Section 5 of the Registration of Persons Ordinance (Cap. 177) confers on a public officer[16] the power to require any registered person in all dealings with the Government to furnish his HKID Card number. The Labour Department staff, being public officers, is therefore entitled to collect HKID Card numbers in the provision of the employment service. The Commissioner also notes that one of the Labour Department's duties is issuing of licences to and regulating the operation of employment agencies in Hong Kong under Part XII of the Employment Ordinance (Cap. 57), which defines an employment agency as "an establishment or person who aims at obtaining employment for another person or supplying personnel to an employer". Section 56(1)(a) of the Employment Ordinance stipulates that an licensed employment agency has to maintain a record of all registered job applicants containing, among other information, their HKID Card numbers. Although the Labour Department, as the issuing

[16] Section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) defines "public officer" to mean any person holding an office of emolument under the Government, whether such office be permanent or temporary.

authority of licences for the operation of employment agencies, is exempted from this requirement under the Employment Ordinance, since the nature of its employment services is the same as that of an employment agency, and the Labour Department itself is responsible for regulating the employment agencies, it is axiomatic for the Labour Department to follow the requirements of the Employment Ordinance to collect and keep the HKID Card number of job seekers. Besides, according to the Immigration Department[17], in order to be lawfully employable in Hong Kong, a person should hold either a Hong Kong permanent identity card or a Hong Kong identity card and who is free to take up employment in Hong Kong without prior permission and has not breached any condition of stay. Before referring job seekers to employers, the Labour Department should have the responsibility to check that they are lawfully employable and collection of HKID Card numbers from job seekers can serve the purpose of verifying whether they are lawfully employable.

4.15 As regards the collection of personal data from employers, the Commissioner observes that it is not transparent to the job seekers what are the types of personal data that the Labour Department may collect from the employer after an interview has been conducted because such collection can only be inferred from reading the Reply Slip, which is primarily intended for the employer, instead of the job seeker, to read and complete. This is particularly so if the job seeker is not given the Introduction Letter in the situation where the job seeker uses the telephone employment service, or attends a job fair. The Commissioner is of the view that a job seeker should be fully informed by the Labour Department of the types of personal data that it intends to collect from employers and the purposes for which the data is to be used.

[17] Frequently Asked Questions of Visit/Transit published by the Immigration Department (www.immd.gov.hk/en/faq/visit-transit.html)

Recommendation:

(1) State clearly in the PICS provided to the job seekers both the types of personal data that will be collected from the employers after job interviews and the purposes of collecting such personal data.

DPP2 – Accuracy and Retention of Personal Data

Requirements under the Ordinance

4.16 DPP2(1) requires data users to, among other things, take all reasonably practicable steps to ensure that the personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used.

4.17 DPP2(2) stipulates that personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used. Section 26(1) of the Ordinance similarly stipulates that once the personal data held is no longer required for the purpose (including any directly related purpose) for which the data was used, a data user must take all practicable steps to erase the personal data unless any such erasure is prohibited under any law or it is in the public interest (including historical interest) for the data not to be erased. DPP2(3) stipulates the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

The Team's findings on accuracy of personal data

First time registration

4.18 When a job seeker submits a Registration Form in person at a Job Centre, the Labour Department staff will check the job seeker's name and HKID Card number against the HKID Card presented on site. Accuracy of other information such as education level, skills and work experience provided by the job seeker will not be verified by the Labour Department. It is stated in the Registration Form that the provision of such information assists the Labour Department in searching suitable jobs for the job seekers and so it should be in the job seeker's interest to provide accurate data.

4.19 After receipt of the Registration Form at Job Centre, the Labour Department staff will input the data into the Internal Computer System. In March 2014, the Labour Department's Employment Services Division introduced the practice of random checking of the accuracy of data input into the Internal Computer System. A staff member assigned by the Job Centre's manager will select 5% of the Registration Forms received in the last month and verify the accuracy of the data input into the Internal Computer System. The staff verifying data accuracy must be different from the one inputting the data. The Labour Department advised that the Job Centres' managers have full discretion as to detailed implementation of the random check, including whether and how the results of the checking are reported to the Job Centres' managers. The Labour Department also advised that around 90% of cases checked achieved 100% accuracy, with input errors usually caused by the unclear handwriting of the job seekers found in the remaining samples.

Subsequent amendments

4.20 In case a job seeker wishes to update his data provided to the Labour Department, he can submit an amendment form in person to the Job Centre, call a Job Centre, or the Telephone Employment Service Centre to request for

amendment of his record, or amend the data on his own through the iES Website.

4.21 If a job seeker submits the amendment form in person at a Job Centre, the staff will verify his identity by checking his HKID Card and amend the computer record accordingly.

4.22 When a job seeker calls a Job Centre to amend his record, the Job Centre will encourage him to visit the Job Centre in person or amend the record through the iES Website. The staff can amend the record for simple data amendments such as where the job seeker requests to stop receiving promotional information about the Labour Department's employment services, or in special circumstances. The staff will (a) verify the job seeker's name, HKID Card number and one additional type of registered data, such as date of birth, contact phone number, (b) record the requested amendment in a form and (c) amend the computer record accordingly. There is no random checking of the accuracy of data input for amendment cases. It is however not common for a Job Centre to receive such request over the phone (only two cases in 2013).

4.23 Telephone Employment Service Centre can also amend the following record of a job seeker after verifying his identity in accordance with the procedure mentioned in paragraphs 3.40 - 3.43: (a) correspondence address; (b) phone/fax number; (c) email address and (d) qualification and skill.

4.24 The staff will follow the steps below:

(1) Ask the job seeker to provide the previously registered data for each of the proposed change;
(2) Complete a specific form for change of record;
(3) Inform the job seeker that another staff will contact him to verify the data;
(4) Pass the form to another staff who will contact the job seeker by phone using the contact phone number in the computer record

within three working days to confirm the change; and

(5) Update the computer record.

The Team's findings on retention of personal data

4.25 According to the internal guideline on "Destruction of Records" issued by the Labour Department's Employment Services Division, Registration Forms will be destroyed two years after completion of data input. The Labour Department also explained that the disposal schedule of Registration Forms has been approved by Government Records Service. However, during the site inspection of one of the Job Centres, the Team found that Registration Forms dating back to 2008 were retained.

4.26 The computer records in the Internal Computer System are purged after the two years' retention period and the Team confirmed that no computer records aged over two years were kept when sample check was conducted during the Inspection.

4.27 The Internal Guideline on Destruction of Records was last revised in 2003. Since then, there has been no formal review of the retention policies.

4.28 The Team noted some inconsistent practice in the file retention arrangement by the Job Centres and Telephone Employment Service Centre. For example, job seekers' amendment forms were kept for two years in Job Centres but only three months in Telephone Employment Service Centre.

4.29 The Labour Department engages a contractor for sending job fair promotional message by SMS. The Labour Department sends a file with phone numbers and around 60 words of the promotional message to the contractor who then sends the SMS to the phone numbers. Contractual obligations are imposed on the contractor to delete the file within 12 months after receiving such file.

Commissioner's comments and recommendations

4.30 The Commissioner noted the introduction of the random checking of the accuracy of data input in March 2014. However, no guidelines have been drawn up as regards how the results of the random check should be followed up to enhance overall data accuracy. The effectiveness of the random check has yet to be tested due to the short implementation period. Job Centres' managers are given the discretion on the implementation details including whether and how they monitor the result, whether and what actions will be taken for repeated incorrect data input, etc. It was observed that each of the Job Centres visited has deployed different checking procedures and designated staff of different grades to conduct random checking. The Labour Department should formulate more detailed guidelines to improve management control on data input and assess its effectiveness. The accuracy checking should also be extended to cover subsequent data amendments.

4.31 There is no checking by the Divisional Headquarters to ensure documents that passed the retention period have indeed been destroyed. In addition, the reliance of a retention policy established more than ten years ago without any plan of regular review is not satisfactory.

4.32 The contractor is allowed to keep files containing phone numbers of job seekers for sending SMS for as long as 12 months, which appears to be longer than necessary for the purpose of sending promotional messages by SMS. The Labour Department should review the retention period imposed on the contractor.

Recommendations:

(2) Monitor the error rate of data input and review whether the newly adopted 5% accuracy check is adequate; introduce standard procedures designating supervisory staff to conduct checking and requiring the Job Centre's manager to review the error reports and improve the accuracy rate, for example by setting out the actions taken against staff who

repeatedly input incorrect data, sharing the common mistakes among the team, etc.; extend the accuracy check to cover subsequent data amendments.

(3) Introduce management control for example by paying surprise visit to the Job Centres to ensure Registration Forms and other forms containing personal data are destroyed according to schedule.

(4) Review file retention policies on a regular basis and across different Divisions within the Labour Department.

(5) Review the appropriateness of the retention policy imposed on the contractor in respect of files containing phone numbers of job seekers for sending SMS and shorten the retention period where appropriate.

DPP3 – Use of Personal Data

Requirements under the Ordinance

4.33 DPP3 requires data users not to use (which includes "transfer" or "disclose") personal data for a new purpose unless with the prescribed consent from the data subjects. New purpose is defined under the Ordinance to mean any purpose other than a purpose which is the same as or directly related to the collection purpose.

The Team's findings

4.34 The PICS specifies that the Labour Department may transfer job seeker's personal data to employer or related organisation, as well as other divisions of the Labour Department for enforcement of the ordinances under the Labour Department's jurisdiction.

Transfer of personal data to employer

4.35 When providing job referral services, the Labour Department staff will disclose to the employer the job seeker's suitability for the post upon obtaining the job seeker's consent. The Team was informed that the majority of employers (99%) who post their job vacancies at the Labour Department provide their contact details in the job advertisement and job seekers can contact the employers directly. It is only with regard to the remaining 1% of employers whose contact details are not disclosed that job seekers will need to approach Job Centres or Telephone Employment Service Centre for job referral services. A tripartite tele-conference may be arranged upon agreement with the employer and the job seeker. The Team observed the job referral process and noted that verbal consent has been obtained from job seekers before the placement officers of Job Centres and Telephone Employment Service Centre called the employers.

4.36 If the employer requests for the job seeker's resume, the Labour Department staff will ask the job seeker to send the resume to the employer directly. The Team was informed that the Labour Department would disclose the employer's identity and contact means to the job seeker during the referral process and no irregularity was detected during the Inspection. However, there is no written guideline stating clearly the requirement to disclose the employer's identity to the job seeker before provision of the resume. In this situation, if only the employer's fax number or email address but not the employer's identity is disclosed to the job seeker, this may be unfair to the job seeker as his personal data is collected by the employer whose identity is unknown to him.

Disclosing of personal data to employer

4.37 In case the job seeker has consented to let employers view his selected information including education background, skills, language proficiency, work experience and job preference via the iES Website when

choosing suitable candidates, his information can be searched and viewed anonymously by the employers who have registered in the iES Website and posted job vacancies through the Labour Department.

Use of personal data for promotional purpose

4.38 The Registration Form and registration interface provide a check box for the job seeker to indicate if he wishes to receive information of the relevant job vacancies, recruitment activities and employment services, and state the ways (by contacting the manager of the Job Centres or sending an email to the Labour Department) for the job seeker to inform the Labour Department if he decides not to receive such information at a later stage. Employment services will still be provided if the job seeker chooses not to receive any such promotional information.

4.39 The Labour Department will send job fair promotional materials by mail or SMS and may approach the job seekers over the phone for potential job opportunities to relevant registered job seekers who agree to receive promotional messages. When sending promotional message by SMS, the Labour Department will provide only the phone numbers of job seekers to the contractor for sending SMS. Names or other personal data are not provided to the contractor.

Transfer of personal data to other parties

4.40 There was no transfer of personal data to the Law Enforcement Division in the Labour Department in 2013. The Labour Department explained that there were transfers of the personal data to the Law Enforcement Division for the purpose of discharging the duties under the ordinances administered by the Labour Department, such as investigating default in salary payment and disputes.

Commissioner's comments and recommendations

4.41 The Commissioner notes the types of information disclosed to the employer for job referral purpose and is satisfied that consent from the job seekers have been obtained before such transfer. However, the Labour Department should ensure the employers' identities are made known to the job seekers in case they are requested to send their resume directly to the employers. In the event that the employer does not wish to disclose his identity, the Labour Department should provide the employer's contact phone number to the job seeker who could then make enquiries with the employer directly before providing his personal data.

4.42 The Commissioner is pleased to note that job seekers' profile is disclosed anonymously in iES Website for employers to view and search. He is also pleased to see the option offered to job seekers on the receipt of promotional information in the Registration Form and registration interface, and the option of change of mind after registration. Moreover, if the promotional messages are job fair related, such use is in line with the original purpose of assisting job seekers in procuring employment.

Recommendation:

(6) Devise clear guidelines to disclose employer's identity for the situation where a job seeker is requested by the employer to provide his resume to ensure fair collection of personal data by the employer, and provide the employer's contact phone number to the job seeker if the employer does not wish to disclose his identity.

DPP4 – Security of Personal Data

Requirements under the Ordinance

4.43 Under DPP4, data users are required to take all reasonably practicable steps to ensure that the personal data they keep is protected against unauthorised or accidental access, processing, erasure, loss or use. In ascertaining the appropriate steps to take, the data users have to consider, among other things, the kind of data and the harm that could result if such irregularities should arise, and the security measures incorporated into any equipment in which the data is stored. The requirement is not to impose an obligation on data users to provide absolute security of personal data, but the steps taken to safeguard security should be proportionate to the sensitivity of the personal data involved.

The Team's findings

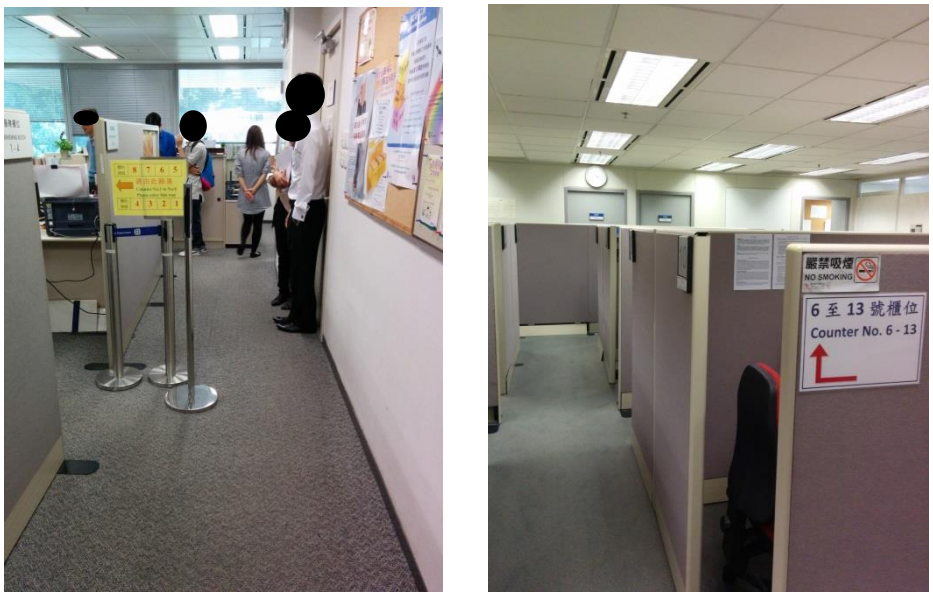
Physical security at Job Centres in protecting personal data

4.44 At Job Centres, completed Registration Forms are kept by individual staff for data input (usually completed on the day upon receipt of the Registration Forms) and then passed to a designated staff who will temporarily lock the Registration Forms in his cabinet for performing random check of accuracy of data input on a monthly basis. After the monthly check, the Registration Forms are stored in locked cabinet in a storage room.

4.45 Confidential files containing complaints received from job seekers are kept in the Job Centre manager's steel cabinet fitted with a locking bar and padlock.

Steel cabinet fitted with a locking bar and padlock to store confidential files.

4.46 The service booths where the placement officers meet the job seekers for provision of employment services are located inside the office area, shared with other internal staff of the Job Centre. When asked if there could be any separation of the area serving the public and other internal restricted area, the Labour Department explained that the setting had been previously designed and was unlikely to be changed but their staff will be very alert of any persons wandering inside the office areas.



There is no separation between the cubicles serving the public and the internal office area.

Computer system where personal data is stored

4.47 Job seeker's personal data is stored in the Internal Computer System and iES Website system.

4.48 There are three different privilege rights in accessing job seekers' personal data in the Internal Computer System according to the staff's rank. The more senior staff will be granted more access rights such as for generating a list of job seekers from the system by inputting certain search criteria. Each staff is provided with a login account and he is obliged to change his password every six months or login will be disallowed.

4.49 Reports showing the records of registered job seekers can be generated from the Internal Computer System. The records generated however will not contain job seekers' HKID Card number as all HKID Card numbers have been masked. In each Job Centre that we visited, only three staff members, out of a total of 17 staff of a Job Centre on average, with their ranks not lower than Assistant Clerical Officer are authorised to generate such reports to identify job seekers for job referrals and job fairs and for statistical purpose.

4.50 The Internal Computer System account will be disabled upon departure (or posting out) of a staff member. However, the same default password for creation of a new Internal Computer System account is assigned to every new staff who comes on board. Members of IT Unit therefore know the default password for the Internal Computer System accounts (for new comers) which are not so set up as to force the user to change it after the first login. Although an e-mail reminding the new staff to change the password will be sent after his first login and the Team was advised that most of the new staff will change the password immediately, there is a potential risk that the default password may be kept unchanged for six months if the new staff does not change the password after receiving the reminder and a third party may easily impersonate the user to access the Internal Computer System.

4.51 According to the Labour Department's Personal Data Handling Guidelines for the Internal Computer System Users, in no circumstances shall users of the Internal Computer System be allowed to store personal data retrieved from the Internal Computer System in an external storage device, unless exceptionally warranted for the purpose of rendering employment/recruitment services to registered job-seekers/employers and with prior approval obtained from the Division Head. The Division Head of Employment Services Division claimed that no approval has been granted so far.

4.52 Staff of the Labour Department cannot access a job seeker's iES Website account. A job seeker's iES Website account will be locked due to repeated incorrect login. In such case, the job seeker is required to send an email providing his personal data including English name as shown on his HKID Card, date of birth, contact phone number, the first four digits of his HKID Card number and his account login name to unlock the iES Website account. The Labour Department, after noting the Team's on-the-spot observation of such transmission of extensive data via unsecured means, restricted the types of personal data required to unlock the account to only account login username and registered contact phone number from the second week of June 2014. However, email is still not considered a secure way to transfer personal data.

4.53 Job seekers can use the public sharing computers at Job Centres to build resumes. These computers are separated by partition and the monitors protected by privacy screen filters. A passer-by could not see the contents displayed on the monitor easily except if he stands right behind the user, but this will be easily spotted by the counter staff who will periodically pay attention to that area and check whether those computers are in proper usage. After reboot, all settings and data used by the previous user/session will be erased because the system installed will reload a new Windows installation.

The public sharing computers at Job Centre

Disposal of storage devices

4.54 The Labour Department advised that staff must follow the guidelines[18] given by the Office of the Government Chief Information Officer ("**OGCIO**") to dispose of storage devices containing personal data. An email was issued during the Inspection to remind staff concerned of the steps on disposing of IT equipment involving computers, notebooks and servers.

4.55 The Labour Department maintains a list to monitor the movement of all IT equipment and explain why the equipment was disposed of. An internal committee would certify the disposal of IT equipment. Upon receiving confirmation from the committee, IT staff would follow up the removal of the personal data stored therein (e.g. degaussing or physical destruction) before disposal.

4.56 There is no departmental-wide procedure or control on the disposal of equipment including computers and storage devices nor a remark in the list to remind staff to erase the personal data stored therein according to OGCIO's instructions. This may be of concern especially when it comes to the disposal of equipment other than IT equipment which may store personal data (e.g. photocopiers might come with in-built storage that retains copies of documents

[18] OGCIO Circular No. 5/2010: Maintenance, Re-Use and Disposal of Office Equipment and Computers Containing Classified Information

scanned or copied or printed.)

Other security issues

4.57 The Team noted that the Labour Department has devised a department-specific high-level IT security policy based on the OGCIO recommendation. However, no department-specific IT security guideline is in place. The Labour Department advised that its users can refer to the OGCIO IT Security Guidelines if needed. However, the OGCIO Security Guidelines are not made immediately available in Labour Department's intranet. Instead, users would have to indirectly visit the Central Cyber Government Office (the government's intranet portal) to access the OGCIO IT Security Guidelines. The Team also noted that no formal assessment was conducted as to whether OGCIO's IT Security Guideline could be fully adopted by the Labour Department.

4.58 There is a detailed document setting out information security incident handling procedures. However, similar details are not provided in respect of data breach handling. A memorandum titled "Handling of Documents Containing Personal Data" contains one paragraph mentioning the handling of a data breach, but it merely states that the subject officer concerned should report the incident to their supervisor(s) in a timely manner (without specifying the expected timeframe) after a thorough search of the document concerned has been done, and that the subject officers are reminded to refer to the Guidance Note issued by this Office.

4.59 Staff may store files in shared drive which can be accessed by other staff in the same office. Files containing personal data of job seekers will be saved in the shared drives temporarily in some tasks such as preparing the contact information list of selected job seekers for promotion of job fair. The concerned files will be removed after use. A designated staff is assigned in each office to conduct regular check on the shared drive to ensure files containing personal data are deleted after use. The Team checked on the spot

the shared drives of each Job Centres visited and found no files containing personal data. However, no written guideline can be found on this aspect.

Commissioner's comments and recommendations

4.60 The Commissioner is concerned about the risk of trespass by unauthorised persons into restricted areas where the personal data of job seekers is stored or processed.

4.61 The Commissioner is satisfied with the overall security of the Internal Computer System. However, improvements on reactivation of iES account and password control on new users of the Internal Computer System are suggested.

4.62 Though the Team did not spot any major security issues, the Inspection shows a lack of appropriate measures, in the form of guidelines, procedures or other form of elaboration, to minimise human error in the operation of the Internal Computer System, disposal of storage device and erasure of records in shared drives. Besides, a data breach incident may or may not involve information security. The guidance note issued by the PCPD is only for general reference by data users. The lack of a detailed procedure tailored to the circumstances of the organisation may mean delay in handling a data breach incident and inability to timely contain the harm.

Recommendations:

(7) Introduce means to prevent trespass by unauthorised persons into restricted areas where the personal data of job seekers is stored or processed as a stop-gap remedial measure to address the unsatisfactory office layout, for example, install an electronic lock at the entrance to internal office areas, escort the job seeker when he enters internal office area to meet with the officer, and post prominent signs that demarcate clearly the service booth area and the internal office area, etc.

(8) Allow job seekers to apply for account re-activation after unsuccessful login via iES Website with encryption enabled instead of by email.

(9) Enforce, by technical means, the change of default password of the Internal Computer System by new staff at first login.

(10) Formulate guidelines on the disposal of equipment that may store personal data such as computers and photocopiers to ensure all personal data is erased.

(11) Devise Data Breach Handling guidelines, evaluate the need to devise Labour Department-specific guidelines on IT security to include implementation details for staff to follow and clearly inform the staff of which IT security guidelines to follow and where to locate such guidelines.

(12) Formally devise procedures and monitoring mechanism on the erasure of records containing personal data in shared drives.

DPP5 – Information to be Generally Available

Requirements under the Ordinance

4.63 DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can (i) ascertain a data user's policies and practices in relation to personal data; (ii) be informed of the kind of personal data held by a data user; and (iii) be informed of the main purposes for which personal data held by a data user are or are to be used.

The Team's findings

4.64 The "Employment Services Division's Privacy Policy and Practice Statement" is posted in each service booth in the Job Centre. The Team noted that the statement covers how the division applies the six DPPs in the handling of personal data and provide ways for the individual to make enquiries in relation to its privacy policy.

4.65 Different Privacy Policy Statements are available on the iES Website (http://www1.jobs.gov.hk/1/0/WebForm/commonpage/com_privacy.aspx) and iES Mobile App. The Team noted that the statements state the types of data that may be collected through the website and the mobile application. The Privacy Policy Statement for the mobile application specifically sets out that no individually identifiable data will be collected through the mobile application.

4.66 As mentioned in paragraph 4.12, the Team noted that job seekers are not explicitly informed of the types of personal data that will be collected from employers after job referrals or job fairs. Such collection can only be inferred from reading the Reply Slip of the Introduction Letter.

Commissioner's Comments

4.67 The obligations of accessibility and transparency of a data user's personal data policies and practices under DPP5 are important. The Commissioner has not found major issue in relation to the Labour Department's compliance with DPP5. The Labour Department should, however, refer to the recommendations made under DPP1 for improving the clarity of the types of job seekers' personal data collected from employers and the purposes of such collection.

Other Findings

CCTV

4.68 The Labour Department has installed for security purpose closed-circuit television ("**CCTV**") cameras in the public areas of the Job Centres and Recruitment Centres. Notices have been posted prominently but contact phone

number for questions are not provided. The Labour Department advised the Team that it is its practice to retain the CCTV video images for a period of about 90 days. However, no specific written instructions or guideline on the use of CCTV has been issued by the department. The Labour Department explained that it simply adopts the "Guidance on CCTV Surveillance Practices" published by the PCPD in the management of the CCTV systems. The "Guidance on CCTV Surveillance Practices" was last circulated in February 2013.

Notices are prominently displayed in the vicinity of areas with CCTV operation.

4.69 The Team notes that the control panels and monitors for the CCTV systems are kept in different places in the three Job Centres and two Recruitment Centres visited. Only one Job Centre and two Recruitment Centres placed the CCTV control panels and monitors in a locked cabinet or locked room, while one Job Centre placed them in an unlocked room and another Job Centre placed them beside a staff member's work station located in the open area of the office accessible by job seekers using employment services. No login or password is required to prevent unauthorised persons from accessing the system/images. The Team also notes that the systems are installed with DVD Read/Write drives and USB ports with operation manuals

placed near the systems. There is no designated staff in charge of the CCTV operation except in one of the Centres visited.

Monitor displaying CCTV images with Read/Write capabilities.

Commissioner's comments and recommendations

4.70 Overall speaking, the security measures for protecting the CCTV images are not satisfactory and must be strengthened. The guidance note published by PCPD is for general reference and efforts must be made by the data user to adapt it to its specific operations. With no written policy on the security, retention and disposal of the captured CCTV images, it would be difficult for the Labour Department to ensure systematic protection and security, prompt disposal and destruction of the data. This could result in unauthorised access to the data and its being kept for longer than is necessary.

Recommendation:

(13) Devise and implement CCTV policies and/or procedures specifying who are authorised to access the captured CCTV images, the security of the CCTV systems and the retention period of the captured CCTV images; include in the CCTV notice the contact phone number of Labour Department staff for public enquiry.

Training

4.71 All newly recruited Assistant Clerical Officers and Clerical Assistants are required to attend an Induction Course organised by Civil Service Bureau which includes a session entitled "Introduction to PD(P)O". Office-based briefing which covers the Ordinance will also be arranged to staff of different ranks from time to time to brief and remind them of the procedures/guidelines in handling job seekers' personal data and the importance of complying with the Ordinance. The Information Systems Office will also provide regular workshops to focus on information protection and security for staff computer users generally. The Team noted that an IT Security Awareness Seminar which was compulsory for all staff handling personal data was held in late March 2014. However, previous workshops entitled "A workshop on Information Protection and Security for General Computer Users for staff of ESD and EIPD" held in 2011, 2012 and early 2014 were attended on a voluntary basis only. The Team also noted that there is no training plan to ensure staff handling personal data are provided with regular training on personal data protection.

4.72 "Guidelines on Handling Documents Involving Personal Data at ESD(HQ), JCs/EOS/RCs, WTSCO and EPMCO of ESD" are circulated once every six months to remind staff of the procedures and general principles to be observed in handling personal data. The Team noted that staff are required to sign off to acknowledge having read these Guidelines.

Commissioner's comments and recommendations

4.73 All personnel involved in the handling of personal data should be made aware of the importance of respecting the data privacy rights of individuals and the legal requirements of the Ordinance. They should be adequately trained in understanding the requirements of the Ordinance and the Labour Department's compliance procedures in place.

Recommendation:

(14) Devise a training plan to ensure staff handling personal data is provided with regular training on personal data protection.

Chapter Five

Conclusion

5.1 It is necessary for the Labour Department to collect and retain the personal data provided by the job seekers when rendering its employment services, including job referral and counselling services and provision of job fair information to the job seekers.

5.2 The Commissioner is reasonably satisfied with the data protection measures in the personal data system of the employment services provided by the Labour Department. Based on the findings of the Inspection, he makes 14 recommendations, including but not limited to notifying the job seeker as to the types of personal data that will be collected from the employer and the purposes for which the data is to be used.; introducing management control to ensure Registration Forms and other forms containing personal data are destroyed according to schedule; devising clear guidelines to ensure disclosure of employer's identity if a job seeker is requested to send his resume to the employer directly; introducing means to prevent trespass by unauthorised persons inside the office area; and devising and implementing CCTV policies and/or procedures.

5.3 The Commissioner wishes to thank the co-operation of the staff of Labour Department, which helped this Office understand the data flow and the reasons for collecting, retaining and processing of personal data. The Commissioner appreciates their assistance, rendered over and above their normal duties.

5.4 The Commissioner hopes that this report will be of value to the Labour Department. Other government departments and public organizations which collect personal data from members of the public for providing public service in a similar way are encouraged to take reference from this report.

5.5 More generally, recalling the pledge made by government bureaux and departments to implement Privacy Management Programmes ("**PMP**"), the Commissioner hopes that bold and decisive steps will be taken by them in this regard. PMP will build a robust privacy infrastructure supported by an effective

ongoing review and monitoring process to facilitate compliance with the requirements under the Ordinance. It will also demonstrate the government's commitment to good corporate governance and building trust with the citizens that it serves. More details about PMP are found in "Privacy Management Programme – A Best Practice Guide" (www.pcpd.org.hk/pmp/).

Annex 1 - Data Protection Principles and Part VIA of the Personal Data (Privacy) Ordinance

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

(1) Personal data shall not be collected unless-

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

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

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

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

(a) lawful; and

(b) fair in the circumstances of the case.

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

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

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

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

(b) he is explicitly informed-

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

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

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

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

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

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

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

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

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

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

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

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

(ii) the data is erased;

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

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

(ii) that data was inaccurate at the time of such disclosure,

that the third party-

(A) is informed that the data is inaccurate; and

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

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

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data

user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes.

3. Principle 3 - use of personal data

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

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

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

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

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

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

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

4. Principle 4 - security of personal data

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

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

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

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

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

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

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

(3) In subsection (2)—

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

5. Principle 5 – information to be generally available

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

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

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

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

Part VIA – Use of Personal Data in Direct Marketing and Provision of Personal Data for Use in Direct Marketing

Section 35A - Interpretation of Part VIA

(1) In this Part—

consent (同意), in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision;

direct marketing (直接促銷) means—

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

(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means;

direct marketing means (直接促銷方法) means—

(a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or

(b) making telephone calls to specific persons;

marketing subject (促銷標的), in relation to direct marketing, means—

(a) any goods, facility or service offered, or the availability of which is advertised; or

(b) any purpose for which donations or contributions are solicited;

permitted class of marketing subjects (許可類別促銷標的), in relation to a consent by a data subject to an intended use or provision of personal data, means a class of marketing subjects—

(a) that is specified in the information provided to the data subject under section 35C(2)(b)(ii) or 35J(2)(b)(iv); and

(b) in relation to which the consent is given;

permitted class of persons (許可類別人士), in relation to a consent by a data subject to an intended provision of personal data, means a class of persons—

(a) that is specified in the information provided to the data subject under section 35J(2)(b)(iii); and

(b) in relation to which the consent is given;

permitted kind of personal data (許可種類個人資料), in relation to a consent by a data subject to an intended use or provision of personal data, means a kind of personal data—

(a) that is specified in the information provided to the data subject under section 35C(2)(b)(i) or 35J(2)(b)(ii); and

(b) in relation to which the consent is given;

response channel (回應途徑) means a channel provided by a data user to a data subject under section 35C(2)(c) or 35J(2)(c).

(2) For the purposes of this Part, a person provides personal data for gain if the person provides personal data in return for money or other property, irrespective of whether—

(a) the return is contingent on any condition; or

(b) the person retains any control over the use of the data.

Section 35B - Application

This Division does not apply in relation to the offering, or advertising of the availability, of—

(a) social services run, subvented or subsidized by the Social Welfare Department;

(b) health care services provided by the Hospital Authority or Department of Health; or

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

Section 35C - Data user to take specified action before using personal data in direct marketing

(1) Subject to section 35D, a data user who intends to use a data subject's personal data in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject—

(i) that the data user intends to so use the personal data; and

(ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use;

(b) provide the data subject with the following information in relation to the intended use—

(i) the kinds of personal data to be used; and

(ii) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and, if in written form, easily readable.

(5) Subject to section 35D, a data user who uses a data subject's personal data in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(7) In any proceedings for an offence under subsection (5), the burden of proving that this section does not apply because of section 35D lies on the data user.

Section 35D - Circumstances under which section 35C does not apply

(1) If, before the commencement date—

(a) a data subject had been explicitly informed by a data user in an easily understandable and, if informed in writing, easily readable manner of the intended use or use of the data subject's personal data in direct marketing in relation to a class of marketing subjects;

(b) the data user had so used any of the data;

(c) the data subject had not required the data user to cease to so use any of the data; and

(d) the data user had not, in relation to the use, contravened any provision of this Ordinance as in force as at the time of the use, then section 35C does not apply in relation to the intended use or use, on or after the commencement date, of the data subject's relevant personal data, as updated from time to time, in direct marketing in relation to the class of marketing subjects.

(2) If—

(a) a data subject's personal data is provided to a data user by a person other than the data subject (***third person***); and

(b) the third person has by notice in writing to the data user—

(i) stated that sections 35J and 35K have been complied with in relation to the provision of data; and

(ii) specified the class of marketing subjects in relation to which the data may be used in direct marketing by the data user, as consented to by the data subject, then section 35C does not apply in relation to the intended use or use by the data user of the data in direct marketing in relation to that class of marketing subjects.

(3) In this section—

commencement date (本部生效日期) means the date on which this Part comes into operation;

relevant personal data (有關個人資料), in relation to a data subject, means any personal data of the data subject over the use of which a data user had control immediately before the commencement date.

Section 35E - Data user must not use personal data in direct marketing without data subject's consent

(1) A data user who has complied with section 35C must not use the data subject's personal data in direct marketing unless—

(a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively;

(b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming—

(i) the date of receipt of the consent;

(ii) the permitted kind of personal data; and

(iii) the permitted class of marketing subjects; and

(c) the use is consistent with the data subject's consent.

(2) For the purposes of subsection (1)(c), the use of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data; and

(b) the marketing subject in relation to which the data is used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a use of personal data either through a response channel or other means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

Section 35F - Data user must notify data subject when using personal data in direct marketing for first time

(1) A data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.

(2) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(3) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(4) In any proceedings for an offence under subsection (3), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

Section 35G - Data subject may require data user to cease to use personal data in direct marketing

(1) A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject—

(a) has received from the data user the information required to be provided in relation to the use of personal data under section 35C(2); or

(b) has earlier given consent to the data user or a third person to the use.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) A data user who contravenes subsection (3) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(6) This section does not affect the operation of section 26.

Section 35H - Prescribed consent for using personal data in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for using any personal data of the data subject in direct marketing, the data user is to be taken to have obtained the consent if the data user has not contravened section 35C, 35E or 35G.

Section 35I - Application

(1) This Division does not apply if a data user provides, otherwise than for gain, personal data of a data subject to another person for use by that other person in offering, or advertising the availability, of—

(a) social services run, subvented or subsidized by the Social Welfare Department;

(b) health care services provided by the Hospital Authority or Department of Health; or

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

(2) This Division does not apply if a data user provides personal data of a data subject to an agent of the data user for use by the agent in carrying out direct marketing on the data user's behalf.

Section 35J - Data user to take specified action before providing personal data

(1) A data user who intends to provide a data subject's personal data to another person for use by that other person in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject in writing—

(i) that the data user intends to so provide the personal data; and

(ii) that the data user may not so provide the data unless the data user has received the data subject's written consent to the intended provision;

(b) provide the data subject with the following written information in relation to the intended provision—

(i) if the data is to be provided for gain, that the data is to be so provided;

(ii) the kinds of personal data to be provided;

(iii) the classes of persons to which the data is to be provided; and

(iv) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended provision in writing.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and easily readable.

(5) A data user who provides personal data of a data subject to another person for use by that other person in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction—

(a) if the data is provided for gain, to a fine of $1000000 and to imprisonment for 5 years; or

(b) if the data is provided otherwise than for gain, to a fine of $500000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

Section 35K - Data user must not provide personal data for use in direct marketing without data subject's consent

(1) A data user who has complied with section 35J must not provide the data subject's personal data to another person for use by that other person in direct marketing unless—

(a) the data user has received the data subject's written consent to the intended provision of personal data, as described in the information provided by the data user under section 35J(2)(b), either generally or selectively;

(b) if the data is provided for gain, the intention to so provide was specified in the information under section 35J(2)(b)(i); and

(c) the provision is consistent with the data subject's consent.

(2) For the purposes of subsection (1)(c), the provision of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data;

(b) the person to whom the data is provided falls within a permitted class of persons; and

(c) the marketing subject in relation to which the data is to be used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a provision of personal data either through a response channel or other written means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction—

(a) if the data user provides the personal data for gain, to a fine of $1000000 and to imprisonment for 5 years; or

(b) if the data user provides the personal data otherwise than for gain, to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

Section 35L - Data subject may require data user to cease to provide personal data for use in direct marketing

(1) A data subject who has been provided with information by a data user under section 35J(2)(b) may, at any time, require the data user—

(a) to cease to provide the data subject's personal data to any other person for use by that other person in direct marketing; and

(b) to notify any person to whom the data has been so provided to cease to use the data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject has earlier given consent to the provision of the personal data.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) If a data user is required to notify a person to cease to use a data subject's personal data in direct marketing under a requirement referred to in subsection (1)(b), the data user must so notify the person in writing.

(5) A person who receives a written notification from a data user under subsection (4) must cease to use the personal data in direct marketing in accordance with the notification.

(6) A data user who contravenes subsection (3) commits an offence and is liable on conviction—

(a) if the contravention involves a provision of personal data of a data subject for gain, to a fine of $1000000 and to imprisonment for 5 years; or

(b) in any other case, to a fine of $500000 and to imprisonment for 3 years.

(7) A person who contravenes subsection (5) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(8) In any proceedings for an offence under subsection (6) or (7), it is a defence for the data user or person charged to prove that the data user or person took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(9) This section does not affect the operation of section 26.

Section 35M - Prescribed consent for providing personal data for use in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for providing any personal data of the data subject to another person for use in direct marketing, the data user is to be taken to have obtained the consent if the data user has not contravened section 35J, 35K or 35L.

Annex 2 - Data Fields in Registration Form and Registration Interface of iES Website

** Mandatory fields*

Item	Description	Registration Form	Registration Interface of iES Website
1.	Are you legally employable in Hong Kong		√*
2.	HKID Card number	√*	
3.	The last four digits of HKID Card number excluding that in the parentheses		√*
4.	Title		√*
5.	English name	√*	√*
6.	Chinese Name	√	√
7.	Year, month and date of birth	√*	√*
8.	Daytime contact telephone number (Home, Mobile/Pager, Other)	√*	√*
9.	Login username		√*
10.	Password		√*
11.	Residential district		√*
12.	Correspondence address	√*	√*
13.	Permanent Resident of HKSAR (Do you hold a HK permanent identity card)	√*	√*
14.	Stay Hong Kong for 7 years or more	√	
15.	Ethnic origin	√	√
16.	Email address	√	√*
17.	Fax number	√	√
18.	Agree to receive information on job vacancies, recruitment activities and employment services	√	√
19.	Agree to receive SMS for recruitment activities	√	√
20.	Mobile number for receiving the above information through SMS	√	√
21.	Agree to let Labour Department put on the Internet and other channels certain information provided in the form	√	√

Item	Description	Registration Form	Registration Interface of iES Website
22.	Present employment status (Do you have a job now)	√	√*
23.	Unemployed period in past 1 year is not less than 1 month	√	
24.	Highest education level	√*	√*
25.	Secondary education public examination result	√	√
26.	Qualification obtained in post-secondary education	√	√
27.	Place of receiving the highest education	√	√
28.	Proof of highest education level	√	√
29.	With completion of "Project Yin Ji"	√	
30.	Other qualifications/training course(s) attended	√	√
31.	With completion of any retraining course	√	
32.	Typing skills	√	√
33.	Computer skills	√	
34.	Accounting skills	√	
35.	Youth Employment and Training Programme	√	
36.	Other clerical skills	√	
37.	Driving licence	√	
38.	Construction Industry Safety card	√	
39.	Intermediate Trade Test for Construction Craftsmen	√	
40.	Trade Test for Construction Craftsmen	√	
41.	Construction/Repairing skills	√	
42.	Security Personnel Permit	√	
43.	Skill Type and Skill		√
44.	Other skills/licences	√	√
45.	Language (Cantonese/ English/ Putonghua/Other)	√	√
46.	Major Work Experience (Position, Industry, Years of experience and average monthly salary)	√	√*

Item	Description	Registration Form	Registration Interface of iES Website
47.	Recent Jobs (Name of company, industry, position, employment period)	√	√
48.	Jobs Preference (Industry, Position, Years of experience and Minimum expected salary)	√	√*
49.	Preferred job nature	√	√
50.	Accept shift duty	√	√
51.	Preferred working hours	√	√
52.	Preferred working district	√	√
53.	Other useful information	√	√

Annex 3 - Mandatory fields to be filled during registration via iES Website

(1) Are you legally employable in Hong Kong;
(2) The last four digits of HKID Card number excluding that in the parentheses;
(3) English Name on HKID Card;
(4) Year, Month and Date of Birth;
(5) Title;
(6) Contact telephone number;
(7) Login name;
(8) Password;
(9) Email address;
(10) Residential District;
(11) Full Address;
(12) Do you hold a HK permanent identity card;
(13) Do you have a job now;
(14) Highest Education Level;
(15) Position (of first job preference);
(16) Industry (of first job preference);
(17) Relevant Experience (of first job preference);
(18) Expected Salary (of first job preference);
(19) Position (of major work experience);
(20) Industry (of major work experience);
(21) Year(s) of Employment (of major work experience); and
(22) Average Monthly Wage (of major work experience).

(Note: Items 15 to 22 have been changed to optional fields since 7 August 2014.)

Annex 4 - Code of Practice on the Identity Card Number and other Personal Identifiers

Extract of the paragraphs on the collection of HKID Card number

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

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

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

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

2.3.3.1 for the advancement of the interest of the holder;

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

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