Annex

A summary of Real Cases:
Collection and handling of personal data during employment cycle

(29 May 2014)

Hong Kong has a labour force of more than 3.8 million people[1]. Given the vast amounts of personal data collected and processed during the recruitment, in-employment and post-employment stages, employers should take steps to put in place an effective data protection programme in meeting their employees' privacy rights and expectations. Strategically, they are encouraged to embrace personal data privacy protection as part of their corporate governance responsibilities.

In recent years, the general public's awareness of privacy protection has risen significantly. To alert data users to respect the privacy rights of data subjects when collecting and using personal data, the Privacy Commissioner for Personal Data (the "**Commissioner**") has published investigation reports in relation to a number of cases which seriously violated the Personal Data (Privacy) Ordinance (the "**Ordinance**"). Regrettably, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") continues to receive employment-related complaints which are highly invasive of privacy. From 2010 to 2013, PCPD received an average of 116 employment-related complaints each year. In the first 4 months of 2014 alone, 53 complaints of such nature have been received. The parties being complained against included listed companies, public bodies, government departments and small and medium enterprises.

Many employers tend to err on the generous side. They collect personal data without giving serious thought to what real purposes the data collected would serve. In fact, the vast majority of mistakes could be avoided had employers given due consideration before collection.

On the other hand, eager job seekers may worry about not being considered for employment and therefore dare not question the privacy intrusive acts of potential employers. Inexperienced young people looking for employment may be ignorant about their privacy rights.

To promote understanding in this regard, the following selected cases have been adapted from actual complaint cases and compliance checks handled by PCPD. They illustrate the common mistakes made by employers during recruitment stage,

[1] Announced in the website of Government Census & Statistics Department.

in-employment stage and post-employment stage in relation to the collection and handling of employees' personal data, to help remind employers and the public of the requirements under the Ordinance.

The Commissioner calls on all employers to take initiative to implement an accountability-based privacy management programme and apply it throughout their organisations using a top-down approach so as to win their employees' trust and enhance their corporate competitive edge.

(1) Recruitment Stage

Premature collection of personal data from job applicants which is not necessary for recruitment purpose

Case 1.1-Collection of job applicants' personal data

A large-sized catering chain recruited short-term shopkeepers and demanded the applicants to provide their date of birth, bank account number and marital status, spouse's name and Hong Kong Identity Card ("**HKID Card**") number, as well as the name and telephone number of an emergency contact person.

The said personal data might be useful in human resources management upon formal establishment of an employer-employee relationship. However, for the sole purpose of identifying suitable candidates, the chain can do so without collecting the said personal data.

Upon PCPD's intervention, the chain ceased to collect the said personal data from job applicants and destroyed the job application forms of unsuccessful job applicants.

Lesson: Employers should not collect "all" personal data from job applicants but only such data that is directly relevant to the identification of suitable candidates in the recruitment exercise. The employer should only collect other personal data of the job applicants according to actual needs of the employment/position upon employment.

Case 1.2-Collection of personal data from job applicants' referees

A law enforcement agency requested job applicants to provide the names of two referees and the referees' HKID Card number in the job application form. The HKID Card number would be used for identity verification during subsequent interview.

With the information provided by the job applicant in the job application form, the agency contacted the referee for an interview. However, in fact, the agency could verify the identity of the referee either by cross checking his details in the application form or making a professional judgement based on the interview. Therefore, it was not necessary for the agency to collect the referee's HKID Card number for verifying the referee's identity.

The agency complied with the enforcement notice issued by the Commissioner to cease collecting the HKID Card number of referees and to destroy the data previously collected.

Lesson: Potential employers should carefully consider before collecting the personal data from persons other than the job applicant whether such personal data is necessary and not excessive in relation to the purpose(s) to be served, and in particular, they should consider whether there are any less privacy-intrusive alternatives to the collection of HKID Card number.

(2) Employment Stage

Employers should carefully consider whether to collect employees' sensitive personal data

Case 2.1-Collection of fingerprint data

To strictly enforce the attendance system and eliminate the malpractice of punching time-cards for one another among its staff members, a furniture company collected fingerprint data of its 400 employees.

The furniture company did not operate in high-security premises. To deter staff from punching time-cards for one another, the furniture company had already installed surveillance cameras to monitor staff members and record their attendance. In the circumstances, for the purpose of recording attendance, the collection of staff members' fingerprint data by the furniture company was unnecessary and excessive. Moreover, since the furniture company had specified that staff members who refused to provide their fingerprint data would be dismissed, the Commissioner had good reason to believe that they were under undue pressure to comply with the request from the employer and dared not raise objection to the collection of fingerprint data.

The furniture company complied with the enforcement notice issued by the Commissioner to use other alternatives for recording attendance and destroy all fingerprint data collected.

Lesson: Given the uniqueness and immutability of fingerprint data, it could be used to accurately identify a particular staff member. But because of its uniqueness and immutability, fingerprint data is sensitive personal data and its misuse can lead to serious personal data privacy risks and consequences. From the perspective of protection of personal data privacy, a data user should as far as practicable resort to other less privacy intrusive alternatives than fingerprint data collection. In the circumstances, employers are advised to carry out prudent assessment to determine whether the collection of such personal data is necessary and in compliance with the requirements under the Ordinance.

Case 2.2- Collection of DNA data

What were believed to be menstrual bloodstains were found in the female toilet of an investment company. Suspecting that the bloodstains had been left by one of its female employees, and to deter any recurrence of such inconsiderate behaviour, the management of the company required all female staff to give blood sample for a DNA test. The test results would be matched against the sample bloodstains found in the toilet with a view to positively identifying the employee concerned.

The investment company complied with the enforcement notice issued by the Commissioner to cease collecting DNA samples from its staff members and destroy those DNA samples or reports that had been collected.

Lesson: The Commissioner takes the view that it is highly invasive of privacy to identify an individual by examining unique DNA data. Thus, the collection and use of DNA data is only justifiable in serious circumstances e.g. a criminal investigation. The collection of DNA data by the company, solely for the purpose of ensuring hygienic conditions in the female toilets, is neither necessary or reasonable. Employers should consider using other proportionate and less privacy intrusive alternatives to attain the purpose.

Employers should not disclose unrelated personal data of employees to third parties

Case 2.3-Disclosure of employee's medical appointment information

Whenever a staff of a public hospital left office for medical appointment during office hours, his supervisor would record his medical appointment date, time, name of the hospital or clinic and purpose of medical consultation on a form. He would then post the form on the notice board in the department office which was accessible by all staff of the office. The purpose was to let the staff member's colleagues cover his duties in his absence. In this case, the hospital recorded in the form provided psychiatric treatment only.

The disclosure of the name of the hospital designated for psychiatric treatment was, in this case, not necessary to attain the said staff deployment purpose. Moreover, it would indirectly lead to the disclosure of the staff member's illness to third parties causing serious intrusion to his privacy.

Upon PCPD's intervention, the public hospital had revised the form and deleted the column for inserting the name of the hospital or clinic that the staff attended.

Lesson: In case an employer needs to disclose an employee's personal data to third parties, it should only disclose necessary information on a need-to-know basis to attain the relevant purpose.

(3) Former Employees

Case 3.1-Public announcement about former employee containing excessive personal data

A salesperson of a fashion shop was dismissed due to misconduct. He was required to sign an exit notice specifying his name and reason for leaving the shop. The shop subsequently posted the notice in the shop without the salesperson's consent.

Eventually the shop removed the exit notice and undertook to PCPD not to disclose the reason for departure of former employees in the public announcement in future.

Lesson: If an employer finds it necessary to announce publicly that a former employee has left employment, generally, the individual's full name, former job title and name of the organisation would be sufficient for the purpose. Stating the reason for leaving the job is considered excessive disclosure.

Case 3.2-Employers should obtain prescribed consent from former employees before giving a reference on them to a third party

A former employee of a listed company applied for a job with another company. The potential employer then requested the listed company to provide a job reference about that former employee. Without obtaining the former employee's consent, the listed company provided a job reference to the potential employer, believing that the former employee had authorised the potential employer to obtain such information.

The listed company subsequently undertook to PCPD in writing that it would obtain prescribed consent from former employees before giving a reference on them to a third party.

Lesson: Employers should ensure that prescribed consent from former employees have been obtained before giving a reference on them to a third party.

Case 3.3-Employers should comply with data access requests made by former employees for a copy of personal data

A former employee of a logistic company made a data access request to the company requesting for a copy of his employment contract. The company did not respond to the data access request before expiry of the period of 40 days within which compliance with the request had to be made legally. The company explained that records in relation to former employees were confidential and stored in a warehouse, and such records could only be accessed by management staff.

Upon PCPD's intervention, the company acceded to the former employee's request and provided him with the data requested.

Lesson: Employers are obliged to comply with data access requests made by employees/former employees for a copy of their personal data within 40 days after receiving the request under the Ordinance. An employer which is unable to comply with a data access request within 40 days shall by notice in writing inform the requestor that it is so unable and of the reasons why it is so unable before the expiration of the 40-day period, and comply with the request as soon as practicable.