
2H. The Personal Data (Privacy) Ordinance (PD(P)O)

Personal data means any data “relating directly or indirectly to a living individual, from which it is possible and practical to ascertain the identity of the individual from the said data, in a form in which access to or processing of the data is practicable”. Obvious examples of personal data are an individual’s identity card number and fingerprints, through which they can be identified.

The Ordinance places a statutory duty on data users to comply with the requirements of the six Data Protection Principles contained in Schedule 1 to the Ordinance. The Ordinance provides that a data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under the Ordinance. It also gives data subjects certain rights, including the right to be informed of whether any data user holds their personal data; to be supplied with a copy of such data; and to request correction of any data they consider to be inaccurate.

Generally speaking, the Ordinance governs the ways of collecting and using personal data, and prevents any abuse of data that is considered as intruding on an individual’s privacy.

2H.1 Coverage of the Ordinance

The Ordinance applies to any person who collects, holds, processes and uses personal data within the private and public sectors as well as government departments.

2H.2 Employers’ responsibilities

Data users who handle personal data in performing human resource management functions and activities need to observe the PD(P)O when handling issues concerning collection, holding, accuracy, use and security, and data subject access and correction in relation to the personal data of prospective, current and former employees. Employers are liable to protect the data of their prospective, current and former employees.

The protection covers the scope of using, collecting, maintaining and sharing of the collected data. All practicable steps should be taken to ensure the proper handling on the personal data including the implementation of adequate security measures and that access should be authorized.

Sections 53 and 55 of the Ordinance state that personal data used for following employment-related purposes are exempt from the provisions of data access requests (data protection principle 6):

- ✦ personal data relating to staff planning;
- ✦ personal data generated by certain evaluative processes, including a recruitment or promotion exercise, prior to a decision being taken and where an appeal can be made against such a decision;
- ✦ a personal reference for an appointment up to the time when the position is filled.

Refer to Table 2 below for the Do's and Don'ts under Personal Data (Privacy) Ordinance.

Table 2:

	Do's	Don'ts
Recruitment	Recruitment advertisements that directly ask job applicants to provide personal data should include a statement informing applicants about the purposes. And contact information of the employer should be stated in the advertisement.	An employer should not solicit personal data from job applicants in a recruitment advertisement that doesn't provide identification of either the employer or the employment agency acting on its behalf.
	To conceal its identity, an employer may, in recruitment advertisements, upon request provide job applicants with application forms that bear the employer's identity. Personal data collected from job applicants should be: <ul style="list-style-type: none"> - adequate - relevant to the purpose of identifying suitable candidates for the job 	An employer should not collect a copy of the identity card of a job applicant during the recruitment process unless and until the individual has accepted an offer of employment.
	Personal data concerning the health condition of a selected candidate may be collected (eg. by pre-employment medical examination) if the data directly relate to the inherent requirements of the job (eg. bank guards).	
	Personal data of unsuccessful applicants may be retained for two years from the date of rejecting applicants and should then be destroyed.	
Current Employment	On appointment, employer may collect additional personal data from employee and their family members: <ul style="list-style-type: none"> - for the purpose of employment, or - to fulfill lawful requirements 	Information compiled about an employee in the process of disciplinary proceedings, performance appraisal or promotion planning should not be disclosed to a third party unless such party has legitimate reasons for gaining access to those data.
	Information compiled about an employee in the process of disciplinary proceedings, performance appraisal or promotion planning should only be used for purposes directly related to the process concerned.	When employment-related data are transferred or disclosed to a third party, an employer should not disclose data in excess of that necessary for the purpose of use by the third party.
	Employer should provide the employee with a Personal Information Collection Statement ("PICS") before collecting personal data from them.	Employer should not disclose employment-related data of employees to a third party without first obtaining the employees' consent unless the disclosure is for the purposes directly related to the employment, or such disclosure is required by law/statutory authorities.

	Do's	Don'ts
Current Employment	An employer who engages a third party organisation to handle its employment-related functions (eg. administration of medical benefits) should implement appropriate measures to ensure that the third party protects the employment-related data against unauthorised or accidental access or disclosure.	
Former Employment	Personal data of a former employee may be retained for a period of up to seven years from the date the former employee ceases employment. The data may be retained for a longer period if there is contractual or legal justification.	In any public announcement notice regarding a former employee having left employment, do not disclose the identity card number of the employee concerned in the notice.
	Upon the departure of an employee, ensure that only relevant information of the former employee is retained to satisfy its retention requirements.	Should not provide a reference concerning a former employee to a 3 rd party without first obtaining the employee's consent for this unless the employer is satisfied that the 3 rd party requesting the reference has obtained the prior consent of the employee concerned.

Refer to the following publications issued by the Privacy Commissioner for Personal Data for more practical guidance to data users on how to properly handle personal data that relate to each phase of the employment process. These publications cover issues concerning collecting, holding, correcting, use and security and data subject access in relation to the personal data of prospective, current and former employees; available from the Office of the Privacy Commissioner for Personal Data, Hong Kong website <http://www.pcpd.org.hk>> Publications & videos > Code of Practice/Guideline & Explanatory Booklet:

- "Code of Practice on Human Resource Management"
http://www.pcpd.org.hk/english/ordinance/code_hrdesp.html
- "Privacy Guidelines: Monitoring and Personal Data Privacy at Work"
http://www.pcpd.org.hk/english/publications/files/monguide_e.pdf
- "Compliance Guide for Employers and HRM Practitioners"
http://www.pcpd.org.hk/english/ordinance/code_hrm.html
- "Fact Sheet -- Frequently Asked Questions About Recruitment Advertisements"
http://www.pcpd.org.hk/english/ordinance/code_faq.html
- "Code of Practice on the Identity Card Number and other Personal Identifiers"
http://www.pcpd.org.hk/english/ordinance/code_id.html
- "Code of Practice on the Identity Card Number and other Personal Identifiers – A Compliance Guide for Data Users"
http://www.pcpd.org.hk/english/ordinance/code_data_1.html