PCPD
H K
PCPD.org.hk
Information Leaflet
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Human Resource Management: Common Questions

This Fact Sheet is designed to help human resource practitioners comply with the requirements set out in the Personal Data (Privacy) Ordinance (the **Ordinance**). It includes frequently asked questions about the application of the Ordinance to human resource management practices.

The Ordinance is centred around six Data Protection Principles (**DPPs**) that govern the handling of personal data, encompassing the collection, accuracy, retention, use, security, policies and practices, access and correction of personal data.

Data Protection Principle 1 (DPP 1): Purpose and Manner of Collection of Personal Data

Q1: Can employers inquire about a job applicant's criminal record?

A: DPP 1(1) provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. Further, it requires that the collection of the data is necessary for or directly related to that purpose, and, in relation to that purpose, the data is adequate but not excessive. No hard and fast rules can be laid down as to which data is necessary for human resource management. This will depend on the specifics of the individual case, including the role and nature of the job involved, its function and potential tasks.

As a general rule, under section 2(1) of the Rehabilitation of Offenders Ordinance (Cap. 297) (**ROO**), if an individual has been convicted for the first time in Hong Kong of an offence and he was not sentenced to imprisonment exceeding three months or to a fine exceeding HKD$10,000 for such conviction, and a period of three years has elapsed without that individual being convicted of any other offence in Hong Kong, the individual's first conviction will become spent after the three years' period and he will be deemed to have no conviction record.

Employers should also note that by virtue of the ROO, a job applicant does not have to disclose any spent conviction records to others, unless any of the exceptions under sections 3 and 4 of the ROO apply, for example, if the applicant is applying for admission as a barrister, solicitor or an accountant, for a job in the disciplined services or for appointment as a senior civil servant or judicial officer.

However, for roles that require frequent contact with children or mentally incapacitated persons (**MIPs**), employers may request eligible applicants to apply to the police, on a voluntary basis, for a check on their criminal conviction record (if any) in respect of any specified sexual offences under the Sexual Conviction Record Check Scheme[1] to safeguard the well-being of children and MIPs.

Furthermore, it is important for employers to inform a job applicant, 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, as stipulated in DPP1(3).

Q2: A company's job application form includes questions about the occupations of the applicant's spouse or children, the sole purpose of which is to ascertain whether any relative of the applicant works for its competitors. Is this acceptable?

A: The key question here is whether the data collected is necessary for the specific purpose of determining whether an applicant's relative is employed by a competitor. To serve this purpose, a prospective employer may only need to ask the applicant whether he is related to anyone who works in the same or a similar field. If the answer is in the affirmative, then further inquiries can be made to assess whether this creates potential concerns for the prospective employer. However, if the applicant has no relative who works for a competitor, the employer does not need to know about the actual occupations of the relative(s) and should not collect this data.

1 Please refer to the Sexual Conviction Record Check Scheme Protocol (May 2023) for details at https://www.police.gov.hk/info/doc/scrc/SCRC_Protocol_en.pdf

Q3: Is a company's practice of requiring a prospective employee to submit to a pre-employment health check an infringement of a prospective employee's personal data privacy?

A: It is common for employers to request a prospective employee to undergo a pre-employment medical check. As long as the individual in question consents to undergo the medical check and to release the results to the employer, this practice does not contravene the provisions of the Ordinance.

However, employers must be careful not to collect excessive health data during the pre-employment medical check. For example, it would be unacceptable generally to require the individual to submit to genetic testing. An employer should only collect information regarding the candidate's health condition that is necessary, adequate but not excessive to support the medical practitioner's opinion about his fitness for the job. In this regard, employers may find it useful to refer to the codes of practice on employment under the various anti-discrimination ordinances issued by the Equal Opportunities Commission.

Q4: Is an employer permitted to ask employees to install a mobile app on their phones to track their location during work hours?

A: The Ordinance is a principle-based and technology-neutral legislation, it does not prohibit employers from monitoring employees to meet operational needs (such as ensuring employees' safety or checking whether employees have arrived at specified work locations on time). However, if an employer collects the personal data (e.g., name, live location, attendance record) of employees in the process, the employer must ensure the act is in compliance with the requirements under the Ordinance.

For example, it may not be fair to use electronic surveillance on employees at work if there are less privacy-intrusive ways to monitor their whereabouts. As a matter of good practice, employees should be informed in writing if specific techniques are to be deployed to monitor their activities.

Employers can refer to "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" and "Physical Tracking and Monitoring Through Electronic Devices" published by the Privacy Commissioner for Personal Data (the **Commissioner**) to learn more about the points to note when conducting employee monitoring and the personal data privacy risks associated with tracking and monitoring via electronic devices.

Data Protection Principle 2 (DPP 2): Accuracy and Duration of Retention of Personal Data

Q5: What should a company do if an unsuccessful job applicant asks to have his personal résumé returned?

A: If a company still requires the personal information for the purposes for which the data was to be used at the time of the collection of the data (or a directly related purpose), or a new purpose for which the applicant has given express consent after its collection, then the company may retain and use the personal data. However, once the recruitment objectives have been fulfilled, and unless the unsuccessful applicant consents to the company's retention of his personal résumé for future recruitment exercises, the company should take all practicable steps to erase the data of the unsuccessful applicant. That said, the Ordinance does not confer any right for a data subject to request the return of personal data after its use. If his personal data is suspected to have been retained longer than necessary, the job applicant may enquire with the company concerned or file a complaint with the Commissioner.

Q6: If an employer needs to retain the personal data of a former employee, is the employer required to update the data regularly or keep it as is?

A: DPP 2(1) requires a data user to take all reasonably practicable steps to ensure that 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. Whether or not the employer needs to update the data depends on the purpose for which the data is kept. For example, an employer may need to update the records of a former employee to administer pension funds and make monthly payments. Where the personal data of a former employee is retained only for record-keeping purposes or for future job references, the employer is under no duty to update records that are meant to be static after the cessation of the employment relationship.

Q7: An employer may need to provide the personal data of employees to a third-party service provider to handle some administrative tasks. Is this a contravention of the Ordinance if outdated personal data of employees is provided to the service provider?

A: DPP 2(1) requires an employer to take all practicable steps to ensure that the personal data of the employees is accurate in the circumstances having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used. Therefore, an employer has to make sure that the personal data of the employees provided to the service provider is accurate.

An employer should formulate appropriate policies and procedures to update employees' personal data. For example, when there are changes to the contact information of employees, on top of updating the internal personnel record, an employer should also update the record provided to the service provider timely to ensure that the data is accurate.

Q8: For how long should an employer keep the personal data of former employees and unsuccessful job applicants?

A: DPP 2(2) requires all practicable steps to be taken to ensure that personal data is not kept longer than is necessary to fulfil the purpose (including any directly related purpose) for which the data is or is to be used. In addition, section 26 of the Ordinance also requires a data user to take all practicable steps to erase personal data no longer required for use, unless doing so is prohibited under the law or it is in the public interest (including historical interest) for the data not to be erased. In general, an employer should not retain the personal data of a former employee for more than seven years.

However, some exceptions may justify a longer period of retention, such as the administration of remaining duties to former employees in relation to pension, superannuation, or mandatory provident fund schemes; or the retention of evidence in relation to legal action brought under the Employees' Compensation Ordinance.

When a job application is unsuccessful, the applicant's personal data should not be retained for more than two years from the date of rejection, bearing in mind possible discrimination claims or complaints that may be lodged by an aggrieved applicant. The retention period may exceed two years if there is a reason that obligates the employer to do so, or if the applicant has given the prescribed consent (i.e. express consent given voluntarily) for the data to be retained beyond this period.

Q9: Must an employer obtain consent from the relevant employee before giving an employment reference to another employer?

A: Yes, an employer should obtain the prescribed consent (i.e. express consent given voluntarily) from an employee or former employee before giving an employment reference. This consent should preferably be given in writing. The reason for this is that the disclosure of an employee's or former employee's employment records (including performance assessment) to another party constitutes a change in the purpose for which the data is used at the time of collection and no longer directly relates to the original employment purpose.

Q10: Should the personnel department seek employees' consent for internal auditors to access staff files for auditing purposes?

A: DPP 3(1) provides that unless with the data subject's prescribed consent, personal data may only be used for a purpose for which the data is to be used at the time of collection, or a directly related purpose. If an organisation wishes to use personal data for a new purpose, it must first obtain the individual's voluntary express consent. Generally, personal data in staff files collected for personnel management purposes may be used for internal auditing without the consent of the employees, because the auditing activity is directly related to the personnel management function. To avoid disputes, an employer could include this purpose in the "Personal Information Collection Statement" communicated to employees on or before the collection of their personal data.

Q11: Can employers still use their employees' personal data for business purposes after they have left employment?

A: According to DPP 3(1), unless the employees have given their express consent voluntarily, their personal data may only be used by their employers for the purpose for which the data is to be used at the time of collection, or a directly related purpose. Generally, employees' personal data collected by employers is mostly intended for use during the employment period (exceptions may include personal data collected for handling matters in relation to employees' pension fund, superannuation or mandatory provident fund scheme). Therefore, unless with the prescribed consent of an employee, an employer should not use the employee's personal data for other purposes after he has left the employment.

Q12: If a company retains personal data in a computerised human resource management system, and supervisors and heads of departments are able to access this computer system to carry out their personnel management functions, is this a contravention of the Ordinance?

A: As long as supervisors and heads of departments use the employees' personal data only for the original purposes for which it was collected (e.g., carrying out personnel management functions), then there is no contravention of DPP 3(1). However, if a company discloses more personal data than necessary to supervisors for the latter's personnel management functions, then this will be a contravention of DPP 3(1). Because an employee's personal data may be collected for many purposes, and supervisors and heads of departments have roles to perform, the employer should ensure that the personal data contained in the human resource management system is accessed on a "need-to-know" basis. An employer is therefore advised to assign clear access rights to its staff members and restrict access to personal data through appropriate means such as password control, encryption, and the retention of access logs. Human resource staff members, supervisors, and heads of departments should be trained to ensure their compliance with the privacy policies and practices of the company.

Q13: The overseas head office regularly accesses personnel information related to salaries, bonuses, ex-gratia payments, and similar information pertaining to the staff members employed by its Hong Kong branch. Would such practice constitute a contravention of the Ordinance?

A: The Hong Kong branch has to ascertain the purpose of collection of such personal data by its overseas head office. If it is collecting the personal data for purposes directly related to the purpose for which the data was to be used at the time of the collection of the data (e.g., to properly discharge human resource administration functions), then the Hong Kong branch may provide such personal data to its overseas head office. However, the Hong Kong branch should, through the "Personal Information Collection Statement", clearly inform its employees that the overseas head office is included among the classes of transferees of their data.

Q14: Can an employer disclose the employee's sick leave applications to his direct supervisor and the general manager?

A: The employer should ensure compliance with DPP 3(1) when the employee's personal data is disclosed. Generally, if the relevant personnel (e.g., the company's management and the employee's direct supervisor) needs to know the employee's health conditions to make relevant work arrangements, then there is no contravention of DPP 3(1). Nevertheless, an employer should only allow authorised personnel to access and handle this information on a "need-to-know" basis.

Q15: When an employer makes suitable work arrangements based on the health conditions of an employee after receiving his medical certificate(s), can the employer disclose the employee's health conditions to other affected employees?

A: If an employee submits medical certificate(s) to an employer showing that he is unfit or unable to perform certain duties due to his health conditions so that the employer can make suitable work arrangements, under DPP 3(1), the employer can only use (including disclose) the personal data contained in the medical certificate(s) for the purpose of making arrangements based on the employee's health conditions, or a directly related purpose. Employers should note that generally, other affected employees do not need to know the health conditions of the relevant employee when suitable work arrangements are to be made.

Data Protection Principle 4 (DPP 4): Security of Personal Data

Q16: When an employer provides another company with personal references for former employees, must the employer mark the envelope "confidential"?

A: The level of security adopted in relation to personal data depends on a range of factors set out in DPP 4(1); these include the kind of data in question and the harm that could result in cases of unauthorised or accidental access, processing, erasure, loss, or use of the data. The greater the sensitivity of the information in the personal reference, the more stringent the security measures that need to be adopted. Generally, it would be desirable to mark the envelope to indicate that only staff members dealing with personnel matters in the recipient organisation should open it; marking the envelope "confidential" would usually be appropriate and good practice.

Data Protection Principle 5 (DPP 5): Information to be Generally Available

Q17: Do employees have the right to know the kind of personal data about them held by the company, along with the main purposes for which such personal data is used?

A: Yes. DPP 5 requires a data user to take all practicable steps to ensure that anyone can be informed of the kind of personal data held by a data user and the main purposes for which personal data held by a data user is or is to be used. Therefore, an employee has the right to be informed of the kind of personal data held by the employer, including the main purposes for which personal data held by a data user is or is to be used.

Data Protection Principle 6 (DPP 6): Access to Personal Data

Q18: Does an employee have the right to obtain a copy of his appraisal reports?

A: Under DPP 6, a data subject has the right to ascertain whether a data user holds any personal data about him, and he has the right to request access to such data. As appraisal reports contain an employee's personal data, the employee has the right to obtain a copy of them (excluding the parts not being his personal data) to access his personal data therein. Unless exempted by the Ordinance, a data user has to comply with the data access request and to supply the data subject with the requested data within 40 days after receiving the data access request.

Notwithstanding applicable exemptions are available, they are optional ones. The burden of proof is on the data user if he places reliance on them. It is up to the employer to choose whether to invoke an exemption or to provide the employee with access to the personal data, as requested.

Q19: Does an employer first need to obtain consent from the appraiser before disclosing appraisal information to an appraisee?

A: No. Comments about an appraisee constitute his personal data which he is entitled to access albeit they were written by the appraiser. However, an appraisal report typically contains the appraiser's name and job title. Unless the employer is certain that the appraiser has consented to the disclosure of this data to the appraisee making the request, then in complying the data access request made by the appraisee, the employer should redact the appraiser's personal data from the copy of the appraisal report provided to the appraisee.

Q20: A former employee requests a copy of employment certificate or reference letter from its former employer by submitting a Data Access Request Form (OPS003). If such documents have never been issued to the former employee, is the employer required to issue such documents so as to comply with the data access request?

A: According to section 18 of the Ordinance, an individual or a relevant person on behalf of an individual may make a request to a data user (e.g., a former employer) to be informed whether it holds personal data of which the individual is the data subject, and, if so, to be supplied with a copy of the data. However, if the data user has never held the data requested by the data subject, it is not required to compile any personal data that it does not hold in order to comply with the data access request. Thus, if an employer has never issued an employment certificate or reference letter to the former employee, it is not required to generate these documents for complying with the data access request. Instead, the employer is required to inform the requestor in writing within 40 days after receiving the request that it does not hold the requested data.

Q21: Who is the "data user"? Is it the employer, department head, or the staff of the human resource department?

A: As defined under the Ordinance, a data user is a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data. In the private sector, it is generally the company, as a legal person, that is taken to be the data user. The company is generally to be held accountable under the Ordinance for the acts or omissions committed by its employees and agents.

Q22: Who is liable for a contravention of the Ordinance in relation to employment-related personal data: the employer or the human resource manager?

A: The employer is generally taken to be the data user who has control over the collection, holding, processing, or use of the personal data. The employer must comply with the requirements of the Ordinance, and in the event of a breach of any such requirement, the Commissioner may issue an enforcement notice against the employer, requiring it to take necessary actions to remedy and, if appropriate, prevent any recurrence of the contravention.

PCPD website
pcpd.org.hk

Download
this publication

Tel : **2827 2827**
Fax : **2877 7026**
Address : **Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication are for general reference only. This publication is not an exhaustive guide to applying the Personal Data (Privacy) Ordinance (the Ordinance). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the Commissioner) makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided do not affect the functions and powers conferred upon the Commissioner under the Ordinance.

First published in May 1997
April 2016 (First Revision)
December 2023 (Second Revision)