Privacy Commissioner's Office Published a Report Relating to Three Data Security Incidents

Published under Section 8 of the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) earlier intervened in three incidents involving the security of personal data. All of the organisations complained against in the cases were the employers of the complainants. Owing to various deficiencies of the organisations in the handling of employment data that resulted in the improper disclosure or unauthorised or accidental access, processing or use of personal data, the organisations in question were found to have contravened the relevant requirements of the Personal Data (Privacy) Ordinance (PDPO).

Summaries of the Three Data Security Incidents (see Annex 1 for details)

(1) The complainant worked for a security service company. The complainant's supervisor sent a notice of termination of employment containing the complainant's HKID card number to a work-related chat group in an instant messaging application. This resulted in the disclosure of the complainant's personal data to other staff members in the group.

(2) The head of the security department of a hotel stored annual performance appraisal forms of departmental staff members in a desk drawer. As the desk was shared among staff members of the department and the department head did not lock the drawer in accordance with the hotel's guidelines, the complainant (an employee of the hotel's security department at the material time) inadvertently read the appraisal forms that contained the personal data of all the departmental staff members stored in the drawer while searching for other documents.

(3) An administrative staff member of a social welfare organisation was responsible for scanning a dismissal document relating to the complainant. During the process, the staff member mistakenly saved the scanned copy in the department's shared folder. As a result, the complainant's personal data contained in the document was accessible to other staff members of the department.

Results of Follow-up actions

Data Protection Principle (DPP) 3(1) of Schedule 1 to the PDPO stipulates that personal data shall not, without the prescribed consent of the data subject (namely, express consent voluntarily given by the data subject), be used (including disclosed or transferred) for a new purpose that is not or is unrelated to the original purpose when collecting the data. Furthermore, DPP 4(1) of Schedule 1 to the PDPO stipulates that all practicable steps shall be taken by a data user to ensure that any personal data held by the data user should be protected against unauthorised or accidental access, processing, erasure, loss or use.

In the above cases, having considered the circumstances of the individual incidents and the information obtained, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the organisations concerned had contravened DPP 3(1) of the PDPO concerning the use (including disclosure) of personal data, or DPP 4(1) of the PDPO concerning the security of personal data.

The Privacy Commissioner's Decisions

The Privacy Commissioner has respectively served Enforcement Notice or warning letter on the three organisations, directing them to remedy and prevent recurrence of their respective contraventions.

Recommendations

Through this report, the Privacy Commissioner would like to remind employers to regard the protection of employees' personal data privacy as an integral part of the organisations' data governance. This would help to demonstrate the organisations' commitment to safeguarding employees' personal data and ensuring compliance with the requirements of the PDPO, thereby creating a win-win situation for both employers and employees.

Employers' protection of employees' personal data privacy is closely related to daily lives and forms part of employers' statutory responsibilities. The PCPD encourages organisations to work hand in hand with employees to create a working environment that safeguards personal data privacy and data security. The PCPD offers the following five recommendations to employers:

1. **Introduce a Personal Data Privacy Management System and formulate clear data security policies that embed personal data privacy**

protection into the core values of the organisations, so as to promote a top-down culture that prioritises personal data privacy and data security;

2. **Develop robust workflows and procedures**, and regularly remind staff of the key points of work procedures and policies to ensure compliance;

3. **Implement ongoing monitoring mechanism** to ensure consistent enforcement of personal data security policies by employees through technical checks or regular inspections, and conduct periodic reviews to optimise oversight procedures and maintain effective monitoring;

4. **Provide training to employees**: Provide targeted training to employees (particularly the employees responsible for handling sensitive data) to enhance their awareness and capability in safeguarding privacy;

5. **Actively engage with employees and work with them to examine the workflow involving the handling of personal data** in order to understand their concerns and challenges, so as to effectively develop policies, procedures and training programmes tailored to the daily operations and needs.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
3 February 2026

Annex 1

Personal Data Security Incidents of Three Organisations
Case Summaries

Case (1) - A security service company sent a notice of termination of employment of an individual employee to a chat group of an instant messaging application

The complainant worked for a security service company and was assigned to work at a leisure facility. When the complainant's supervisor issued a notice of termination of employment to the complainant, he sent the notice to an instant messaging chat group ("the Group") set up for work purposes. This resulted in the disclosure of the complainant's personal data contained in the notice, including her name, HKID card number and information relating to the complainant's dismissal to other staff members of the Group.

The company explained that considering the need for members of the Group to know that the complainant should no longer enter staff-only area of the relevant venue or have access to internal information of the company upon departure, the complainant's supervisor sent the notice to the Group. The supervisor acted hastily and without due consideration, and failed to redact personal data that should not have been disclosed to third parties.

The PCPD commenced an investigation into the case. After investigation, **the Privacy Commissioner considered that disclosing the HKID card number and dismissal information of the complainant contained in the notice to the other members of the Group was beyond the original purpose of use of the data (namely, to handle the complainant's employment matters)**. As such, the disclosure of personal data was not for the original purpose or a directly related purpose and amounted to using the data for a new purpose. Given that the company did not obtain the complainant's prescribed consent for such use, **the company had contravened the requirements of DPP 3(1) as regards the use of personal data in the present case**.

The Privacy Commissioner has served an Enforcement Notice on the company, directing it to request members of the Group to delete the relevant notice from the Group and all other copies of the notice (if any), formulate policy for handling personal data related to employment contracts and incorporate the same into staff training.

Case (2) - The security department of a hotel failed to lock the work desk drawer where staff annual performance appraisal forms were stored

While working in the security department of a hotel, the complainant inadvertently discovered annual performance appraisal forms of all departmental staff in an unlocked drawer when searching for other documents at the desk of the department head in the control room. The appraisal forms contained the personal data of the departmental staff including their names, dates of joining and performance appraisals.

According to the hotel, the desk was primarily used by the head of the security department. However, when the department head was on leave, the security staff on duty could use the desk to handle paperwork. The hotel explained that the incident happened because the department head had forgotten to lock the desk drawer after placing the relevant appraisal forms inside. Upon learning the incident, the hotel had taken disciplinary actions against the head of the security department for failing to properly safeguard confidential documents in accordance with the relevant rules and guidelines, and had also imposed requirements on the safekeeping of such documents by the security department head.

The PCPD commenced an investigation into the case. As a result of the investigation, **the Privacy Commissioner found that the hotel had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) of the PDPO concerning the security of personal data**.

The Privacy Commissioner has served an Enforcement Notice on the hotel, directing the hotel to implement monitoring measures to ensure compliance with and execution of the policies and guidelines on personal data privacy protection by staff members and to formulate a concrete training plan to strengthen staff awareness of personal data privacy protection.

Case (3) - A social welfare organisation mistakenly saved a scanned copy of a document relating to staff dismissal in a shared folder

The complainant was formerly employed by a social welfare organisation. When processing the written record of the complainant's dismissal, an officer of the organisation scanned the document but mistakenly saved the scanned copy in a departmental shared folder in the organisation's internal information network. As the document was not encrypted with a password, the relevant document which contained the complainant's name, date of joining, salary, performance appraisal and reasons for dismissal was accessible by all staff members within the department.

The organisation admitted that the incident stemmed from human error of an administrative officer, who mistakenly selected to store the document in the shared folder during scanning. The document was deleted immediately upon discovery of the incident. The organisation stated that the document remained in the shared folder for about half an hour and there was no record of other staff accessing it.

Upon the PCPD's intervention, the organisation had attended to the matter immediately and debriefed the relevant administrative officer. The department in question disabled the function of saving scanned documents in the shared folder. The organisation also reminded all staff to handle documents containing sensitive personal data with care during departmental staff meetings and arranged regular training sessions on the protection of personal data privacy.

Having considered the circumstances of the case and the information provided by the organisation, **the Privacy Commissioner found that the organisation had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) of the PDPO concerning the security of personal data**. As a result**, the Privacy Commissioner issued a warning letter to the organisation**, requesting it to duly implement measures for protecting personal data privacy and monitor the compliance of which by its employees.