# Privacy Commissioner's Office Published a Report Relating to Eight Personal 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 handled eight incidents relating to the disclosure and security of personal data involving organisations in various sectors and completed the follow-up actions. Owing to the deficiencies of the organisations in different aspects which 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 the Personal Data (Privacy) Ordinance (PDPO).

## Summaries of the eight data security incidents (see Annex 1 for details)

1. After performing an ultrasound scan on the complainant, the doctor of a medical diagnostic centre did not log out of the system before leaving the examination room. As a result, the complainant who remained in the examination room was able to read the information of other patients displayed on the screen of the examination equipment, including the English names, the full Hong Kong Identity Card (HKID card) numbers and brief medical histories of the patients concerned.

2. A tour guide distributed group electronic flight tickets to tour members that contained the English names and dates of birth of over 30 individuals including the tour guide and all the tour members. As a result, the personal data of each tour member was made known to all tour members through the group electronic tickets.

3. When handling a complaint about parking matter, a security guard disclosed the complainant's phone number to another carpark tenant to facilitate direct handling of the parking complaint between the two parties. This constituted improper disclosure of the complainant's phone number to the other tenant.

4. A medical institution failed to properly apply the appropriate setting in the "View Summary of Responses" function during the collection of citizens' personal data via an online registration form. As a result, the personal data of over 100

registrants, including their names in Chinese and English, phone numbers, email addresses and dates of birth, were accessible by other registrants using the "View Summary of Response" function.

5. A government department posted a letter to the complainant. As the relevant staff member did not follow the established procedures in folding letters, the subject line of the letter and the case number comprising the complainant's HKID card number were visible through the envelope window.

6. An insurance company printed documents on recycled papers and sent the documents to other companies. However, the papers used were obsolete resumes and HKID card copies, and this resulted in the personal data contained therein being wrongfully sent to other companies.

7. A retailer sent a promotional email to its members, but the responsible staff member mistakenly entered the email addresses of all members in the recipient field, resulting in the recipients being able to view the email addresses of over 1,000 members in the email.

8. Owing to a wrong script applied to the membership accounts system of an airline company, the complainant was erroneously directed to another customer's account when he logged into his membership account. This enabled him to access the account information of the other customer.

**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, namely, any purpose other than the purpose for which the data was to be used at the time of collection of the data, or a purpose directly related to that purpose.

DPP 4(1) of Schedule 1 to the PDPO stipulates that all practicable steps shall be taken to ensure that any personal data held by a 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 had contravened DPP3(1) of the

PDPO concerning the use (including disclosure) of personal data and DPP4(1) of the PDPO concerning the security of personal data.

## The Privacy Commissioner's Decisions

The Privacy Commissioner served enforcement notices, warning letters or advisory letters to the respective organisations, directing them to take measures to remedy the contraventions and prevent recurrence of similar incidents.

## Recommendations

Data security pitfalls may lie in any single procedure of work. To assist organisations in addressing the challenges relating to personal data security, the Privacy Commissioner would like to make the following six recommendations to organisations of all sectors through this Report.

1. **Incorporate the protection of personal data privacy into the core values of the organisation**, appoint appropriate managerial personnel to be responsible for data security, and publicly demonstrate the management's commitment to protecting personal data privacy while enabling staff members to embrace the importance of personal data privacy;

2. **Enhance the awareness and capabilities of employees to protect privacy through training**, provide targeted training for employees according to their job functions, with a focus on explaining common risks and conducting scenario drills;

3. **Develop clear and easy-to-understand work guidelines**, design checklists or flowcharts to clearly communicate operational guidelines to employees based on the job natures of different positions, and reiterate relevant key points through emails, internal platforms or meetings on a regular basis;

4. **Adopt technical security measures**, such as using an email system that is encrypted by default or enabling auto-filling of correct email recipients to reduce the risk of errors;

5. **Regularly monitor, assess and improve compliance with data security policy**, including arranging supervisors to conduct regular or surprise inspections of frontline work, ensuring thorough implementation of the personal data security policy through monitoring and regularly collecting feedback from staff for continuous improvement of the policy; and

6. **Develop a comprehensive data breach response plan** to help the organisation swiftly respond to and effectively manage data breach incidents.

**Ada CHUNG Lai-ling**
**Privacy Commissioner for Personal Data**
**7 July 2025**

**Annex 1**

# Improper Disclosure of Personal Data by Eight Organisations

## Case Summaries

**Case (1) - A medical diagnostic centre failed to take adequate security measures, resulting in the leakage of patients' data**

The complainant went to a medical diagnostic centre for an ultrasound scan. After the examination was completed, the doctor left the examination room, leaving the complainant alone in the room to tidy up his clothes. During the period, the complainant noted that the English names, complete HKID card numbers and brief medical histories (e.g. the organs to be scanned or the diseases suffered) of several patients (including the complainant) were displayed clearly on the screen of the ultrasound machine. The complainant was dissatisfied with the disclosure of his personal data and lodged a complaint with the PCPD.

Upon the PCPD's intervention, the centre adjusted the orientation of the screen to avoid it from facing the patients directly, ceased showing the names and HKID card numbers of patients on the screen and installed movable partition to cover the screen. The centre also revised operational guidelines to require healthcare professionals to log out of the system before leaving the examination room, enhanced staff training on personal data privacy and conducted regular privacy risk assessments.

**Case (2) - A travel agency distributed group e-tickets which contained personal data of all tour members**

The complainant provided his personal data to a travel agency for joining a group tour. Prior to the group's arrival at the destination country, the tour guide provided tour members with a copy of the same group e-ticket to present to the local customs authority during immigration procedures. However, the e-ticket contained the full English names and the dates of birth of over 30 individuals, including those of the tour guide and all the tour members. As a result, every tour member was able to view the personal data of others.

The travel agency subsequently acknowledged that the incident stemmed from the tour guide's failure to recognise that the airline had included the passengers' dates of birth on the tickets before he distributed the group e-tickets. Upon the PCPD's intervention, the travel

agency instructed the designated contact person of each subgroup to dispose of the group e-tickets and implemented several remedial measures regarding the handling of group e-tickets, including the standardisation of the format of e-tickets. Under the new protocol, only flight details and the relevant passenger's name and e-ticket number would be shown, and the e-ticket customised for each tour member would only be supplied to the tour guides after review. The group e-tickets would no longer be distributed to tour members. The travel agency also strengthened internal controls and staff training.

**Case (3) — A security service company disclosed carpark tenant's phone number to another tenant in the handling of a parking complaint**

The complainant was a tenant of a parking space in a residential estate. The complainant received a call from another tenant (Tenant A) asking the complainant to go to the car park to properly park his car so that Tenant A could park in his designated parking space. Upon arrival, the complainant discovered that the security guard on duty had disclosed his mobile phone number to Tenant A.

The security service company subsequently admitted that the incident stemmed from a request made by Tenant A to the security guard to assist him in contacting the complainant, and the security guard wrongly disclosed the complainant's phone number to Tenant A as requested for Tenant A and the complainant to handle the parking issue directly.

Upon the PCPD's intervention, the security service company took measures to remedy the contravention and prevent the recurrence of similar incidents in the future, including the formulation and implementation of policies and procedures to ensure all staff members would not use the personal data of any car park user for any "new purpose" without the data subject's consent, and the circulation of such policies and procedures to all staff members on a regular basis.

**Case (4) - The online registration form of a medical institution improperly disclosed the personal data of registrants**

The online registration form of a medial institution was found to have improperly disclosed the personal data submitted by over 100 registrants, including their names in Chinese and English, phone numbers, email addresses and dates of birth. The incident occurred because of the negligence of a staff member of the relevant organisation in failing to update the "View Summary of Responses" function in the settings of the online form, which allowed registrants

filling in the form access to the data of other registrants using the "View Summary of Responses" function.

Upon learning the incident, the medical institution ceased the use of the hyperlink to the online registration form and removed the form from the website. The institution undertook that it would apply the correct setting of the "View Summary of Responses" function in future before uploading any online form to the website for use.

**Case (5) – The contents of a letter sent by a government department could be viewed through the envelope window**

A government department posted a letter to the complainant relating to his notification of change of address. Upon receipt of the letter, the complainant found that the subject line of the letter and the case number were visible through the envelope window. As the complainant's HKID card number was used as the case number, the complainant lodged a complaint with the PCPD against the government department for failing to properly safeguard the security of his personal data.

Subsequently, the government department admitted that the incident arose from the failure of the staff member concerned to follow the department's established procedures of folding letters when handling the issue of the letter concerned to the complainant, and the staff member was also unaware that the case number could be viewed from the envelope window. Upon the PCPD's intervention, the government department took a series of follow-up measures, including reminding relevant staff members to follow the established procedures for handling letters, formulating clear graphical guidelines on the relevant letter folding requirements and procedures, moving the position of case numbers in the letter template downwards, arranging regular spot checks on the letters by supervisors, and arranging staff training to enhance their awareness of personal data privacy protection.

**Case (6) – An insurance company used documents containing personal data as recycled papers**

An insurance company used copies of resumes and HKID cards that were intended to be disposed of as recycled papers. As documents printed on the said recycled papers were sent to other companies, personal data contained therein was leaked.

Upon the PCPD's intervention, the company interviewed the staff member involved in the handling of personal data and explained the severity of the incident, emphasising that similar

incidents should not happen again. In addition, the company issued a notice to all staff members instructing them on the matters to note regarding the use of recycled papers and the disposal of documents containing personal data. Staff members were reminded that documents which become obsolete after the insurance application procedures are completed should be disposed at designated locations for processing, disposal or destruction by the recycling company. The company also arranged regular circulation of the notice to ensure that the same mistake would not be committed by staff members.

**Case (7) - A retail company accidentally disclosed members' email addresses when sending promotional emails to them**

The incident related to the dispatch of promotional emails to members by a retail company. In sending the emails, the company erroneously filled in the email addresses of all members in the recipient field, thereby revealing the email addresses of over a thousand other members to the recipients. The incident was caused by a staff member who mistakenly filled in the email addresses of all members in the recipient field when the emails were sent.

After the incident, the company sent letters of apology to all affected members, drawing their attention to the wrongly sent email and requesting them to delete the email. Upon the PCPD's intervention, the company implemented remedial measures for the email sending process. Whenever an employee sends emails to two or more external email addresses, the system would automatically send the email by using the blind carbon copy (b.c.c.) feature, ensuring that all email addresses other than that of the recipient are hidden. The company also issued a notice reminding all staff members to use the b.c.c. feature correctly.

**Case (8) — Scripting error in an airline's membership account system causing leak of personal data**

The complainant was a customer of an airline. After the complainant logged into his account using his email address, personal data belonging to another customer was shown in the account.

The airline admitted that the incident arose from a scripting error of a vendor during the update of the membership accounts system. The script erroneously read some special characters (e.g. "_" "*" and "%") contained in email addresses as wildcard characters, which resulted in the linkage of one customer's account with another customer's account with a similar email address.

The PCPD directed the airline to formulate guidelines and procedures to ensure that its vendor would include the checking of special characters in the test plan for any enhancement of system; and to establish and put in place measures to ensure that additional review of the scripting or similar protocols would be carried out by the vendor when system enhancement with impact on personal data is performed.