Personal Data System of HKICC Lee Shau Kee School of Creativity Inspection Report

Published under Section 48(1) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Background

On 13 May 2024, the HKICC Lee Shau Kee School of Creativity (HKICC) submitted a data breach notification to the Office of the Privacy Commissioner for Personal Data (the PCPD), reporting that its servers had been compromised, resulting in the encryption of the personal data stored in the servers (the Data Breach Incident), which affected approximately 1,300 individuals. The affected personal data included the names, addresses, email addresses, phone numbers, dates of birth, Hong Kong Identity Card numbers, photos, bank account details relating to students, parents, employees, freelancers, alumni and tenants, and tax information relating to employees and tenants. Upon receiving the data breach incident notification, the PCPD initiated a compliance check into the Data Breach Incident in accordance with established procedures, and issued an advisory letter to HKICC upon the completion of the compliance check.

Against this background and given that an upward trend in data breach incidents involving educational institutions was observed in recent years, the Privacy Commissioner for Personal Data (the Privacy Commissioner), Ms Ada CHUNG Lai-ling, considered that it was in the public interest to carry out an inspection (the Inspection) of the personal data system used by HKICC under section 36(a) of the Personal Data (Privacy) Ordinance (the PDPO) to assess the effectiveness of the remedial measures taken by HKICC following the Data Breach Incident and to further examine the data security of its information systems containing personal data.

HKICC, as a data user under the PDPO, is obliged to comply with the requirements under the PDPO, which include the six data protection principles in Schedule 1 to the PDPO with respect to the collection, holding, processing and use of personal data. The Inspection focused on the measures implemented by HKICC regarding the security of personal data.

PCPD officers conducted on-site inspections twice this year to inspect the personal data system of HKICC and assess the compliance with HKICC's security policies and practices by its employees. Through two rounds of written enquiries (including those following on-site inspections), the team examined HKICC's policies, procedures, guidelines, training materials and other documents related to its personal data system.

Results of the Inspection

Areas of Good Practice

The Privacy Commissioner noted HKICC's good practices in the following areas:-

(i) Following the Data Breach Incident, HKICC has implemented various technical measures to enhance the security of its information systems, including establishing a patch management system, enabling two-factor authentication for VPN login access, and enforcing strong password requirements;

(ii) Following the Data Breach Incident, HKICC has also implemented enhanced controls over VPN access to internal systems, which include restricting access to VPN to only one IT staff member with two-factor authentication enabled and enabling VPN gateway and remote access to HKICC's network only when required;

(iii) Both before and following the Data Breach Incident, HKICC's principal team is designated to be responsible for matters relating to data protection within HKICC, including the implementation of its policy on IT security (the Policy) and guideline on the use of personal data (the Guideline). The Policy will be reviewed annually and updated when necessary. The Policy and Guideline are available on the intranet for staff access;

(iv) Both before and following the Data Breach Incident, HKICC adopts the "least privilege" and "role-based" approach, granting users only the necessary permissions to access systems that contain personal data based on their roles and job responsibilities; and

(v) Both before and following the Data Breach Incident, HKICC offers training activities and awareness programmes on personal data protection and information security to staff members, and regularly communicates to them policies and guidelines relating to information security and personal data protection. Questionnaires are provided to staff members to collect feedback, which would be reviewed by the principal team to make necessary adjustments to staff training.

Areas for Further Improvement

Notwithstanding the good practices described above, the Privacy Commissioner noted the following areas for improvement in the measures implemented by HKICC in safeguarding personal data:-

(i) The Policy sets out general principles without implementation details and control measures to ensure compliance. However, there are no supplementary guidelines or procedures to support the principles set out therein, which may result in inconsistent practices and hence increase the chance of security breaches;

(ii) HKICC conducts firewall log reviews on a weekly basis which the PCPD considers insufficient and not regular enough to be certain that HKICC can promptly detect suspicious activities within its information systems. In addition, HKICC relies on the inbuilt alert mechanism of its firewall and no alert thresholds are defined for firewall traffic. There is no automated alert mechanism in place to notify IT staff of potential anomalies owing to resource constraints, which can delay the identification of and response to security incidents;

(iii) It has been HKICC’s practice to conduct vulnerability assessments on its information systems, but owing to resource constraints, the findings of the latest vulnerability assessment conducted in October 2024 have not been fully addressed at the time of the Inspection;

(iv) The Guideline specifies different retention periods for physical and electronic records across categories of data subjects. Although HKICC is committed to conducting annual reviews of personal data in its possession that has reached the relevant retention period and maintains records of data destruction activities, there is a lack of detailed procedures to ensure that personal data has in fact been securely and systematically destroyed or purged once the relevant retention period expires; and

(v) HKICC signed a data processing agreement with its third-party vendor to operate the student admission system. While the third-party vendor is required to purge the personal data on a yearly basis, HKICC has not monitored the destruction of records or requested any record of data destruction from the third-party vendor.

Conclusion

After HKICC's information system was hacked, various technical measures have been implemented to enhance the security of its information system. These include, for instance, establishing a patch management system, enabling two-factor authentication for VPN login, and enforcing strong password requirements. In terms of access control, HKICC continues to adopt the "least privilege" and "role-based" access control mechanism, granting users the necessary permissions based on their roles and job responsibilities. Additionally, HKICC continues to offer training on data protection and information security to staff and has regularly communicated relevant policies and guidelines.

Overall, the Privacy Commissioner considers that HKICC has complied with the requirements of Data Protection Principle 4 of Schedule 1 to the PDPO concerning the security of personal data in the handling of the personal data of students and staff members.

Despite HKICC's good practices, the Privacy Commissioner considers there are areas which can be improved in safeguarding personal data. These include developing more comprehensive and specific policies on information security and data retention, enhancing detection capabilities for information systems, and strengthening management and oversight of data processors in the proper destruction of personal data held by them.

Recommendations

Through the Inspection, the Privacy Commissioner wishes to make the following recommendations to HKICC to implement appropriate organisational and technical measures to safeguard the information systems that contain personal data and enhance data security:-

(i) Establish a privacy management programme and appoint data protection officer(s) to effectively manage the entire lifecycle of the handling of personal data from collection to destruction, and to promptly respond to any data breach incidents. The data protection officer(s) should be responsible for devising and managing the privacy management programme, including overseeing all procedures as may be required, and monitoring compliance with the PDPO and reporting to senior management;

(ii) Develop detailed implementation guidelines that translate the principles outlined in the Policy into specific procedures and technical controls. In this regard, supplementary documentation such as operating procedures and checklists should be devised and implemented to support consistent application across departments. Additionally, HKICC should establish control measures to monitor compliance with all the requirements relating to data security to reduce the risk of inconsistent practices and security vulnerabilities;

(iii) Implement a proactive monitoring mechanism to promptly detect and respond to potential security threats to systems containing personal data. Rather than relying solely on weekly firewall log reviews, real-time monitoring and automated alert systems, such as email notifications, should be established to immediately flag suspicious activities;

(iv) Conduct regular vulnerability assessments and audits of information systems, with a view to strengthening cybersecurity resilience and minimising potential security risks. Vulnerability assessments are essential for identifying weaknesses in systems, while security audits serve to evaluate the effectiveness of the existing security measures. In addition, a structured follow-up mechanism should be established to promptly review the findings of vulnerability assessments, prioritise the identified vulnerabilities by risk level, and implement remedial measures without delay;

(v) Enhance the Guideline by establishing clear and detailed procedures for the secure and systematic destruction of personal data once the relevant retention period expires. This includes specifying methods for purging both physical and electronic records, assigning responsibilities and implementing verification steps to ensure proper execution; and

(vi) Manage data processors prudently and conduct regular reviews of their practices to ensure that their handling of personal data complies with the agreed standards outlined in the contract, such as by obtaining records of data destruction from data processors for review.

Through the above inspection results, the Privacy Commissioner would also like to make the following recommendations to educational institutions that handle vast amounts of personal data of students and staff members to ensure data security, including:-

- Establish a Personal Data Privacy Management Programme and appoint designated officer(s) as Data Protection Officer(s);
- Establish clear internal policies and procedures on data governance and data security, and ensure thorough implementation of the same;
- Provide staff with training on data protection and information security upon onboarding and at regular intervals;
- Adopt the “least privilege” principle and “role-based” access control mechanisms;
- Implement effective measures to prevent, detect, and respond to cyberattacks;

- Conduct comprehensive security risk assessments and audits for information systems regularly;
- Exercise due diligence in appointing and managing data processors; and
- Formulate response plans for data breach incidents and incidents involving artificial intelligence.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
13 November 2025