Data Breach Incident of Yau Yat Chuen Garden City Club Limited Investigation Report

Published under Section 48(2) 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) completed its investigation in relation to a data breach incident reported by Yau Yat Chuen Garden City Club Limited (the Club).

The investigation arose from a data breach notification submitted by the Club to the PCPD on 31 October 2025, reporting that its club management system (the CMS) was rendered inoperable as a result of a ransomware attack that encrypted information system files stored on a server (the Incident).

The CMS was provided and maintained by an external service provider (the Service Provider) for managing members' information of the Club, with all associated personal data stored on the server (the Server). The Service Provider had the ability to remotely access the Server via dedicated remote access software (the Software) for the purpose of providing technical support.

The investigation revealed that the Software was operating on an outdated version that contained a known security vulnerability at the time of the Incident. The vulnerability enabled the threat actor to compromise the account credentials used by the Service Provider and the threat actor obtained direct entry to the Server where personal data was stored. This was further facilitated by the Server being left in a logged-in state without the implementation of additional authentication controls, thereby further undermining the security defences of the CMS. In addition, the Club's antivirus software and firewall were outdated, rendering them unable to detect and prevent the hacking activities.

The Club is a private, non-profit social and recreational organisation that provides recreational facilities and dining services exclusively to its registered members and their guests. A total of 9,045 data subjects were affected by the Incident, which included 1,553 active members, 1,723 supplementary card holders, 1,313 former members, and 4,456 former supplementary card holders. The personal data affected included the full names, Hong Kong Identity Card numbers and/or passport numbers, dates of birth, email addresses, contact numbers, and addresses.

The Club notified the affected persons after the Incident, and implemented various remedial measures, which included discontinuing the use of the previously vulnerable remote access software and monitoring all remote access, updating the antivirus software and firewall for all servers and endpoints to the latest versions, and applying encryption to the personal data files on the servers.

Investigation Findings

The PCPD conducted four rounds of inquiries and reviewed the information provided by the Club in relation to the Incident, and the follow-up and remedial actions taken by the Club after the Incident. Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of the Club contributed to the occurrence of the Incident (See Annex 1 for details):-

1. Use of outdated remote access software that contained a known security vulnerability;
2. Absence of user authentication measures for remote access to the Server;
3. Use of outdated antivirus software and firewall;
4. Lack of organisational measures for information security; and
5. Prolonged retention of personal data.

The Privacy Commissioner's Decision

The Privacy Commissioner was disappointed that the Club had not adopted appropriate and adequate organisational and technical information security measures before the Incident to safeguard the personal data stored in its information systems. Based on the above, the Privacy Commissioner found that the Club 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 Data Protection Principle (DPP) 4(1) of the Personal Data (Privacy) Ordinance concerning the security of personal data.

In addition, the Privacy Commissioner found that the Club had not taken all practicable steps to ensure that personal data was not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening DPP 2(2) concerning the retention of personal data.

The Privacy Commissioner has served an Enforcement Notice on the Club, directing it to take measures to remedy the contravention and prevent recurrence of similar contraventions in the future.

Recommendations

Through this report, the Privacy Commissioner recommends organisations to adopt adequate and appropriate organisational and technical measures to safeguard their information systems that contain personal data. In particular, organisations should:

- Timely update remote access software, antivirus software and firewalls in order to patch any known vulnerabilities;
- Implement effective user authentication for data access, including strong passwords and multi-factor authentication;
- Establish adequate organisational measures, including clear internal policies for information security, as well as secure and reliable remote access solutions;
- Conduct regular security risk assessments, vulnerability scans and system audits to identify and rectify security weaknesses;

- Formulate a data retention policy to ensure that personal data is not retained longer than is necessary; and
- Provide regular staff training on information security.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
23 April 2026

Annex 1

Data Breach Incident of Yau Yat Chuen Garden City Club Limited
Deficiencies that Contributed to the Happening of the Incident

1. **Use of outdated remote access software that contained a known security vulnerability**: The Software used for remote access was operating on an outdated version that contained a known security vulnerability. The vulnerability was exploited by the threat actor to facilitate the ransomware attack. The investigation found that the Service Provider was unaware of the security alert issued to affected users in January 2025 by the software developer. Furthermore, neither the Club nor the Service Provider had established mechanism for applying security patches or updates to the software concerned;

2. **Absence of user authentication measures for remote access to the Server**: The computer hosting the Server was intentionally kept logged in to ensure that the software used for remote access could run continuously in the background and remained remotely accessible to the Service Provider without the requirement of additional authentication. The Club explained that this was a legacy practice adopted for operational convenience to facilitate immediate remote support from the Service Provider without delay. Additionally, multi-factor authentication was not available for the Software at the time of the Incident, which allowed the threat actor to access the Club's information systems through the Software using the compromised credentials without any further verification;

3. **Use of outdated antivirus software and firewall**: The firewall that was enabled on the Server was outdated because of lapses in the maintenance cycle, which limited the Club's ability to detect and prevent the threat actor's activities. The Club acknowledged that its antivirus software was similarly outdated, which contributed to the absence of any alerts in respect of the ransomware in the Incident;

4. **Lack of organisational measures for information security**: The Club had not established any written information security policies or guidelines prior to the Incident. Although the Club had entered into a service contract with the Service Provider for technical support of the CMS and the Server, the contract did not stipulate any explicit information security requirements. The Club was unable to

demonstrate the existence of any effective organisational measures to safeguard the security of the Server or the personal data stored therein; and

5. **Prolonged retention of personal data**: The Club stated that it retained the personal data of former members and former supplementary card holders for a minimum of seven years following the cessation of membership, citing statutory financial record-keeping obligations in support, as well as the need to verify membership history for reinstatement requests and to resolve any historical billing disputes. However, it was found that the personal data of 888 former members and 3,321 former supplementary card holders had been retained for longer than seven years.