July/Aug 2025 Legal and Regulatory Update

Top stories

The Privacy Commissioner for Personal Data (PCPD) published 2 investigation reports on data breaches by companies in retail industry:
(A) Kwong's Art Jewellery Trading Company Limited and My Jewelry Management Limited and (B) Adastria Asia Co; Limited. (Press release)

(A) Kwong's Art and *(its subsidiary)* **My Jewellery incident**

The companies submitted a data breach notification to PCPD in Nov 24, that the personal data stored in their database server had been stolen and deleted. The threat actor conducted a brute-force attack to obtain the credentials of an administrator account.

Around **79,400 data subjects** were affected, including their respective corporate/retail customers and current/former employees. These included the names, HK ID Card numbers, dates of birth, telephone numbers, addresses and commencement dates of employment of employees, as well as the names, HK ID Card numbers *(first four alpha numeric characters)*, years and months of birth, telephone numbers, email addresses, and membership numbers of customers.

What you should watch out for
Deficiencies identified by PCPD

- Failure to **delete a former employee's account** in a **timely** manner
- Lack of **effective security and detection measures** in the information systems
- **Outdated** operating systems of servers
- Lack of **policies and guidelines** on information security
- Absence of **security assessments and audits** of the information systems

(B) Adastria Incident

Adastria, a Japanese MNC in fashion retail, submitted a data breach notification to PCPD in Nov 24, that its customer relationship management and e-commerce platforms were accessed by an unauthorised third party. They operated as a Software-as-a-Service (SaaS) provided by a third party. The threat actor used the credentials of an administrator account of a current employee to connect to the platforms.

Personal data of 59,205 customers was affected. These included the names, telephone numbers and order information of customers *(including the transaction reference numbers, order dates, membership numbers, delivery methods, deliver/pickup dates, delivery addresses, product names and descriptions, and price information)*.

It was subsequently discovered that the data were disclosed in the Dark Web approximately two months after the incident and was made available for download.

What you should watch out for

Deficiencies identified by PCPD

- **Weak password management**
- Failure to enable **multi-factor authentication** for access to accounts
- Lack of **awareness to ensure the security** of personal data
- Failure to conduct proper **security reviews** on the platforms

(C) PCPD message to retail organisations

PCPD reminds the retail industry and organisations that hold **significant amounts of personal data of customers** to allocate sufficient resources to **cybersecurity and data security.**

In general, PCPD encourages organisations to make reference to its **"Guidance Note on Data Security Measures for Information and Communications Technology**" and **"Guidance on Data Breach Handling and Data Breach Notifications"** *(also see our Jul/Aug 23 update).* Useful resources also include the PCPD Data Security thematic webpage, data security hotline (2110 1155) and the "Data Security Scanner"*(a self-assessment toolkit).*

What you should do

Recommended organisational and technical measures

- Establish **clear internal policies and procedures** to safeguard the security of information systems
  - Also **thorough implementation**
- Implement **effective measures to prevent, detect and respond to cyberattacks**
  - Including regular vulnerability scans and patching cybersecurity vulnerabilities in a timely manner
- Cease the use of **end-of-support software** and **upgrade** in a **timely** manner
- Enhance **password management**; adopt **multi-factor authentication**
- Conduct comprehensive **security risk reviews and audits** regularly

- Configure appropriate security functions on **service platforms provided by third-party vendors**
    - Also conduct **regular security review**
- Formulate a **data breach response plan**
- Provide appropriate **training** to employees to improve **data security awareness**

Also in this issue

ESG: HK sustainability reporting standards

(i) **HKICPA has released** **HKFRS S1 and S2 Guidance – Part 1** , a practical application guidance designed to support both sustainability and non-sustainability professionals in applying HKFRS S1 *General Requirements for Disclosure of Sustainability-related Financial Information* and HKFRS S2 *Climate-related Disclosures*.

Regulators

(ii) **HKEX published some updated FAQs and Guide on general meetings**

- **Updated Guide on general meetings** *(version with changes marked)*
    - updates include guidance on **virtual/hybrid meetings**; updated template proxy form
- **FAQ 16** *(marked-up version)*
    - addresses the **"core shareholder protection standard"**; including that the standard will **NOT be met if a shareholder is allowed to submit questions electronically before the meeting**
    - (Q4) *(Updated)* "Guide on general meetings" states that issuers should make arrangements to allow **shareholders attending the meeting virtually** to listen, speak and submit real-time questions during the meeting
- **FAQ 10** *(marked-up version)*
    - updates cover the **"paperless regime"**, including those arrangements to be effective upon the implementation on the **USM** regime

Published by Practising Governance Limited

Sept 2025