Feb 2023 Legal and Regulatory Update

Top stories

HKEX published updated (i) Guide on General Meetings (ii) relevant FAQ .

The updated Guide principally **reflects recent amendment of HK Companies Ordinance** which now expressly enables companies holding **general meetings virtually** or in **hybrid** mode, rather than holding meetings only at **physical locations.** *(Background: see our Jan 23 update)*

It contains HKEX **guidance relating to holding virtual/hybrid *meetings*** *(e.g. shareholder authentication)*, which are also in line with HK Companies Registry's Guidance Note.

There was consequential update of the relevant **FAQ**, withdrawing 1 question.

Also in this issue

Legislation

The Privacy Commissioner for Personal Data ("PCPD") published an investigation report into a data breach incident of HK Institute of Bankers ("HKIB"). (Press release, Executive summary of investigation report)

In Jan 22, HKIB notified PCPD of a data breach incident, that servers containing **personal data** *(of 13,000 members and 100,000 non-members)* had been attacked by **ransomware** and maliciously encrypted. The hacker had threatened to upload the files to the internet and demanded a ransom.

*(Background: HKIB purchased a firewall from a **service provider** which also performed **outsourced maintenance** service. **Firewall manufacturer** issued a security advisory on its website as regards a specified vulnerability, and **suggested specific measures** by users ("multi-factor authentication"). The Government Computer Emergency Response Team HK also issued a high threat security alert on such vulnerability, advising organisations to "patch" any affected systems immediately.*

Neither HKIB nor its outsourced service provider was aware of such vulnerability. The recommended measures were not implemented).

HKIB, as the data user, had breached the **Data Protection Principles**.

*(Principle 4: **all practicable steps** shall be taken to ensure that any personal data held by a **data user** is protected against unauthorised or accidental access, processing, erasure, loss or use).*

PCPD considered that HKIB **lacked effective data security risk management mechanism** and adopted a **lax approach** towards **service providers** in the maintenance of critical network infrastructure.

It also made **recommendations to other organisations** that handle personal data using information and communications technology.

What you should watch out for/do:

Failures

- Inadequacies in **management of data security risks**
  - Did not stipulate any **risk management mechanism for data security**
  - E.g. service providers not requested to perform regular security checks/vulnerability scans
- Deficiencies in **data information management**
  - E.g. antivirus software only had basic protection capabilities
- Prolonged implementation of multi-factor authentication

Recommendations to other organisations

- **Stay vigilant** to prevent hacker attacks
  - Conduct **regular risk assessment**
- Establish **personal data privacy management programme**
- Appoint **dedicated "data protection officer"**
- Enhance **information system management**
  - E.g. develop effective patch management procedures
- Conduct **data backup** conscientiously
- **Monitor service providers** properly

Published by Practising Governance Limited

March 2023