Jan 2025 Legal and Regulatory Update

Top stories

HKEX conclusions on paperless reforms

HKEX published consultation conclusions on proposals to further expand its paperless listing regime and other rule amendments. (Press release; full document).
(Background on consultation: our August 24 update)

Our focus is on proposals regarding continuing obligations of issuers of listed equity securities. The proposals were **adopted with some modifications**, with **transitional periods.** *(See summary tables, from P.2 of full document)*

- **(1) Electronic instructions from securities holders**: to provide an **option** for securities holders to send "requested communications" to issuers electronically
- **(2) Real-time electronic payment of "Corporate Action Proceeds": option** for securities holders to receive the same *(e.g. dividends)* electronically; *(modified)* **not** limited to **CHATS** system
- **(3) Hybrid general meetings and E-voting:** *(to the extent permitted by applicable laws)* **issuers** to ensure their **constitutional documents** enable them to do so

Proposals 1 and 2 are also related to the "Uncertificated Securities Market" regime (USM). **Transitional periods** are provided**, referencing USM implementation** date *(expected to be around end of 2025)***.**

Further details on **Proposal 1** are set out below, with transitional periods varying with the nature of communications.

Proposal 2 will be effective **1 year after USM implementation.**

Proposal 3 will be effective for issuers by the **first AGM held after July 25**.

What you should know

Electronic instructions from securities holders

- **Option** for securities holders to send **"Requested Communications"** to issuers electronically
  - "Meeting Instructions" re: a meeting of securities holders, including an indication as to attendance and proxy-related instructions
  - "Non-meeting Instructions" re: "Actionable Corporate Communications" *(except response to provisional allotment letter in a rights issue)*

- Issuers might need to **amend constitutional documents**
- Issuers expected to have appropriate arrangements to **verify the authenticity** of requested communications
  - **Free to choose** authentication mechanisms
- **Transitional period *(after USM implementation)***
  - Ending 1 year thereafter, for **"Standardised Requested Communications"** *(dividend election instructions, meeting instructions)*
  - Ending 5 years thereafter, for **"Non-standardised Requested Communications"**

What you should do

- Note the interaction with the **USM** regime, for future preparations

Also in this issue

Regulators

(i) HKEX and SFC collaborate in the enforcement action against FingerTango Inc. and 8 former directors *(including executive and independent directors).*

Background: The case involved (i) material deviation of use of **IPO proceeds** per its prospectus *(for an unlisted wealth management product)*, (ii) **grant of loans** *(total: around RMB 426.5M)* without proper director oversight; breach of Listing Rules disclosure requirements. There was substantial impairment subsequently.

(A)HKEX aspects (Press release, Statement of disciplinary action)

HKEX sanctions include censuring the company, imposes a Director unsuitability statement/Prejudice to investors statement/censures/criticises specified former directors respectively.

In its press release, HKEX stressed that before an issuer engages in any **money lending activities**, directors must ensure that appropriate and effective **internal controls** and procedures are in place to safeguard the issuer's interest and procure compliance with the Listing Rules.

(B)SFC aspects (Press release)

In parallel, SFC has commenced legal proceedings in the Court of First Instance *(s. 214, Securities and Futures Ordinance)*, seeking court orders including **compensation and disqualification orders** against the company and its 8 former directors.

Legislation

(ii) The Privacy Commissioner for Personal Data (PCPD) published (A) an investigation report on data breaches of the Urban Renewal Authority (URA) and (B) Guidance on cloud computing. (Press release, Guidance)

(A) URA incident

URA submitted a data breach notification to PCPD in May 24, that the personal data of members of the public stored on a **cloud platform** by the URA could be accessed by any person without inputting any account or password (No-password access).

It used the e-form platform associated with the cloud platform ArcGIS Online to create two e-forms for briefing sessions on the property acquisition under a development scheme. The No-password access problem was subsequently discovered.

Personal data of 199 persons were affected, including telephone numbers, names of contact persons and details of their ownership/correspondence addresses. After further investigation, URA found out that the e-forms used were an older version, without the benefit of enhanced protection features.

What you should watch out for

Deficiencies identified by PCPD

- **Failure to update the software in a timely manner**
- **Lack of understanding of the software used** to collect personal data, and failure to develop and conduct effective and comprehensive **security tests**

(B) Guidance on cloud computing

The Guidance provides recommended measures on various aspects for organisations to better protect personal data privacy. It covers aspects such as **service and deployment models** *(e.g. dedicated private cloud vs shared public cloud; various service models)*, **standard services and contracts** as well as **outsourcing** arrangements.

(iii) PCPD published an investigation report on data breaches of Oxfam. (Press release)

Oxfam submitted a data breach notification to PCPD in Jul 24, that it has been subject to **ransomware** attack.

PCPD investigation revealed that the attacker conducted brute-force attack, exploited the critical vulnerabilities in the firewalls of Oxfam. It identified vulnerable servers within Oxfam's network and gained administrator privileges. Ransomware was deployed, potentially affecting around **550,000 data subjects** *(e.g. donors, event participants, volunteers, programme partners/participants, staff/job applicants).*

Personal data affected include names/spouses' names, HKID card numbers/copies, dates of birth, phone numbers, email addresses, addresses, credit card numbers, and bank account numbers.

What you should watch out for

Deficiencies identified by PCPD

- **Outdated Firewalls** which contained critical vulnerabilities
- Failure to enable **multi-factor authentication**
- Lack of **critical security patches** of servers
- **Ineffective detection** measures in the information systems
- Inadequacies of the **security assessments** of information systems
- Lack of specificity of its **information security policy**
- **Prolonged retention of personal data**

Published by Practising Governance Limited

February 2025