DORSEY

DORSEY+WHITNEY LLP

Hong Kong PCPD Releases Recommended Data Security Measures

by Janet Wong

On August 30, 2022, the Hong Kong Privacy Commissioner for Personal Data (the "**PCPD**") released a guidance note (the "**Guidance Note**") on data security measures for information and communications technology to provide data users with recommended data security measures to facilitate their compliance with the relevant provisions under the Personal Data (Privacy) Ordinance (Cap 486 of the Laws of Hong Kong) (the "**PDPO**"). The PDPO was amended last year to criminalize doxxing (please refer to our last eUpdate in October 2021 on this topic).

According to the PCPD, in recent months, data users have been confronted with considerable challenges with respect to protection of data privacy and data security in light of the new normal consisting of hybrid modes of working and learning. In the first seven months of 2022, the PCPD received 68 data breach notifications from organizations, a quarter of which involved vulnerabilities of information and communication technology systems of data users. In light of these cybersecurity incidents, the PCPD issued the Guidance Note to provide comprehensive recommendations on best practices to strengthen data security systems in organizations, especially small and medium-sized enterprises.

Background

Data Protection Principle ("**DPP**") 4(1) of Schedule 1 to the PDPO requires data users to take all practicable steps to ensure that personal data held by it is protected against unauthorized or accidental access, process, erasure, loss or use. In essence, it requires an organization to take into account the kind of data and the harm that could result if a data security incident occurs. The resulting harm from a data security breach depends on the volume and sensitivity of the relevant personal data and required steps to ensure security and compliance with the PDPO will need to be accordingly proportionate to the volume and degree of sensitivity.

Related People

- Janet Wong

Related Capabilities

- Corporate Governance & Compliance
- Privacy & Social Media
- Hong Kong
- Technology

Summary of Recommended Data Security Measures

To help guide organizations in their compliance efforts in protecting personal data, PCPD's Guidance Note provides recommendations on data security measures in the following areas:

1. ***Data Governance and Organizational Measures.*** An organization should establish clear internal policy and procedures on data governance and data security that cover areas including, among other things, roles and responsibilities of staff in maintaining systems and safeguarding data security, data security risk assessments and handling of data security incidents (such as an incident response plan and reporting mechanism). It may make reference to the IT security or cybersecurity standards and best practices set by reputable organizations and review and revise its policies and procedures periodically based on prevailing circumstances. A data user should also appoint suitable personnel specifically responsible for personal data security (such as a Chief Information Officer) and should provide sufficient training for staff members to educate and inform them of the organization's data security policies and procedures. It may also include confidentiality obligation in its employment contracts with its staff members where appropriate.
2. ***Risk Assessments.*** An organization is recommended to conduct risk assessments on data security for new systems and applications before launch and periodically thereafter. The PCPD also recommends SMEs to consider engaging third party specialists to conduct security risk assessments to identify relevant risks so as to address them promptly.
3. ***Technical and Operational Security Measures.*** The Guidance Note provides a non-exhaustive list of technical and operational measures that an organization may consider putting in place to ensure data security. It should be noted that the adequacy of the security measures will depend on the circumstances and may vary on a case by case basis. Some of these measures include securing computer networks, establishing a database management system, adopting access control measures, setting up firewalls and anti-malware, protecting online applications, using encryption when transferring or storing data, preventing misuse of and filtering emails, setting up backup systems and ensuring timely destruction or anonymization of unnecessary or expired personal data.
4. ***Data Processor Management.*** The Guidance Note recommends for organizations to properly manage data processors. Since it is common to engage contractors such as data processors for processing personal data (such as cloud and data analytics service providers), organizations should note that they may be liable for acts of its agents including data processors. As such, organizations should consider factors when engaging data processors such as competency and reliability of data processors, nature of personal data being transferred, security measures taken by data processors, protocols for reporting on data security incidents, and conducting field audits to ensure compliance with the data processing contract by data processors.
5. ***Remedial Actions in the event of Data Security Incidents.*** DPP4(1) provides that organizations must take all practicable steps to protect the personal data they hold having regard to harm resulting from a data security incident. The Guidance Note, therefore, provides some common remedial actions organizations may take in the event of such incidents. These include: disconnecting the affected systems, changing passwords and ceasing access, changing system configurations, notifying affected individuals, reporting to PCPD and other relevant regulators, fixing the security weakness and following up on the lessons learnt.
6. ***Monitoring, Evaluation and Improvement.*** The Guidance Notes recommends for

organizations to engage an independent task force, such as an internal or external audit team, to monitor compliance with the organization's data security policy and evaluate the effectiveness of the data security measures periodically.

7. ***Other data security measures and recommendations including cloud services, 'Bring-Your-Own-Devices' ("BYOD") and portable storage.***

As working remotely from the office has become increasingly common, it is also common that data is transferred out from an organization's information and communications systems. As a result, organizations may be exposed to a variety of security issues. The Guidance Note provides recommendations applicable to such circumstances and issues to consider with respect to using third-party cloud services, protecting personal data of an organization in BYOD situations and where portable storage devices are used.

Conclusions

The Guidance Note provides useful guidelines with specific measures that businesses should take to strengthen their data security systems and to minimize risks of data breaches which could cause reputational and financial damages. It would be a good time for businesses to review the adequacy and effectiveness of their existing data security policies and measures or putting in place one that is in line with the prevailing circumstances. If you would like to discuss any of the matters mentioned in this eUpdate, please contact either Hilda Chan or Janet Wong.