

Navigating Data Breach Notification and Prevention in Hong Kong: A New Comprehensive Guide in Hong Kong

by Janet Wong

Introduction

In June 2023, the Privacy Commissioner for Personal Data in Hong Kong (the “Commissioner”) released a new guidance note on data breach handling and notifications (the “Guidance Note”). The purpose of this note is to assist data users in preventing and managing data breaches effectively. The Guidance Note is a comprehensive document which recommends best practices in data governance, risk assessments, technical and operational security measures, data processor management, and remedial actions during data security incidents. In today's new normal, which includes hybrid modes of working and learning, data users face challenges in protecting data privacy and security. The Guidance Note is designed to help businesses minimize the risks of data breaches, which can cause reputational and financial damages. Moreover, it sheds light on essential requirements on the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong) (the “PDPO”), compelling data users to safeguard personal data from unauthorized access, processing, erasure, loss, or misuse.

The Guidance Note focuses on the following areas concerning data breach:

1. **Preparing for Contingency - Data Breach Response Plan** A data breach response plan is crucial for organizations to effectively manage and minimize the impact of data breaches. The plan should encompass procedures for identifying, containing, assessing, and managing incidents. It should also define the roles and responsibilities of team members, communication plans, risk assessment workflows, investigation procedures, and record-keeping policies. Taking swift action in response to a data breach can significantly reduce the extent of damage caused. Regular reviews of the plan and adequate staff training are essential to ensure its effectiveness.
2. **Handling Data Breaches** The recommended steps for handling data breaches demonstrate the data user's commitment to addressing the issue promptly, which can significantly reduce the impact on affected individuals and potential reputational damage. The steps include:

Related People

- Janet Wong

Related Capabilities

- Asia-Pacific
- China
- Privacy & Social Media
- Hong Kong

Step 1: Gather all relevant information about the breach and escalate the incident to the dedicated data breach response team if necessary.

Step 2: Take immediate steps to contain the breach, such as shutting down or isolating compromised servers and disabling relevant system functions.

Step 3: Assess the risks of harm to affected individuals by evaluating the nature and sensitivity of the personal data involved and the circumstances of the breach.

Step 4: Consider notifying the relevant authorities and affected data subjects as soon as practicable after becoming aware of the breach, particularly if there is a real risk of harm to those individuals.

Step 5: Keep a comprehensive record of the breach to facilitate a post breach review, including all relevant details, and use the lessons learned to improve personal data handling practices.

3. *Data Breach Notifications*

Data users need to act quickly in the event of data breaches. They should promptly notify relevant parties, including affected data subjects and the Commissioner, upon becoming aware of a breach. This notification is vital to mitigate potential harm, enable investigative actions, demonstrate commitment to data privacy management, raise public awareness, and seek advice. The notification should include a general description of the breach, date and time of occurrence, source, types of personal data involved, risk assessment, mitigation measures taken, and contact information for the data breach response team. Data subjects can be notified directly or through public announcements, while the Commissioner should be notified using its Data Breach Notification Form, which can be submitted online, by fax, in person, or by post. Oral notifications are not accepted, and the Commissioner provides assistance in completing the form.

Conclusion

The Guidance Note highlights the complex legal framework in Hong Kong that mandates remedial actions for data breaches and is a valuable resource offering insights and strategies to prevent and handle data breaches effectively. Data users must promptly notify affected parties and the Commissioner, take necessary measures to mitigate harm, initiate investigations, demonstrate commitment to data privacy management, raise public awareness, and seek advice. Non-compliance with these regulations can lead to severe legal consequences. Therefore, preventing data breaches has become increasingly crucial to safeguard personal data, protect reputation, and avoid financial harm. By following the recommendations, businesses can enhance their data governance, security measures, and response strategies, thus reducing the risks associated with data breaches. Vigilance and preparedness will be key to safeguarding personal data and preserving the trust of customers and stakeholders alike for any business.

Alongside with the Guidance Note, the Commissioner has introduced an online notification form, streamlining the reporting process for businesses facing data breaches.

Currently, failing to report data breaches to the Commissioner or affected parties does not constitute a breach of the PDPO. However, the Commissioner is proactively pursuing amendments to the PDPO. This endeavor includes working towards establishing a mandatory data breach notification mechanism. While the precise timeline for these legislative amendments remains uncertain, the release of well-defined proposals is expected in the near future.

If you would like to discuss any of the matters raised in this eUpdate, please contact either Hilda Chan or Janet Wong.