HOW SHOULD YOU RESPOND TO A PERSONAL DATA BREACH IN HONG KONG?

A major hotel group has recently reported a data leak to the Office of the Privacy Commissioner for Personal Data (the "**PCPD**") in Hong Kong. Reportedly, it was hit by a cyber hack a few months ago and, as a result, certain data files concerning personal data of more than 290,000 individuals were exfiltrated. The PCPD has launched a compliance check into the data breach incident.

This client briefing discusses how one should respond to a data leak and what the PCPD's expectations are.

Currently, under the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"), it is not mandatory to notify the PCPD of a data breach. However, the PCPD has published a Guidance on Data Breach Handling and the Giving of Breach Notifications ("**Guidance**") which contains the PCPD's recommendations as to the steps a data user should take when a data breach incident is detected. Under the Guidance, it is a best practice to make a data breach notification "as soon as practicable" after the breach is discovered by the data user, except where law enforcement agencies have requested that a notification be withheld for investigative purposes.

Whilst the Guidance does not elaborate on the requirement to make the notification "as soon as practicable", it seems that the PCPD would expect a notification to be made as soon as the data user becomes aware of the data breach and has gathered preliminary information as to the extent and effect of the data breach. A notification should not be delayed until a full internal investigation has been concluded.

From the PCPD's perspective, a timely notification would help draw the attention of the data subjects who have been affected to the incident and allow those data subjects to take appropriate actions to mitigate against the potential harm that the data leak might bring about. Relevant authorities could also take appropriate actions to supervise and assist with the handling of the incident after receiving the notification. Indeed, the Guidance recommends that where a real risk of harm to the data subjects affected is reasonably foreseeable, the data user should consider giving a data breach notification to not only the PCPD but also the affected individuals and other relevant parties such as the law enforcement agencies and Internet companies.

The Guidance also contains recommendations on the immediate steps that a data user could take in response to a data breach:

- **Information gathering:** data users should immediately gather all relevant information relating to the breach, such as the date, time and place of the breach, how it has been detected, its cause, the kind and extent of personal data involved and the number of data subjects affected;

- **Containment measures:** data users should identify the cause of the breach and adopt measures to contain the breach - for example, shutting down the system which was causing a system failure, changing the security settings to prevent further unauthorised access, and seeking technical assistance to stop hacking activities;

- **Contacting relevant parties**: where appropriate, data users should consider contacting the relevant law enforcement agencies, regulators (e.g. the PCPD), Internet companies and IT experts, for reporting, advice and assistance;

- **Risk assessment:** an assessment should be conducted to evaluate the extent of harm that may be caused by the data breach to the data subjects and the data user, including potential threats to personal safety, identity theft and financial loss; and

- **Evidence keeping**: all evidence in relation to the data breach should be preserved to facilitate further investigations and corrective actions.

The Guidance does not have the force of the law, so a non-compliance with the Guidance in itself would not be a contravention of the PDPO. Nor would it lead to any immediate fines or penalties. That said, the Guidance serves as general reference to assist data users in handling data breaches and it is advisable for data users to follow the best practices stated therein.

The Government has been considering the possibility of introducing a mandatory data breach notification mechanism. In particular, the Constitutional and Mainland Affairs Bureau ("**CMAB**") has considered the data breach notification requirements in other jurisdictions. As shown from the Legislative Council Paper which was published in January 2020, the CMAB was still considering the time limit to be specified for a mandatory notification and whether the time limit should allow time for internal investigation before a notification is made. It appears that the Government was inclined to specify a time limit such as "as soon as practicable and, under all circumstances, in not more than five business days". It was also proposed that the PCPD should be empowered to direct the data users to notify the affected individuals.

While there is yet to be a clear roadmap to introduce a mandatory notification mechanism in Hong Kong, data users should keep a close eye on the development on this topic. Moreover, data users having a cross-border presence should also ensure that they comply with all applicable notification requirements in jurisdictions that have a mandatory data breach notification regime, such as Australia, Canada, the People's Republic of China and the European Union. It is also important to follow the applicable time limits for making such notification in each relevant jurisdiction.

CONTACT

WYNNE MOK
PARTNER
T: +852 2901 7201
E: wynne.mok@slaughterandmay.com

JASON CHENG
ASSOCIATE
T: +852 2901 7211
E: jason.cheng@slaughterandmay.com

SHIRLEY CHOI
ASSOCIATE
T: +852 2901 7292
E: shirley.choi@slaughterandmay.com