Proposed Reform to Hong Kong's Data Protection Law

1 April 2020

Background. In October 2018, a major Hong Kong airline publicly announced that the personal information of 9.4 million passengers including their passport numbers, identity card numbers, email addresses and credit card details had been leaked. The airline admitted that it was aware of this breach as early as March 2018. The scale of repercussions for the airline (or the lack thereof) due to this particular data breach, among other cases, emphasizes the significant gaps in Hong Kong's data protection law.

In view of this, the Constitutional and Mainland Affairs Bureau ("CMAB") issued a discussion paper (the "Paper") proposing amendments to the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") to increase protections of individuals and their personal data. Corporates and financial institutions should follow these amendments closely considering the substantial amounts of personal data they collect, retain, process and use. These amendments, if implemented, could mean financial institutions found to be in contravention of the PDPO may be liable to pay a fine linked to their annual turnover.

Enacted in 1996, the PDPO aims to protect individuals' right to privacy with respect to personal data and governs how data users should collect, handle and use personal data. In 2012, the PDPO was significantly overhauled to introduce, among other things, direct marketing provisions and additional protections. However, recent data breach incidents have exposed significant gaps in the current law, particularly the absence of a mandatory requirement to promptly report a data breach and inadequate penalties to deter violations. To address these gaps, the CMAB proposed six amendments (listed in detail below), many of which were drawn from the EU General Data Protection Regulation ("GDPR"), often considered a forerunner on privacy rules.

Mandatory data breach notification mechanism. The Paper proposes establishing a mandatory data breach notification mechanism to require the data user to report data breaches within a specified timeframe (i.e., as soon as practicable and, in any event, in not more than five business days). Where necessary, the data user will also be required to notify the impacted individuals. There is currently no statutory requirement for the data user to notify the Privacy Commissioner for Personal Data ("PCPD") or the data subject in the case of a data breach. Relevant notification is made on a voluntary basis

without a specified notification time frame imposed on the data user. For instance, the breach of the personal data of the 9.4 million passengers was only reported by the airline six months after the incident.

Data retention period. The Paper also proposes requiring data users to formulate a clear retention policy, specifying a retention period for the personal data collected. Like many other jurisdictions, the CMAB recognises that it is not feasible to impose a uniform retention period on the all data users since every data user uses data differently, according to their own business needs. At the same time, the CMAB also recognises that the risk of a data breach increases the longer such data is retained by the data user. Taking these factors into consideration, the retention policy proposed by the Paper will cover a number of aspects: (1) the maximum retention periods for different categories of personal data; (2) the legal requirement which may affect the designated retention periods; and (3) how the retention period is determined (i.e., upon collection or cessation of the business of the data user).

Sanctioning powers. The Paper proposes raising the fine levels and empowering the PCPD to directly impose administrative fines for breaches of the PDPO. Under the current regime, the maximum penalty for non-compliance with an enforcement notice is HK$50,000 and imprisonment for two years on first conviction. This is in stark contrast to the maximum administrative fine imposable by the European Union, €20 million or 4% of the data user's global annual turnover in the preceding year, whichever is higher. As suggested in the Paper, the CMAB explored the feasibility of introducing an administrative fine linked to the annual turnover of the data user and the possibility of classifying data users of different scales according to their turnovers to match with different levels of administrative fines.

Regulation of data processors. The Paper proposes extending the obligation to protect personal data on data users as well as data processors given that it is now common for data users to outsource data activities to data processors. Under the current law, there is no obligation on the data processors to protect any data stored or collected by them. Drawing reference from overseas regulatory authorities, this proposed amendment serves to close this loophole and introduce direct regulation of data processors. For instance, data processors may be accountable for personal data retention and security and required to promptly notify the PCPD and the data user upon becoming aware of any data breach.

Definition of personal data. The Paper proposes expanding the definition of "personal data" to cover information relating to an "**identifiable natural person**" rather than an "**identified person**". This amendment was introduced in view of the wide use of tracking and data analytics technology, whereby the data collected (e.g., Internet protocol (IP) addresses and cookie identifiers) can directly or indirectly identify a person.

Regulation of disclosure of personal data of other data subjects. The Paper also addresses doxxing - a separate but major concern that has arisen recently. To address doxxing behavior more effectively, directions under consideration include conferring statutory powers on the PCPD to request the removal of doxxing content from social media platforms or websites and the requisite powers to carry out criminal investigation and prosecution.

Significance. The amendments proposed by the Paper aim to strengthen Hong Kong's outdated data privacy law and align it more closely with international data protection standards. While these amendments are welcomed by the public, these amendments will unavoidably increase compliance costs for the business sector. In light of the significant liabilities imposed by the increased fines, corporates and financial institutions in particular should be prepared to introduce appropriate measures to their systems and, if necessary, review and potentially renegotiate their contracts with their data processors. It remains to be seen how and when these amendments will be enacted; however, it is increasingly likely that institutions will need to factor in the PDPO into their overall compliance, insurance and risk management policies and procedures, and account for any related contingent liabilities going forward.

* * *

Please do not hesitate to contact us with any questions.

HONG KONG

Gareth Hughes
ghughes@debevoise.com

Mark Johnson
mdjohnson@debevoise.com

Adam Lee
alee@debevoise.com

Ralph Sellar
rsellar@debevoise.com