LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice 22 January 2020 | Number 2580

Hong Kong Considers Sweeping Changes to Privacy Laws

Potential amendments to the PDPO would impose much stricter controls on organisations that process personal data of individuals located in Hong Kong.

Key Points:

- On 20 January 2020 the Legislative Council debated potential changes to the Personal Data (Privacy) Ordinance (PDPO), prompted by a Panel on Constitutional Affairs' discussion paper, which outlines five material potential changes to the PDPO.
- Panel Members discussed the prospect of holding social media platforms that host "doxxing" (起底) content, and fail to remove it promptly, liable for such failure.
- The motion for a public consultation on the PDPO, with the aim of collecting views from the community on privacy and related issues failed to pass, though Members largely support a comprehensive amendment to the PDPO, meaning the paper is likely to be further refined by the PCPD and will lay the foundation to formally draft an amendment to the PDPO.
- Members also discussed the prospect of bringing Article 33 of the PDPO into force, which prohibits the transfer of personal data to places outside Hong Kong unless certain criteria are fulfilled, though no immediate change is expected.

Background to the Discussion Paper

On 17 January 2020, Hong Kong's Panel on Constitutional Affairs (the Panel) released a discussion paper (LC Paper. No. CB(2) 512/19-20(03) (Discussion Paper) and sought feedback from Members on changes to the PDPO. The Constitutional and Mainland Affairs Committee and the Privacy Commissioner for Personal Data (PCPD) then released the Discussion Paper as part of the Panel's agenda for the meeting on 20 January 2020.

Potential Changes Proposed Within the Discussion Paper

The Discussion Paper considers recent trends in data protection law in various jurisdictions, including Australia, Canada, New Zealand, the European Union (EU), and Singapore. Based on a review of these jurisdictions, and concerns identified by the PCPD, a series of potential changes to the PDPO are proposed, including:

- **Definition of personal data**: Expanding the definition of "personal data" to cover information relating to an "identifiable" natural person rather than an "identified" person, to increase the scope of information subject to the PDPO. This recommendation is largely consistent with the approach taken in jurisdictions such as the EU.

- **Mandatory data breach notification**: There is currently no statutory requirement under the PDPO to notify the PCPD of a data breach (although notifications can be, and are, made on a voluntary basis under the existing regime). The Discussion Paper proposes a mandatory data breach notification mechanism with the following high-level structure:
    - Aligning the definition of "personal data breach" with the definition used in the GDPR[1]
    - Setting the notification threshold as data breaches that pose "a real risk of significant harm"
    - Requiring breaches that satisfy the above criteria to be notified to both the PCPD and affected individuals (although the Discussion Paper does suggest that different thresholds could apply to each of the PCPD and individual notification requirements)
    - Requiring breaches to be notified within a fixed timeframe and with specified modes of notification (the Discussion Paper uses the following example: "as soon as practicable and, under all circumstances, no later than five business days")
    - Proposing data breach notifications to be communicated by email, fax, or post
    - Requiring the notification to include a description of the incident and cause of personal data, as well as the type and volume, an analysis of the risk of harm, remedial action taken to mitigate risk of harm, and actions that the data subject should take (the PCPD plans to provide templates and guidelines on data breach notification)
- **Data retention periods**: While the PDPO includes a general requirement that a data user take all practicable steps to ensure that personal data is not kept longer than is necessary, the Discussion Paper suggests that organisations implement a clear data retention policy that specifies the retention periods for different categories of personal data collected, as well as how the retention period is calculated.
- **Increased fines and enhanced powers for the PCPD**: Currently, the PDPO is empowered to issue enforcement orders, but not administrative fines, for breach of the PDPO. This means that a data user that contravenes the PDPO but complies with an enforcement order will not face an administrative fine. In the event of a failure to comply with the enforcement order, the maximum possible fine is HKD50,000. The Discussion Paper contemplates several key changes to this scheme:
    - Equipping the PCPD with the ability to directly leverage administrative fines on data users that fail to comply with the PDPO
    - Linking administrative fines to the annual turnover of the data user rather than a fixed penalty (in the same way the GDPR provides for a maximum fine amounting to 4% of global turnover of a data controller's annual global turnover)
    - Increasing imprisonment for breach of the PDPO (currently an individual can be subject to up to two years' imprisonment for breach of the PDPO), though no specific term is set out in the Discussion Paper
    - Amending the PDPO so that the thresholds for imposing administrative fines, as well as mechanisms for imposing administrative fines, are introduced to enhance fairness of the administrative fines system

- **Regulation of data processors**: The PDPO only directly regulates the processing of personal data by data users (commonly referred to as data controllers in jurisdictions such as the EU and Singapore). The Discussion Paper contemplates imposing direct legal obligations on processors and sub-contractors to ensure a fair sharing of responsibilities of data users and processors and to ensure that processors and sub-contractors are accountable for failing to protect personal data (*e.g.*, failing to prevent personal data leakage). The changes may include rules for processors on data retention and security and processor-specific data breach notification obligations.

- **Regulation of disclosure of personal data of other data subjects**: The PCPD has received and identified over 4,700 instances of deliberate and malicious posting of personal data of individuals online (commonly referred to as doxxing). 1,400 of these instances have been referred to the police for further investigation. The Discussion Paper proposes amending the PDPO to curb doxxing by introducing specific powers for the PCPD to request removal of such content from online platforms, and to undertake criminal investigation and prosecution of such matters.

Outcome of the Panel Meeting

During the Panel Meeting, Members were invited to provide input on the proposed amendments. The Privacy Commissioner for Personal Data, Mr. Stephen Kai-yi Wong, and Secretary for Constitutional and Mainland Affairs, Mr. Patrick Nip Tak-kuen, responded to the input during the Panel Meeting.

Members' comments likely will provide guidance for the Constitutional and Mainland Affairs Bureau and the PCPD as they further refine potential changes to the PDPO, with discussion focusing on the following:

- Certain Members criticised the potential changes as insufficient, suggesting that the PDPO should be updated to more closely align with international standards.

- A significant issue for debate is the extent to which the PDPO can regulate, and the PCPD can enforce, potential new regulations on doxxing (or 起底) — increasing the PCPD's powers is anticipated to assist in curbing the issue.

- Certain Members asked that the amendments to the PDPO consider the extent to which a social media or other platform hosting personal data that is the subject of doxxing should be liable for such content if the content is not promptly removed.

- Several Members raised whether Article 33 of the PDPO — which prohibits the transfer of personal data to places outside Hong Kong, including the mainland, unless certain criteria are fulfilled — should be brought into force. The PCPD indicated that it is currently working on designing guidelines on transfer for release later in 2020 and will consider Article 33 thereafter.

- The PDPO should directly regulate "sensitive" categories of personal data in a different way to other personal data (this data is considered a separate, special category in jurisdictions such as the EU).

- One Member sought to pass a motion to seek, among other things, that the Discussion Paper and proposed amendments be subject to public consultation, however, the motion was tied and therefore failed to pass. The motion is not expected to impact the Constitutional and Mainland Affairs Bureau and the PCPD's plan to draw up changes to the PDPO.

Next Steps

Based on the discussions during the Panel Meeting, the Constitutional and Mainland Affairs Bureau and the PCPD will now seek to conduct an in-depth study on specific legislative amendments and consider further consultation with stakeholders prior to proposing a formal amendment to the PDPO.

Latham & Watkins will continue to track discussions closely and will provide regular updates on potential changes to the PDPO.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

Fiona M. Maclean
fiona.maclean@lw.com
+44.20.7710.1822
London

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Esther C. Franks
esther.franks@lw.com
+65.6437.5345
Singapore

You Might Also Be Interested In

Navigating Data Processing Ethics for FinTech in Hong Kong

China Issues New Cybersecurity Law to Protect Children

5 Ways for Companies to Limit GDPR Penalties

UK Regulator Imposes Two Substantial Fines for GDPR Data Breaches

Endnotes

[1] GDPR, Article 4(12): "…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised. disclosure of, or access to, personal data transmitted, stored or otherwise processed."