Hong Kong's Reform of the Personal Data (Privacy) Ordinance (the "PDPO"): Bridging Troubled Waters

Hogan Lovells

21 January 2020

Hong Kong's Reform of the Personal Data (Privacy) Ordinance (the "PDPO"): Bridging Troubled Waters

On Monday 20 January, the Constitutional and Mainland Affairs Bureau ("**CMAB**"), jointly with the Privacy Commissioner for Personal Data ("**PCPD**"), presented a paper outlining topics for review of the PDPO to the members of the Legislative Council Panel on Constitutional Affairs ("**PDPO Review Paper**"). The CMAB and the PCPD are expected to take panel members' feedback on the PDPO Review Paper and undertake further in-depth study of the issues with a view to making specific proposals for legislative reform in due course.

Background and context

The PDPO stands as one of the Asia-Pacific region's longest standing comprehensive data protection laws. Enacted in 1995, the PDPO has only had one substantial set of reforms since, the principal reform being the introduction in 2013 of new direct marketing controls. It goes without saying that the data protection regulatory landscape, both globally and regionally, has changed significantly since then. The specific proposals discussed in the PDPO Review Paper target a few key areas of reform which would do much to bring Hong Kong's data protection law closer to international norms. The PDPO Review Paper makes specific reference to international legislative developments such as the European Union's General Data Protection Regulation ("**GDPR**"), as well as legislative developments in Australia, Canada, New Zealand and Singapore.

Keeping pace with international developments is, however, only part of the agenda. Equally important is the PDPO Review Paper's focus on Hong Kong's particular challenge with "doxxing" – the unauthorized public disclosure of personal information with the intent to intimidate or encourage acts of vigilantism. Described by constitutional affairs minister Patrick Nip Tak-kuen as the weaponization of personal data, doxxing became a widely used tactic during Hong Kong's recent political unrest, with the PCPD reporting that his office received close to 5,000 complaints and enquiries from individuals who report being the victims of doxxing.

In this context, the review of the PDPO is a critical area of legislative focus for Hong Kong, reflecting both the importance of strong data protection regulation to Hong Kong's efforts to maintain its status as a leading regional financial hub and to the need to set boundaries for principled political debate.

Proposed Amendments to the PDPO

The PDPO Review Paper focuses on the following areas:

Mandatory Breach Notification

The PDPO does not include a mandatory data breach notification obligation. Data Protection Principle 4 ("**DPP**") 4 of the PDPO requires data users to take all practicable steps to prevent unauthorised or accidental access of personal data, but if this provision is breached, there is no obligation to notify the PCPD or impacted data subjects.

In the PDPO Reform Paper, the CMAB suggests that the introduction of a mandatory breach notification would enable the PCPD to: (a) monitor the handling of data breaches more effectively; and (b) follow up with the data users regarding further actions to mitigate the consequences of such breaches.

The Paper identifies the following as key considerations to the formulation of a mandatory breach notification obligation:

a) **How "personal data breach" should be defined**: the CMAB suggests that this definition could mirror the very broad definition in Article 4(12) of the GDPR, which refers to 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.

b) **The threshold for notification**: the CMAB recommends that a data breach having "a real risk of significant harm" should be reported to the PCPD and to affected data subjects; and is considering: (i) whether the same threshold would apply to notifications to the PCPD and to affected data subjects; and (ii) what factors the data user should take into consideration when determining if the notification threshold has been met.

c) **The timeframe for notification**: the CMAB recommends that: (i) when the data user becomes aware of a data breach, it should notify the PCPD within a specified timeframe; and (ii) the PCPD should be empowered to direct the data user to notify the affected data subjects; and is considering whether a specified investigation/verification period for suspected data breaches should be permitted, before a notification needs to be made.

d) **The method of notification**: the CMAB is considering: (i) allowing various methods for data users to notify the PCPD (including by email, fax or post); and (ii) what information should be provided in the notification, which made include a description of the breach, the cause of the breach, the type and amount of personal data involved, an assessment of the risk of harm, and the remedial actions to be taken by the data user. The PCPD is also proposing to develop templates and guidelines on this notification mechanism process.

Mandatory data breach notification obligations are in force in the EU and Canada, under numerous state laws in the United States of America and in the Asia-Pacific region in Australia, mainland China, Indonesia, South Korea, Taiwan and Thailand. Mandatory breach notification regimes are likely to be introduced in India, New Zealand and Singapore in the near future. As mandatory breach notification requirements have essentially become the norm for comprehensive data protection regimes internationally, it is no surprise that Hong Kong is re-evaluating its current position. The PCPD's investigation of a substantial data breach by Cathay Pacific Airways placed a spotlight locally on the increasingly regulatory of data breach incidents. Incidents such as these provide ample evidence that mandatory data breach notification obligations would serve as a means of achieving better data protection compliance and enabling data subjects to take steps protect themselves from the consequences of a breach.

The key practical challenges for implementing an effective breach notification obligation include the issues noted by the CMAB in the PDPO Review Paper. There is a legitimate concern that fixing the threshold for notification too low would result in "notification fatigue", whereby the PCPD's scarce resources could be spread too thin responding to breaches which pose no practical risk of harm, and so do little to advance the cause of data protection. Here the approach taken in the EU, where the notification threshold was not specifically linked to any risk of actual harm to impacted data subjects, may provide important lessons learned. In the wake of the introduction of the GDPR, the UK deputy information commissioner, overwhelmed by the sheer volume of notifications, made a plea to businesses to not over report. Setting a clear materiality threshold for notification would better advance the aims of breach notification, allowing authorities and data subjects to focus on the incidents that matter. Clear guidance on the notification threshold will also be key so as to ensure efficient compliance by organizations seeking to comply with the law.

Similarly, the timeframe required for notification also has critical practical importance. In most data breach scenarios, it takes time for the organization to gather information to assess and contain the breach. Premature notifications add to the risk of

"notification fatigue" and increase the administrative burden for the PCPD. Fixing a specific timeframe for notification brings clarity to the obligation, but may not achieve the obligation's objective.

Data Retention

DPP2 of the PDPO requires data users to take all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose. In line with other data protection laws internationally, DPP2, however, does not specify when such personal data is "no longer necessary".

In light of the diverse nature of different organisations and their differing personal data practices, the CMAB considers that it is, in practical terms, inappropriate to mandate uniform retention periods for different categories of personal data. Accordingly, the CMAB recommends amending the PDPO to require data users to develop clear personal data retention policies, which would cover, among other things: (a) the maximum retention periods for different types of personal data; (b) the legal requirements that may affect those retention periods; and (c) how those retention periods are calculated.

At this stage, then, the CMAB's proposal does not appear to be to prescribe specific retention periods for retaining personal data by regulation, but instead to impose an accountability requirement on data users to assess their personal data holdings and formulate data retention procedures directed at ensuring that DPP2 is complied with in substance.

Fines and Sanctions

At present, fines under the PDPO are set at Level 3 (HK$10,000), Level 5 (HK$50,000) and Level 6 (HK$100,000) of the statutory guidelines. The PCPD may issue an enforcement notice requiring a data user to remediate its breach of the DPPs. Breach of an enforcement notice may result in a Level 5 fine and imprisonment for two years on first conviction.

To reflect the severity of the offences and to improve the deterrent effect of the PDPO, the CMAB is considering increases to these fines. The CMAB notes that data protection authorities in other jurisdictions may issue administrative fines for data protection-related breaches, which the CMAB is also considering introducing.

In particular, the CMAB is considering the following issues in relation to the such administrative fines: (a) the threshold for imposing such fines; (b) the level of those administrative fines, which may be linked to the data user's annual turnover; and (c) the mechanism for imposing such fine, including what information would need to be set out in the administrative fine notice.

It goes without saying that the fines being assessed under the EU GDPR have been a game-changer for organizational focus on data protection compliance. Fines under the GDPR may reach up to four per cent of an organization's world-wide turnover and this has, in many cases, led to a substantial increase in organizations' budgeting for data protection compliance work. There is a widespread perception that the current levels of fines under the PDPO are well within the cost of doing business, except for in relation to the smallest of businesses, and so the risk of a fine does not serve as an effective deterrent. While an increase in the potential fines appears to be long overdue, it will be important, however, to ensure that the potential scale and the approach to the administration of fines be structured in such a way that preserves the important role that the PCPD has in guiding with organizations to advance compliance. The PCPD is constitutionally an independent authority, and it has a well-deserved reputation for working constructively with organizations to advance PDPO compliance in fact.

Regulation of Data Processors

At present, the PDPO only regulates data users - organizations that control the collection, holding, processing or use of personal data. Data processors – organizations processing personal data on behalf of data users – have no obligations under the PDPO. The PDPO does require a data user to ensure that its data processors adopt measures to protect personal data, but CMAB suggests that this is inadequate. The absence of any direct regulation may result in data processors neglecting the importance of protecting personal data.

In the PDPO Review Paper, the CMAB refers to the position adopted by overseas regulatory authorities, many of which impose obligations directly on data processors.

The complexity of modern data processing arrangements, and the sheer volume of personal data that organizations now process through cloud services and other third party data processing arrangements, has resulted in a shift towards the regulation of data processors under data protection laws in many jurisdictions. To leave data processors out of the compliance matrix leaves a critical gap.

There are, however, a number of important practical considerations to bear in mind. In many cases, data processors will have little or no awareness of the nature of the personal data they process on data users' behalf and whether or not, for example, the data has been collected in a compliant manner. To impose the full set of data protection compliance obligations on data processors would introduce a compliance cost which, in many cases, will not be appropriate to the commercial realities of the data processing arrangements, which focus on cost-effective, efficient and secure data storage and processing. Data processing obligations would be best focused on the compliance risk areas that data processors can meaningfully control, such as complying with contracted data security requirements, ensuring secure transfer and disposal of personal data and making data breach notifications where they are known to the processor.

Definition of Personal Data

"Personal data" under the PDPO is defined by reference to information that relates to an "identified" natural person. The CMAB is considering expanding this definition to include data that relates to an "identifiable" natural person. The PDPO Review Paper does not go into detail as to the basis for review other than to refer to the use of tracking and data analytics technology as a justification for the change. The practical context alluded to is that "big data" analytics can involve processing of large datasets of information that do not include the specific identity of any of the individuals concerned. These datasets may readily be combined with publicly available information to establish the identity of the data subject, raising data protection concerns.

Noting that part (b) of the definition of "personal data" under the PDPO requires that data will only be personal data if it is data "from which it is practicable for the identity of the individual to be directly or indirectly ascertained" [emphasis added], there is already some implication that the PDPO regulates the linking of non-personally identifiable information to personal data. Clarification may well be useful, but the language will need to be carefully considered. The boundary between, for example, the processing of personal data and the beneficial use of data that has been subject to appropriate anonymization should be carefully maintained.

Regulating the disclosure of Personal Data relating to other Data Subjects

The final area of reform highlighted in the PDPO Review Paper is consideration of whether or not the PDPO should be amended to address the "doxxing" phenomenon that has plagued Hong Kong in recent months.

The PDPO Review Paper notes that as at 31 December 2019, the PCPD had made over 140 approaches to the operators of websites, online social networks and discussion forums urging them to remove some 2,500 web links apparently relating to doxxing activities. The PCPD reports that close to 70 per cent of the offending links have been removed.

The PDPO Review Paper also notes that the PCPD has requested the platforms concerned to publish warnings stating that doxxing or cyberbullying may violate section 64 of the PDPO, which makes an offence of disclosure of personal data without consent where: (i) the intent is to gain money or cause the data subject financial loss, or (ii) the disclosure has the effect of causing psychological harm.

The PDPO Review Paper reports that as of 31 December 2019, eight persons had been arrested by the police on charges relating to this provision.

At present, the Hong Kong Government is considering how the PDPO may be amended to address doxxing more directly. Proposals under consideration include legislative changes to address doxxing specifically and conferring statutory powers on the PCPD to require the removal of doxxing-related content from social media platforms or websites and to carry out criminal investigations and prosecutions.

Conclusions

The PDPO Review Paper sets out some important proposals for modernising the PDPO, including by making changes that have been widely adopted internationally. At the same time, these issues involve critical nuance and merit careful consideration, so as to ensure the changes are implemented in a way that works best to benefit Hong Kong's status as a thriving regional business hub.

By placing the doxxing issue into the basket of reforms, the CAMB has highlighted a very sensitive point of data protection compliance for Hong Kongers. Doxxing is an issue that must be addressed. However, it is clear that this move risks drawing a political debate that is focused as much on Hong Kong's political and social unrest of recent months as on data protection policy. Above all else, the PDPO Review Paper highlights the need for legislative development of the PDPO, targeting key points of reform that Hong Kong would do well to pursue to ensure that its data protection laws are responsive to international regulatory developments and the increasing demands placed on data protection laws by digital economies.

Key Contacts

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Tommy Liu
Senior Associate, Hong Kong
T +852 2840 5072
tommy.liu@hoganlovells.com

Anthony Liu
Registered Foreign Lawyer, Hong Kong
T +852 2840 5613
anthony.liu@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com