A new year, a new privacy law for Hong Kong?

January 2020

On 20 January 2020, following proposals by the Government and the Commissioner for Personal Data (**Privacy Commissioner**), the Legislative Council (**LegCo**) Panel on Constitutional Affairs (**Panel**) met to discuss proposed reforms to the Personal Data (Privacy) Ordinance (Cap 486) (**PDPO**). The proposed reforms are significant and represent an enhancement to the level of personal data protection offered in Hong Kong, although there is still more that could be done.

Background

In March 2019, we published a Briefing stating that factors such as the European Union's General Data Protection Regulation (**GDPR**) and comments made by the Privacy Commissioner could lead to reform of the PDPO. Following recent proposals for reform and subsequent discussion in LegCo, it appears that 2020 and the Year of the Rat may represent the beginning of a new day for privacy law in Hong Kong.

The PDPO came into force in 1996 and was amended in 2012. Following major reforms in privacy law around the world in recent years, most notably the GDPR, a revamp of the PDPO is, arguably, overdue. An important driver behind the proposed reforms is the constantly changing landscape of data privacy, largely driven by rapidly evolving technologies and, more recently, the concerns over doxxing. In the paper prepared by the Government and submitted to the Panel for its discussion on 20 January 2020 (**Proposals**)[1], the Government identified that incidents of data breaches are now mostly related to digital platforms and data security – and that their frequency has increased. As such, the adequacy of the PDPO (and the Privacy Commissioner's powers to enforce it) has come under increased scrutiny.

In this Briefing, we consider the Proposals and other possible areas for reform.

The proposed reforms

The Proposals cover six main areas:

1. **Definition of personal data**: The Proposals consider that the current wide use of tracking and data analytics technology justifies expanding the PDPO definition of personal data to cover information relating to "*identifiable*" natural persons rather than simply "*identified*" natural persons. One effect of the proposed change would be that the contents of a set of data which, taken alone would not render a person

[1] https://www.legco.gov.hk/yr19-20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf

identifiable, would be personal data if the contents of the set of data could be combined with other information in order to identify data subjects. Such an amendment is consistent with recent global reforms.

2. **Regulation of data processors**: This is one of the areas of most impact introduced by the GDPR. The Proposals state that regulating data processors will not only strengthen protection for individuals, but also result in a fairer sharing of responsibilities between data users and data processors. The Government has drawn on overseas equivalents to the PDPO and intends to focus on direct regulation of data processors by imposing legal obligations on them or their sub-contractors. Such obligations will be imposed by, for example, being required to be directly accountable for personal data retention and security, and to notify the Privacy Commissioner and the data user on becoming aware of any data breach.

3. **Mandatory breach notifications**: At present, the PDPO does not require data users to notify the Privacy Commissioner or data subjects of a data breach. Such notifications are made on a voluntary basis. The Proposals include a requirement that a data breach carrying a "*real risk of significant harm*" must be notified to the Privacy Commissioner and affected data subjects as soon as practicable and, in any event, within five days. It is proposed that the new PDPO definition of data breach will be similar to that in the GDPR. It will be important to achieve clarity on the definition of data breach and the meaning of "*real risk of significant harm*" in order to avoid the over-notification of data breaches which has been seen since the introduction of the GDPR.

4. **Data retention periods**: While the PDPO requires data users to take all practicable steps to ensure that personal data is not kept longer than necessary to fulfil the purpose for which it was collected, it does not specify when the period of 'necessity' expires. While acknowledging that a uniform retention period may be inappropriate because of the unique needs of different organisations and the sectors in which they operate, the Proposals suggest amending the PDPO to require data users to formulate a clear retention policy which specifies a retention period for the personal data collected.

5. **Sanctions**: The Government proposes to explore the feasibility of introducing direct administrative fines to remedy the fact that the PDPO contains no such direct administrative powers (presently any fines can only be imposed by the Privacy Commissioner following the issuing of an enforcement notice). In particular, the Proposals will look at introducing an administrative fine linked to the annual turnover of the data user, and the possibility of classifying data users of difference scales according to their turnovers to match with different levels of administrative fines. Relevant factors when assessing the level of fine might include: (i) the data compromised; (ii) the severity of the data breach; (iii) the data user's intent and attitude; (iv) any remedial action taken; and (v) the data user's track record. Such fines will be issued by the Privacy Commissioner and the data user will be able to make representations and ultimately appeal to the Administrative Appeals Board. The level of fines handed down under the GDPR has been one of the most significant talking points since it became effective. Such fines are an important deterrent, but equally important are alternative enforcement tools (such as monitoring and reporting), so it will be interesting to see what other powers are given to the Privacy Commissioner.

6. **Regulation of the disclosure of personal data of other data subjects**: This part of the Proposals stands apart from the others because it is driven by local factors, in particular incidents of 'doxxing'. While

tackling doxxing is part of wider government studies, the Proposals include a suggestion to empower the Privacy Commissioner to request the removal of doxxing content from social media platforms or websites, in addition to powers of investigation and prosecution.

Comment

The Proposals represent the most significant reform of the PDPO since its enactment. In his Annual Report for 2018 – 2019 [2] (which was published on 17 January 2020), the Privacy Commissioner described data as "*the new gold or oil of this era*" and stated that "*a comprehensive review of the [PDPO is] indispensable*" not least because "*[d]ata protection policies, regulations and practices are invariably lagging behind ICT developments*". Our previous Briefing also included reference to the Privacy Commissioner's concept of 'data ethics' and the need to "*work with the government authorities to review the current legal framework…with a view to enhancing the deterrent effect of sanctions as appropriate*".

As such, the Proposals are generally unsurprising. For example, the introduction of a mandatory breach notification scheme was one of the areas we suggested ought to be reformed in our previous Briefing. Moreover, Hong Kong organisations appear to appreciate the importance of notifying breaches and working with the Privacy Commissioner to learn from the breach. In his Annual Report, the Privacy Commissioner noted that 113 voluntary breach notifications had been made to his office during the year under review and that his office has "*worked hand in hand with the relevant organisations and engaged them to take immediate remedial actions to contain the possible damage to the attacked individuals…[and] put forward steps to re-establish their consumers' trust*". However, the Privacy Commissioner underlined the case for reform by noting that the number of voluntary notifications "*did not reflect the complexity and severity of the nature of the incidents, or the large number of individuals affected, not to mention the substantive technical and legal issues advanced in defence by the professional teams*".

It is also welcome that the Proposals draw on reform from other jurisdictions and regions. For many organisations, compliance with data privacy laws can be challenging because of the fact that they operate in multiple jurisdictions, each with different requirements. It follows that a degree of consistency will aid compliance. However, it is also important to note that local data privacy laws should be tailored to local issues – hence the Proposals' inclusion of reforms designed to prevent and tackle doxxing.

The Proposals are silent on other areas where reform might be welcome. For example:

- **Sensitive personal data**: While there is a proposal to expand the definition of personal data, the Proposals are silent in relation to sensitive personal data (a concept which is not recognised by the PDPO). Under the GDPR, such data attracts a higher degree of protection and includes, for example, data such as genetic data, biometric data, data concerning sexual orientation or revealing political opinions, religious or philosophical beliefs. It is important that such data is protected in a world which the Privacy Commissioner, in his Annual Report, describes as one where challenges to data protection

2 https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/annualreport2019.html

are increasingly acute as a result of the rise of digital services and data technologies such as social media, big data analytics and artificial intelligence. Much of the personal data processed in those situations is 'sensitive' and there are strong arguments for its enhanced protection.

- **International transfers of personal data**: This was one of the key areas identified in our previous Briefing. While section 33 of the PDPO provides for a regime to regulate the transfer of personal data outside Hong Kong, it is yet to be enacted. As organisations grow and processing activities become more global in nature, an increase in the cross-border transfer of personal data is inevitable (and is already occurring). This is particularly relevant to Hong Kong as a leading global financial centre and a jurisdiction where personal data might reasonably be expected to be transferred overseas.

- **The principle of accountability**: The GDPR introduced into law the principle of accountability, whereby organisations are not only required to comply with the GDPR, but must also be able to demonstrate compliance. In his Annual Report, the Privacy Commissioner noted that the accountability principle is yet to be provided for in the PDPO but that organisations in Hong Kong should be well positioned to adopt a proactive approach to data management. We are yet to see if this concept of accountability will be introduced into law.

What next?

In terms of timing, the Proposals could be reflected in a draft Bill more quickly than might otherwise be the case. In the LegCo meeting on 20 January 2020, Patrick Nip Tak-keun, the Secretary for Constitutional and Mainland Affairs suggested that the government might not follow its usual route of a three to six month public consultation period on the Proposals. Nevertheless, it is likely that it will be many months before any reform of the PDPO is enacted into law.

Conclusion

While the Proposals are a welcome and, arguably, overdue platform for reform of the PDPO to reflect global trends and personal data challenges, their effectiveness will depend on how they are framed in the draft legislation. Further, the Proposals are lacking in some key areas and it will likely be some time before they become law. In any event, in addition to monitoring the local situation, organisations in Hong Kong will still need to keep pace with global developments and be aware of how they impact their ability to do business with organisations outside Hong Kong.

If you would like to discuss any of the contents of this Briefing, please do not hesitate to contact those listed below.

Wynne Mok
Partner
T +852 2901 7201
E wynne.mok@slaughterandmay.com

Kevin Warburton
Counsel
T +852 2901 7331
E kevin.warburton@slaughterandmay.com

Jason Cheng
Associate
T +852 2901 7211
E jason.cheng@slaughterandmay.com

Dated January 2020