BCLP. Client Intelligent

Insights

PART 1 OF 6 - IMPORTANT CHANGES TO HK DATA PROTECTION LAW UNDER WAY

Sep 24, 2020

SUMMARY

The Hong Kong Government currently is reviewing and putting forward possible amendments to the Personal Data (Privacy) Ordinance ("PDPO") with a view to strengthening the protection for personal data. Multiple areas of the data protection law are expected to be changed, the better to align with the standards set by the General Data Protection Regulation ("GDPR") of the European Union. Businesses should begin reviewing their internal policies to prepare for the upcoming wave of amendments.

The Government's review of the PDPO

At present, the PDPO does not require data users to notify data breaches, either to the Privacy Commissioner for Personal Data ("PCPD") or to the data subjects concerned. To date, reporting to the PCPD has been voluntary and only was encouraged as a matter of good practice. Following recent incidents of personal data privacy breaches (for example, the data breach incident involving Cathay Pacific and Hong Kong Dragon Airlines (as it then was) in 2018), public concerns about the adequacy of the PDPO began to find voice.

On 20 January 2020, the Hong Kong Government proposed a series of amendments to the PDPO with a view to strengthening the protection for personal data . The proposed amendments include the following significant aspects:-

(i) Introduction of a mandatory data breach notification mechanism for data users to notify the PCPD and data subjects within a prescribed timeframe;
(ii) Requirement for data users to formulate a clear data retention policy which specifies the retention period for personal data collected;
(iii) Imposition of administrative fines for contravention of the PDPO;
(iv) Direct regulation of data processors by imposing legal obligations on them or sub-contractors;

(v) Widening of the definition of “personal data” to cover information relating to an “identifiable” natural person, instead of only an “identified” person; and
(vi) Regulation of disclosure of personal data to cover doxing.

The proposals made by the Government in January 2020 in relation to the above areas were not very detailed, as the Government was desirous of seeking input from various stakeholders. However, these initial proposals are clear enough to enable businesses to undertake an internal review of their policies to prepare for the upcoming changes.

This present blog will be the first of a series, with each blog in the series considering a different one of the six significant proposed amendments outlined above.

Accordingly, this present blog will consider the introduction of a mandatory data breach notification requirement.

The introduction of this notification requirement is expected to be one of the most significant changes.

Data breach notification – HK’s current position

A data breach means a breach of data security of personal data held by a data user, exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

As mentioned above, at present in Hong Kong, there is no statutory requirement for a data user to notify the PCPD or the data subjects in the event of a data breach. The PCPD has from time to time published Guidance Notes on the handling of data breaches. The PCPD has advised that breach notifications should be given as a matter of recommended practice. A Data Breach Notification Form is published by the PCPD to assist and facilitate reporting by data users.

Under the current regime, data users in breach of data security may walk away unsanctioned even if they choose not to notify or choose to notify after a long delay. In fact, taking the example of Cathay Pacific’s data breach incident in 2018, the PCPD found that no law was contravened by Cathay Pacific and Hong Kong Dragon Airlines in connection with the late notification of the breach, even though the data breach concerned approximately 9.4 million passengers worldwide.

When compared to the standard of practice set by the GDPR in respect of breach notification, the Hong Kong voluntary notification regime is argued by some advocated to be less than satisfactory. Under the GDPR, businesses must notify the relevant authority in the EU without undue delay, and where feasible, no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, businesses must (with some exceptions) notify the data subjects without undue delay, and do so using plain and clear language.

It is argued by many that it is time Hong Kong took steps to establish a mandatory data breach notification mechanism to align with international standards.

Proposed amendments regarding mandatory breach notification

The Government has proposed to introduce the following amendments with a view to establishing a mandatory data breach notification mechanism:

1. Definition of “personal data breach” to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This amendment will adopt the same definition used in the GDPR. Note that “accidental” breaches also would be notifiable under this definition.

This would mean that businesses will need to ensure that they have policies in place to ensure that even inadvertent mishandling of data by their employees is reported internally to its data officer for the purpose of determining whether notification is needed.

2. Notification threshold: a data breach having “a real risk of significant harm” would be notifiable to both the PCPD and the affected data subjects.

Note that this is different from the position under the GDOR, where two different notification thresholds are used when determining whether a breach is notifiable to the authority and the data subjects. Under the GDPR, a data breach is notifiable to the supervisory authority unless it unlikely will result in a risk to the rights and freedoms of natural persons. However, a breach does not have to be notified to the affected data subjects unless it is likely to result in a high risk to the rights and freedoms of natural persons.

The single notification threshold of a “real risk of significant harm”, as is being proposed for Hong Kong, appears to be more akin to the higher threshold that the GDPR has for notification to data subjects. This means that the PCPD would not mandated to oversee relatively trivial incidents of breach. The resources of both the PCPD and data users may be focused on dealing with the more significant breaches.

Once we know what factors for determining whether a breach has reached that threshold appear in the final enactment, data users / businesses will need to devise and implement appropriate action plans for when a data breach is detected.

3. Notification timeframe: a data breach would have to be notified to the PCPD as soon as practicable after awareness of the breach and, under all circumstances, within five business days. The PCPD would then have the power to direct the data user to notify its data users.

While the proposed Hong Kong timeframe is slightly more relaxed than that under the GDPR, the proposed timeframe nonetheless is rather a tight timeframe for Hong Kong data users, especially if they do not already have an existing crisis management system or action plan to cope with the even shorter notification timeframe under the GDPR. Though the 72-hour window prescribed under the GDPR is an even tighter timeframe, that timeframe has to be complied with only "where feasible" and not "under all circumstances".

The Government's proposal of five business days under all circumstances is a challenging timeframe. Businesses should begin devising crisis management systems or action plans to enable themselves to respond quickly enough according to the new notification requirements.

After breaches have been reported to the PCPD, we expect that some time would be needed by the PCPD and the data users to investigate further and respond to queries before the PCPD would make a direction for data subjects to be notified. In any event, businesses will be expected to act swiftly in order to comply with the mandatory notification requirements.

4. Mode of notification: notifications to the PCPD would need to be made in writing by email, fax or post with specified information to be given according to templates to be provided by the PCPD.

The kinds of information proposed to be notified are very similar to those required under the GDPR. The degree of complexity of the details to be given in the notification very much affects a data user's ability to comply with the notification timeframe. Templates and guidelines issued by the PCPD should assist data users in reporting breaches in time.

How businesses should brace for change

With the ever-changing technological advancement and widespread use of internet and mobile communications, it remains a sad reality that the security of personal data held by businesses is prone to compromise.

To prepare for the upcoming amendments to the PDPO, in particular the introduction of mandatory notification requirements, businesses should undertake a timely review of their risk profile and put in place a response plan appropriate to the level of risks they face in the event of a data breach. A business may start by appointing a data protection officer dedicated to overseeing data privacy issues, responding to data compromises and handling investigations related to data breaches. External legal advice immediately should be sought when need arises so as to cope with the challenging notification timeframe.

As noted above, this present blog is the first of a series. We will deal in future blogs with the remaining five significant proposed amendments to the data privacy regime in Hong Kong, being the five matters identified in items (ii) to (vi) at the start of this present blog, above.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
