BCLP. Client Intelligent

Insights

PART 2 OF 6 - AMENDMENTS TO HONG KONG DATA PROTECTION LAW REGARDING DATA RETENTION POLICY: REQUIREMENT FOR A CLEARLY STATED RETENTION PERIOD

Sep 28, 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. One of the amendments proposed is to require data users to formulate a clear data retention policy which specifies a retention period for the personal data collected. This article sets out the background to this proposed amendment and what businesses need to know.

This post is the second one in the series of six articles in which we discuss the proposed amendments to the data protection regime in Hong Kong.

This post deals with that part of the proposed amendments that will require the implementation of a clearly stated retention period for personal data.

See link here to the first article for an overview of the six proposed amendments and a discussion of the proposed introduction of a mandatory data breach notification mechanism.

Data retention period – HK's current position and why a change is needed

Under the current PDPO, data users are required to take all practicable steps to ensure that personal data is not kept longer than is necessary for fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used[1]. The current regime, therefore, provides little specification or guidance as to when such personal data is no longer necessary for the fulfilment of its purpose. No maximum or uniform retention period currently is prescribed by the Hong Kong law.

The lack of a mandatory uniform period for retention of data is not necessarily a deficiency in the current data protection law. In fact, the Hong Kong Government recognises the need for some degree of flexibility to suit the vastly different needs and business nature that data users may have. A law which mandates a uniform retention period for all data users will not, it is argued, be appropriate or feasible given the diverse and unique needs of different data users.

Other jurisdictions also have adopted a similar "flexible" approach, with no definite retention period for personal data prescribed in their data protection laws. The relevant laws in Australia, Canada, the EU, New Zealand and Singapore all require data users to keep personal data for not longer than is required or necessary.

The reality is that, without further guidance provided in statute, the likely situation is that not all data users in Hong Kong have their own data retention policy which spells out how long personal data is to be kept. Although a person (a data subject) has the right to ascertain from a data user's policies and practices in relation to personal data[2], if a data user does not have a set of clear data retention policies, it appears that not much protection is afforded in fact to the data subject even if they take steps to enquire. The answer that the data subject is likely to receive simply might be that their data will be retained no longer than what the statute allows.

The failure by data users to delete personal data, which should have been eradicated after the exhausting of its intended purposes with the data user, poses unnecessary data privacy risks. This is perhaps the primary reason why the Hong Kong Government now proposes to tighten the regulation by requiring data users to formulate a clear retention policy.

The proposed amendments

The proposed requirement for data users to formulate a clear retention policy mainly targets the specification of a data retention period. The retention policy formulated by data users should include the following aspects:

1. The maximum retention periods for different categories of personal data.

A data user may of course collect different kinds of personal data for different purposes. Some data obtained may be more sensitive than others. For example, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life and data concerning a natural person's sexual orientation, all belong to special categories of personal data that are afforded greater protection under the GDPR.

The longer the data is retained, the higher the risk for a data breach and the more severe the impact. With this principle in mind, businesses should consider what different categories of personal data currently are or would be processed by them, and accordingly come up with retention periods suitable for their business needs.

2. The legal requirements which may affect the designated retention periods.

Specific legal regimes and requirements need to be taken into account. Examples include:

- Employment-related data held about a job applicant should have a maximum retention period of two years from the date of rejecting the applicant[3]. This is to reflect the two-year limitation period for anti-discrimination proceedings that unsuccessful job applicants may have.
- Employment data held about an employee should be kept for the whole duration of his employment plus a maximum of seven years after the employee leaves employment[4].
- Business transaction records and accounting records (including payroll records) are required to be kept for at least seven years for tax purposes[5]. There also are specific retention period requirements for certain professions. For example, solicitors are required to preserve for at least six years all books, accounts and records kept by them[6]. Solicitors' files on conveyancing, tenancy and criminal cases all have different minimum retention periods as recommended by the Law Society.

Given such varying legal requirements for various businesses and activities, it therefore would be problematic to develop and impose one hard and fast rule which readily can be imposed by the Hong Kong Government as being on universal application with regard to data retention period. Businesses or data users therefore must formulate their own retention policies with the relevant legal requirements in mind. Of necessity, these will need to be business–specific.

3. How the retention period is counted.

Policies formulated by data users will have to include the starting point from which the designated retention period for that category of personal data shall begin to count. For example, the retention period may start to be counted upon collection of that data, upon cessation of business of the data user, or upon the data user's relationship with the data subjects (if applicable).

Apart from the requirement for data users to formulate a clear retention policy, the Hong Kong Government also is considering expressly requiring data users to ensure that data subjects are informed clearly of the details of such data retention policy and that it will be executed effectively. Businesses will have to disclose to data subjects how long their data would be kept. Whether such information has to be provided upfront to the data subjects or upon enquiry still is a matter to be decided.

Take-away points for businesses

In the proposed changes to the PDPO, businesses / data users will have to formulate a clear data retention policy which specifies the data retention period(s) for personal data collected. At present, the Hong Kong Government has not indicated that any mandatory uniform period for retention would be imposed on data users. Businesses will have to decide on retention period(s) which are suitable for their business needs as well as compliant with legal requirements.

---

[1] Data Protection Principle 2 of the PDPO.

[2] Data Protection Principle 5(a) of the PDPO.

[3] Paragraph 2.10 of the Code of Practice on Human Resource Management (April 2016 edition) issued by the PCPD at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

[4] Paragraph 4.2.3 of the Code of Practice on Human Resource Management (April 2016 edition) issued by the PCPD at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

[5] Section 51C of the Inland Revenue Ordinance

[6] Rule 10(6) of the Solicitors' Accounts Rules

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
