BCLP. Client Intelligent

Insights

PART 4 OF 6: AMENDMENTS TO HONG KONG DATA PROTECTION LAW TO REGULATE DATA PROCESSORS

Jul 15, 2021

SUMMARY

In the upcoming round of amendments to the PDPO, Hong Kong likely will follow the footsteps of overseas regulatory authorities to introduce measures that regulate data processors directly.

This post is the fourth 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 to the Personal Data (Privacy) Ordinance ("PDPO") that are aimed at regulating data processors.

See links below for our previous articles on the proposed amendments:

- Part 1 of 6: our first article set out an overview of the six proposed amendments and included a discussion of the proposed introduction of a mandatory data breach notification mechanism.
- Part 2 of 6: our second article on the requirement for the formulation of a clear data retention policy.
- Part 3 of 6: our third article on the imposition of administrative penalties.

Introduction

Many data protection laws in the international community draw a distinction between (a) an entity which controls and defines the policy for the use of personal data collected and (b) an entity which merely processes personal data on behalf of the controller. In Hong Kong, under the PDPO, the former is referred to as the "data user" while the latter is called the "data processor".

Traditionally, data users have been subject to the most stringent regulation. Data processors, on the other hand, mostly handle data as sub-contractors or agents and do not use data for their own

purposes. Most regulators have chosen not to impose heavy legal restrictions on data processors.

When considering what potential amendments are to be made to the PDPO, the Hong Kong government observed that the outsourcing and sub-contracting of data processing activities by data users to service providers are becoming increasingly common. As a result, changes to the current PDPO have been proposed to reflect this trend.

Hong Kong's current position and its inadequacies

Under the current PDPO, the obligation to ensure the safety of personal data rests directly upon data users. There is no specific legal requirement or restriction which targets data processors directly. Under DPP 2(3) and 4(2), if a data user decides to engage a data processor to process data on its behalf, the data user must adopt contractual or other means to ensure the proper safekeeping and processing of the personal data. It appears that the burden of ensuring a properly drafted data processing contract is in place and the enforcement of any breach by data processors rest upon data users.

There is no provision or mechanism under the PDPO which allows the adequacy of data protection under data processing contracts to be checked and verified. The Hong Kong government believes that the absence of direct regulatory provisions in the PDPO which target data processors possibly causes data processors to be less cautious about the importance of preventing data breaches.

Examples from overseas regulatory bodies

Among the countries or overseas regulatory bodies which draw a distinction between data users and data processors, some of them recognise the specific need for data processors to be regulated by and subject to the law.

The Hong Kong government has indicated that it intends to draw reference from other countries which regulate data processors directly. Below is a brief account of some of the recent approaches taken or which will be taken by data protection regulatory bodies outside Hong Kong:

General Data Protection Regulation ("GDPR") of the EU

The GDPR distinguishes between a "data controller" and a "data processor". Article 28 sets out with more particularity the data protection provisions which need to appear in data processing contracts. Specifically, substantive provisions in relation to documented instruction, confidentiality, processor security, sub-contracting authorisation, flow down obligations, liability, response to data subjects, assistance to the data controller, deletion or return of data, audit rights and cross-border transfers have to be included in data processing contracts. The GDPR also imposes restrictions on the engagement of a further sub-processor by the data processor.

Importantly, if the data processor acts in breach of the GDPR by determining the purposes and means of processing, it will be regarded as a data "controller" for the purpose of that processing

activity and as a result be subject to the stringent rules applicable to data controllers in that regard.

California Consumer Privacy Act ("CCPA")

The CCPA refers generally to data processors as "service providers". The CCPA does not contain as many prescriptive provisions as the GDPR in relation to what data processing contracts must contain. It prohibits the retention, use and disclosure of personal information for any purpose other than for the purpose of performing the contract. It also requires service providers to flow down all such obligations to sub-contractors or sub-processors.

Singapore's Personal Data Protection Act ("PDPA")

An organisation which processes personal data on behalf of another organisation is called a "data intermediary". Data intermediaries are not subject to most of the regulatory provisions under the PDPA, except for sections 24 and 25 of the PDPA which relate to the protection and retention of personal data.

China's draft Personal Information Protection Law ("PIPL")

The PIPL has not yet formally been enacted. The latest draft PIPL uses the term "data handler" to refer to what we commonly understand as data users or data controllers. Under Article 22, if personal data needs to be transmitted to a third party, such third party must process data in accordance with its agreement with the data handler, the agreed purpose and manner of data processing. Where the agreement with the data handler is terminated or in any way rendered ineffective, data transmitted needs to be returned or destroyed. Also, the third party is prohibited from further transferring data to a sub-processor without the data handler's consent.

The proposed amendments in Hong Kong

The approach proposed by the Hong Kong government as to the regulation of data processors appears to be similar to the Singaporean approach, i.e. that some legal provisions such as those in relation to the retention and security of data may be expanded and extended to cover data processors.

In addition to the retention and security, the Hong Kong government also is considering to introduce a mandatory requirement for data processors to notify breaches, either to the PCPD or the relevant data user.

From information available to the public at present, there is not much clarity as to what the actual scope of the amendment will be. However, it is anticipated that the upcoming amendment likely will bring the current PDPO in line with other equivalent legislation by introducing direct obligations on data retention, data protection and breach notification.

Final comment

The introduction of direct provisions to regulate data processors will enhance Hong Kong's data protection regime as a whole. A well-thought-out set of provisions which target data processors hopefully will help define a fairer share of responsibility between data users and data processors.

RELATED PRACTICE AREAS

- Data Privacy & Security
- General Data Protection Regulation

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450