iBDG Big Data Governance Launch Event

Monday, 5 August 2019

Hong Kong Convention and Exhibition Centre

Keynote Speech Topic:

"Linkage of Data Governance Principles and PDPO"

Stephen Kai-yi WONG, Barrister
Privacy Commissioner for Personal Data, Hong Kong, China

Secretary Yang, Allen, Alex, Vincent, Ladies and Gentleman,

1. It is my distinct privilege to be able to join you at this significant inauguration launching the Big Data Governance Principles. As repeatedly acknowledged by our national leaders, Hong Kong has a number of "unique and irreplaceable attributes" that lead to its success and prosperity. Among those attributes, "free flow of information", "protection of right to personal data privacy" and "English as one of the official languages" are key attributes of Hong Kong as a regional data centre hub. These attributes will be conducive to performing the international functions of Hong Kong as international financial centre, innovative centre and dispute resolution centre.

2. The idea to develop Hong Kong into a regional data hub within the Greater Bay Area is not new. But the work of iBDG is ground-breaking and is a positive step facilitating and moving Hong Kong to become a regional data hub. The launch of the Big Data Governance Principles today represents a significant milestone in this journey.

3. I offer my warmest congratulations to iBDG for its leadership and efforts in the work to develop a set of data governance principles. Some may ask what the linkage is between these principles and the Personal Data (Privacy) Ordinance ("PDPO"). That is a legitimate question and I will turn to that.

Developing Hong Kong as a data centre hub

4. Thanks to the "one country, two systems" principle, Hong Kong has maintained its internationally compatible social, economic, legal and judicial systems. These well-established systems are cornerstones of maintaining the competitiveness of Hong Kong as an international financial centre and a major international trading and logistics hub.

5. Hong Kong has benefited a lot from the reformed and strong economy of the Mainland for the past few decades. By well positioning the roles of Hong Kong in the recent significant initiatives promulgated by the Central People's Government (in particular the Belt and Road and the Greater Bay Area initiatives), Hong Kong will certainly enjoy more benefits in the future.

6. Hong Kong enjoys free flow of information. Hong Kong SAR Government does not impose restrictions on the setting up and operations of data centres. Free flow of information facilitates the development of a data-driven economy, riding on robust ICT (such as cloud computing, e-business, Internet of Things and logistics). As a result, the demand for data centre services is surging.

7. The right to personal data privacy is a fundamental human right in Hong Kong. Protection of this right provides a conducive and

trustworthy environment for regional data centres to operate. In this regard, the PDPO provides adequate legal protection of personal data that the Mainland and overseas companies would trust.

8. Frequent cross-border flow of data is inevitable for a place to be a data centre hub. World leaders in the recent G20 Summit declared, among other things, that cross-border flow of data generates higher productivity, greater innovation and improved sustainable development, while raising challenges related to privacy, data protection and security. This indicates the importance of having a robust framework to effect cross-border flow of data and at the same time to overcome the entailed challenges.

9. Legislation (like personal data protection laws) would provide such framework. Apart from legislation, commitment (like pledging and certification) as adopted by the scheme underlying the Big Data Governance Principles may also promote cross-border / boundary flow of data.

10. By combining certain requirements under the EU General Data Protection Regulation ("GDPR"), the Cybersecurity Law in the Mainland and ISO standards, the Big Data Governance Principles seek to enhance the data governance practices in Hong Kong to a high standard.

11. Pledging and certification aim to boost confidence of non-Hong

Kong organisations in the Mainland and other jurisdictions in recognizing that a pledged or certified Hong Kong data controller provides requisite level of data protection.

General difference between Big Data Governance Principles and the PDPO

12. It is a great step and start for iBDG to develop the Big Data Governance Principles in promoting data privacy protection. These Principles share some commonalities as well as differences from the PDPO. For example, the Principles have a wider coverage than the PDPO as the Principles concern data of all types, as opposed to just personal data.

Four principles of Big Data Governance Principles

13. iBDG's Big Data Governance Principles comprise the following four principles –

    (a) P1 – data processing principle;

    (b) P2 – personal data breach principle;

    (c) P3 – data transfer principle;

    (d) P4 – continuous improvement principle.

14. Let me share some of my observations by comparing the principles and the PDPO.

P1(data processing principle) and PDPO

15. "Processing" used in Big Data Governance Principles seems to have a wider scope than that in PDPO. iBDG's data processing principle set out rules for both data user and data processor. On the contrary, the PDPO currently does not impose direct regulation on data processors. If a data processor breach relevant requirements under the PDPO (such as retention of personal data under DPP2(3) and security of personal data under DPP4(2)), the liability is borne by the data user who engages the data processor. This is not adequate especially when out-sourcing data activities are common nowadays. Therefore, regulation of data processor would need to be enhanced. In this regard, iBDG shows its foresight to include this data processing principle.

16. iBDG's data processing principle touches upon a few matters similar to those regulated under the PDPO. These matters include data collection, use, transparency, accuracy, retention and security.

Data collection

17. The data processing principle provides, among other things, that data is collected for specified, explicit and legitimate purposes. Similar requirement is laid down in Data Protection Principle ("DPP") 1 of PDPO. That is, DPP1 requires collection of data for a lawful purpose and is necessary for or directly related to the purpose.

18. Apart from this requirement, DPP1 also imposes other requirements in relation to collection of personal data, for example –

(a) data collected must be adequate but not excessive in relation to the purpose;

(b) means of collection must be lawful and fair;

(c) DPP1(3) requires data users to take all practicable steps to notify the data subjects of the purposes for use, the classes of transferees, the rights to request access to and correction of the data, etc.

Data use

19. iBDG's data processing principle operates on similar premise though the drafting is not the same. For example, iBDG's data processing principle also requires that data is not further processed in a manner that is incompatible with the collection purposes. A similar requirement on use of personal data is imposed under DPP3, which provides that personal data must not be used (including disclosed or transferred) by a data user for a new purpose. This requirement however is lifted if data subject gives an express and voluntary consent to the use for a new purpose.

Accuracy and retention of data

20. iBDG's data processing principle also provides that data must be processed with accuracy and storage limitation. Similar areas are

regulated under DPP2 and section 26 of PDPO, namely accuracy, retention and erasure of personal data, and again, the iBDG and PDPO are convergent in spirit though terminology and details differ.

21. Specifically, on accuracy of personal data, DPP2(1) requires data users to take all practicable steps to ensure, among other things, that personal data of data subjects is accurate and that inaccurate personal data is to be rectified or erased.

22. On retention and erasure of personal data, DPP2(2) requires data users to ensure that personal data is not kept longer than is necessary for the collection purpose. Section 26 of the PDPO specifically obligates data user to erase data that is no longer required for the purpose of use. So the provisions of the PDPO are slightly more detailed than the iBDG's data processing principle.

Data security

23. Security of data is also covered under data processing principle. The principle provides that data must be processed lawfully with integrity and confidentiality and the principle also provides that data controller must maintain an organizational governance program/structure that protects data access.

24. Security of personal data is governed under DPP4 of the PDPO. More detailed considerations on protection of personal data against unauthorized or accidental access, processing, erasure, loss or use

are explicitly stipulated in DPP4(1). The considerations include resulting harm, physical location of storage, security measures, measures for ensuring appropriate person to access the data and measures for ensuring secure transmission.

25. The rules laid down in iBDG's data processing principle do provide baseline requirements to give organisations and business enterprises direction for processing data.

P2 (personal data breach principle) and PDPO

26. Data breach notification is an area where adherence to it will be an enhancement as the PDPO does not impose such an obligation on a data user.

27. The personal data breach principle sets out requirements for data breach notification by a data controller incorporated in Hong Kong. We note that these requirements bear similarity with the data breach notification requirements under the EU General Data Protection Regulation ("GDPR"). For example –

    (a) The meaning of "personal data breach" used in Data Governance Principles is the same as that in GDPR (which is defined in Article 4(12) of the GDPR).

    (b) This principle requires data controller to notify supervising authority within 72 hours after being aware of a data breach. Similar requirement is provided for in Article 33(1) of the GDPR.

(c) This principle also provides for the content of notification which includes the nature of personal data breach, likely consequences of personal data breach, measures taken or proposed to be taken. Article 33(3) of the GDPR lists out largely the same content of notification.

(d) Besides, this principle provides for three circumstances under which exemption from notification applies. These circumstances seem to come from those under Article 34(3) of the GDPR.

28. As you may know, Hong Kong currently does not have a mandatory breach notification requirement and this iBDG's principle goes further than our existing PDPO, which is another positive step forward in protecting personal data. Currently, the PCPD encourages data users to report data breach to us on a voluntary basis.

29. There seems to be widespread support in Hong Kong for introducing a mandatory breach notification regime. The personal data breach principle serves as a good reference for organisations and business enterprises.

P4 (continuous improvement principle) and PDPO

30. iBDG's continuous improvement principle lays down the methods to improve data governance practices, that is, adopting data

management principles, conducting annual data governance audit and seeking support from iBDG for unclear scenario. This principle largely relates to the accountability principle that my office, like other data protection authorities in the world, has been advocating.

31. Accountability is the mechanism for assuring data stewardship and protection. Data privacy is no longer a legal compliance issue only, but also business concern which should be addressed by top management as part of its corporate governance, with proper internal policies and procedures put in place to ensure compliance with data protection law.

32. The PDPO does not contain explicit provisions on the accountability principle, although DPP 2 and DPP 4 require a data user to "take all practicable steps" to ensure compliance with data accuracy, data retention and data security requirements.

33. In 2014, the PCPD published the "Best Practice Guide on Privacy Management Programme", which manifested the accountability principle. The privacy management programme ("PMP") encourages data users to shift their paradigm in data protection from compliance to accountability and to embrace data protection as part of their corporate governance. It also encourages data users to apply the PMP as business imperative throughout the organisations. The PMP helps organisations manage compliance with the PDPO and build trust among customers, enterprises and

employees.

34. The continuous improvement principle is thus in line with our thinking behind PMP. We also believe the continuous improvement principle would enhance the awareness of organization to observe the accountability principle in a continuous manner.

P3 (data transfer principle) and PDPO

35. iBDG's data transfer principle provides some general rules on data transfer and the rules concerning cross border/boundary transfer of data are the most notable ones.

36. In Hong Kong, cross-border / boundary transfer of personal data is governed by section 33 of the PDPO, albeit not yet being in operation. Section 33 of the PDPO is intended to prohibit the transfer of personal data to a place outside Hong Kong (i.e. a recipient jurisdiction) unless one of the six specified circumstances is met.

37. In the EU, the GDPR imposes similar restrictions. Personal data located in the EU may only be transferred to those countries outside EU that provide an adequate level of data protection.

38. In the Mainland, the Cybersecurity Law imposes, amongst others, data localisation requirement. Under this requirement, operators of

critical information infrastructure (CII) (such as public communications and information services, energy and transportation) are restricted from transferring personal information and important data to a place outside the boundary of the mainland of China.

39. Obtaining a recognition from other jurisdictions, including the mainland of China that a certified Hong Kong data controller provides adequate level of data protection appears to be the prime objective of the data governance principles. A certification scheme should be one of the means to achieve this objective.

Conclusion – data governance principles as a model for putting a certification scheme in place

40. Certification scheme has become increasingly popular as a legal basis for cross-border data transfer in other jurisdictions. For example, certification has become a legal basis under GDPR of the EU and the Cross-border Privacy Rules ("CBPR") of APEC. A certification scheme focuses on assessment of organisations for complying with adequate data protection standards. Certification can help demonstrate the requisite data protection to businesses, individuals and regulators. This is, in my view, of particular significance in making Hong Kong an electronic dispute resolution centre in the context of the Belt and Road and the Greater Bay Area initiatives.

41. iBDG's data governance principles should be able to set a practicable model for demonstrating how certification scheme could be put in place. I am delighted to see the commendable efforts made by iBDG in developing the data governance principles to form a basis on which cross border / boundary data transfer from the Mainland or overseas in Hong Kong may be effected.

42. Thank you very much.