

**For Discussion**

**15 May 2017**

**The Legislative Council Panel on Constitutional Affairs  
Section 33 of the Personal Data (Privacy) Ordinance**

**Purpose**

This paper briefs Members on section 33 of the Personal Data (Privacy) Ordinance (“PDPO”), which was designed to regulate cross-border transfers of personal data but is yet inoperative, and preliminary findings of a consultancy study on its business impact.

**Section 33 of the PDPO**

2. The PDPO came into force in 1996 with the objective of regulating the use and handling of personal data by data users, which include stipulating that the transfer of personal data to data users or processors in Hong Kong or any other places must comply with various requirements relating to the purpose of use, accuracy, security measures, etc. Section 33 of the PDPO sets out more stringent regulation on the cross-border transfer of personal data. It is provided in section 33(2) that a data user shall not transfer personal data to a place outside Hong Kong unless at least one of the following conditions is met -

(a) The Privacy Commissioner for Personal Data ( “the

Commissioner” ) has, by notice in the Gazette, specified that the place to which the data is to be transferred has law in force which is substantially similar to, or serves the same purposes as, the PDPO;

- (b) The data user has reasonable grounds for believing there is law in force in that place which is substantially similar to, or serves the same purposes as, the PDPO;
- (c) The data subject has given consent in writing to the transfer;
- (d) The user has reasonable grounds for believing that, in all the circumstances of the case, the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; and if it was practicable to obtain such consent, such consent would be given by the data subject;
- (e) The data is exempt from Data Protection Principle 3 by virtue of an exemption under Part 8 of the PDPO; or
- (f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of the PDPO.

3. According to the interpretation of section 33 by the Office of the Privacy Commissioner for Personal Data (“PCPD”), transfers of personal

data between two other places with control of the transfers exercised by data users in Hong Kong are also subject to the requirements set out in section 33(2) as described above.

4. Section 33 has not been brought into force. In fact, prior to the commencement of the PDPO in December 1996, the Government and the PCPD had discussed its provisions with various trades. At that time, the trades expressed that implementing section 33 would affect different industries; data users required specific guidance from the Commissioner on how to comply with section 33; and after receiving such guidance from the Commissioner, more time would be needed for the relevant measures to be implemented. The Government also understood that businesses, especially the small and medium-sized enterprises (“SMEs”), would face certain difficulties in complying with section 33. Therefore it was decided that the implementation of section 33 be deferred.

5. The regulation under section 33 is premised upon geographical boundaries, and the drafting approach was technology-neutral. In view of the trends of digitalisation in the handling of personal data and globalisation of business operations in recent years, the impact of implementing the provision on different sectors would be even more significant. As such, preparation on multiple fronts by the Government and data users is necessary for ensuring that viable means are available for data users (including SMEs) to fulfill the requirements of section 33, and that the adoption of such means will not stifle legitimate business operations or compromise the competitiveness of Hong Kong.

## **Guidance on Personal Data Protection in Cross-border Data Transfer**

6. In December 2014, the PCPD issued the Guidance on Personal Data Protection in Cross-border Data Transfer (“the Guidance”) to assist data users in understanding the requirements on cross-border data transfers which section 33 would impose when brought into force, and to provide practical guidance. In so doing, the PCPD sought to encourage data users to adopt the practices recommended in the Guidance prior to the commencement of section 33 to protect personal data, as part of their corporate governance responsibility. Since the introduction of the Guidance, the views expressed by data users have mainly been concerned with the definitions of “personal data” and “transfer”, and difficulties in adopting the recommended model contract clauses provided by the PCPD to help data users comply with section 33(2)(f) (for instance, SMEs may not be able to require service providers to alter standard contract terms of the latter, and lack the resources to monitor service providers abroad; data users using cloud systems for data storage often do not have information on the actual geographical locations relating to the transfers).

### **Business Impact Assessment**

7. The Government appreciates that the implementation of section 33 could bring about an impact on businesses which is significant and substantive. Acting in prudence, we commissioned a consultant to study the compliance measures that data users would have to adopt in order to fulfill the requirements under section 33.

## Online survey

8. In the first phase of the study, the consultant conducted an online survey to collect information for an overview of cross-border transfers of personal data in different industries, including whether their business operations involved cross-border transfers of personal data, and the scale, means and destinations of the transfers. The consultant received a total of 124 valid responses from businesses. These businesses were engaged in finance and insurance, information and communications, manufacturing, trade and wholesale, professional and business services, etc., and over 70% of them have business operations which involved cross-border transfers of personal data.

9. The participants in this survey raised various substantive concerns over the implementation of section 33, which include whether the “white list”<sup>1</sup> promulgated by the Commissioner under section 33(2)(a) would include the key destinations of the trades’ data transfers, and the possibility of jurisdictions on the “white list” being delisted in future; whether there would be a grace period and a grandfathering arrangement; the applicability of restrictions on “transfers” in the context of cloud computing (e.g. when data stored in places on the “white list” could still be remotely accessed from places not on the list); and how “taken all

---

<sup>1</sup> The “white list” is the list of places specified by the Commissioner by notice in the Gazette as referred to in section 33(2)(a). The destinations of data transfers specified in the list have law in force which is substantially similar to, or serves the same purposes as the PDPO. In December 2013, a consultant commissioned by the PCPD completed a study report, which provides a methodology and criteria for deciding whether different jurisdictions have in force “law which is substantially similar to, or serves the same purposes as, the PDPO”. The consultant studied the relevant regulations of 50 jurisdictions, and considered that 35 of the jurisdictions could be included in the “white list”. Among them, only two were in Asia, one was in North America, one was in Oceania and the other 31 were in Europe. Since the completion of the study, there have been legislative amendments in some of the jurisdictions; therefore the “white list” in the consultancy report is not the list of places to be specified by the Commissioner by notice in the Gazette in exercise of authority under the Ordinance.

reasonable precautions and exercised all due diligence” to ensure sufficient protection of personal data is defined for the purpose of section 33(2)(f).

### Interviews with trade associations and companies

10. The consultant interviewed trade associations in different sectors, as well as companies of different scales and backgrounds and engaging in different businesses. By maximising the study’s coverage of different types of business operations and various modes of cross-border data transfers, the consultant sought to understand the compliance measures required of different organisations (including SMEs) to fulfill the requirements of section 33, and the impact of these measures on their business operations. The organisations interviewed include the Hong Kong General Chamber of Commerce, Federation of Hong Kong Industries, the Chinese Manufacturers’ Association of Hong Kong, Hong Kong Association of Banks, the Hong Kong Federation of Insurers, Hong Kong Information Technology Federation, the Hong Kong Wireless Technology Industry and the Federation of Hong Kong Hotel Owners, and 24 companies of different profiles in the sectors of information and communications, finance and insurance, hotel and tourism, professional and business services, transportation, storage, postal and courier services, manufacturing, and trade and wholesale. The consultant also received views from the Chinese General Chamber of Commerce in writing.

11. In the interviews, the trades expressed views similar to those obtained through the online survey (refer to paragraph 8 above) and also some other views as summarised below:

- (a) To transfer personal data in accordance with section 33(2)(b) to places not on the “white list” (i.e. a data user shall have reasonable grounds for believing there is law in force in that place which is substantially similar to, or serves the same purpose as, the PDPO), companies need to have an in-house legal team or engage legal advisors who are conversant with personal data protection. It is difficult for most companies, especially the SMEs, to have sufficient resources for a professional assessment of the privacy protection laws of the destinations of intended data transfers. They are also wary about whether the assessment by legal advisors would be accepted by the PCPD;
- (b) The trades considered that most companies would have to rely on section 33(2)(c) (i.e. obtaining written consent from data subjects for the cross-border transfers) or section 33(2)(f) (i.e. imposing requirements on data recipients outside Hong Kong through contracts, internal regulations, etc.) to meet the requirements of section 33 as far as possible;
- (c) With respect to section 33(2)(c), it would be very difficult to obtain written consent from all existing customers. If some of the customers or employees have not given consent in writing to the data transfers, the companies might have to establish processing systems or even a business department specifically to cater for them; the companies might also need to consider termination of the services;
- (d) Data recipients abroad might not be willing to enter into new

contracts incorporating, for the purpose of complying with section 33(2)(f), the requirements of the PDPO and the Guidance with data users in Hong Kong. It may be difficult for data users to obtain the business services they require for their operations, or they could only choose from a limited number of providers. The difficulties in finding service providers and the increase in operating costs would have an impact especially significant for the SMEs;

- (e) The PCPD should study whether data users having adopted certain existing rules and standards in highly regulated industries, such as banking, finance and insurance, could be regarded as having complied with section 33(2)(f); and
- (f) Hong Kong is a jurisdiction made up of one single city. Given the small scale of the domestic market, cross-border business activities have always been buoyant and so far there is no indication that cross-border data transfers has undermined personal data privacy. It is neither necessary nor appropriate to introduce additional restrictions based on geographical boundaries on top of the current regulatory framework which is based largely on data protection principles.

### **Experience of Other Jurisdictions**

12. We have studied whether other jurisdictions have statutory requirements similar to that of section 33. It is noted that there are regulations on cross-border transfers of personal data in places including the European Union ("EU"), the United Kingdom ("UK"), New Zealand,



Singapore and Macao, whereas some of the trading partners of Hong Kong, such as the United States, have no such requirement. Even in the EU, there are provisions permitting data users to transfer personal data outside the EU to countries which have not been accredited as having adequate legal protection for personal data, by the use of binding corporate rules or contractual terms which impose control on the receiving end of the data. According to the information collected by the consultant on the implementation of relevant requirements in the UK, New Zealand, Singapore and Macao, data protection authorities in these jurisdictions have hardly encountered any case of enforcement concerned with provisions regulating cross-border transfers of personal data.

### **Way Forward**

13. After listening to the views of Members, the consultant will complete the detailed analysis of the information and views provided by the trades, and consolidate the final business impact assessment report. The PCPD will further study the issues raised by the trades with regard to section 33, the Guidance and compliance requirements in respective industries, such as PCPD's mechanism for reviewing and updating the "white list"; whether the industries already subject to stringent regulations could be regarded as having met the requirements of section 33 by means of compliance with the data protection requirements of their regulatory authorities; the criteria to be applied in determining whether a data user has "taken all reasonable precautions and exercised all due diligence", etc.. The Government will formulate the steps forward in the light of the results of PCPD's study.

## **Advice Sought**

14. Members are invited to offer views on the content of this paper.

**Constitutional and Mainland Affairs Bureau**

**May 2017**