立法會
Legislative Council

LC Paper No. CB(1)398/18-19(06)

Ref : CB1/PL/FA

Panel on Financial Affairs

Meeting on 7 January 2019

Background brief on personal data protection issues relating to credit reference agencies

Purpose

This paper summarizes the discussion of the Panel on Financial Affairs ("FA Panel"), the Panel on Constitutional Affairs ("CA Panel") and the Panel on Information Technology and Broadcasting ("ITB Panel") on issues relating to the protection of personal data and cyber security, in particular the protection of customers' data by commercial organizations, such as banks, stored value facility ("SVF") operators and credit reference agencies ("CRAs") in the 2017-2018 and 2018-2019 sessions.

Background

Protection of personal data privacy

2. The Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), which came into force in December 1996, aims to protect the individual's right to privacy with respect to personal data. PDPO applies to any data relating directly or indirectly to an individual, from which it is practicable to ascertain the identity of the individual and which is in a form in which access to or processing is practicable. Users of personal data in both public and private sectors are subject to the provisions of PDPO. PDPO was amended in

mid-2012 and all the amended provisions have already come into operation.[1] The main features of PDPO are set out in **Appendix I**.

Handling of consumer credit data by credit reference agencies

3. According to the Administration, with a view to providing practical guidance for CRAs in Hong Kong, the Privacy Commissioner for Personal Data ("PCPD") issued the Code of Practice on Consumer Credit Data ("Code of Practice")[2] in February 1998 to regulate the handling of personal credit data by CRAs and credit providers. The Code of Practice covers areas on the collection, accuracy, use, security, access and correction of data. According to paragraph 3.12 of the Code of Practice, a CRA shall take appropriate measures in protecting personal credit data in its daily operations to safeguard against any improper access to personal credit data held by it, including monitoring and reviewing on a regular and frequent basis the usage of the database, with a view to detecting and investigating unusual or irregular patterns of access or use, etc.

4. Hong Kong Monetary Authority ("HKMA") has explained that CRAs provide credit reference services to banks in Hong Kong and other credit institutions and shall comply with the relevant provisions of the PDPO and the Code of Practice. Although CRAs are not regulated by HKMA under the current legal framework, HKMA, as the regulatory authority for banks, requires banks to comply with the provisions of PDPO when carrying out relevant businesses so as to ensure that personal data of customers are properly safeguarded when providing data to and using the service of CRAs. HKMA also requires banks to comply with the relevant supervisory requirements set out in HKMA's Supervisory Policy Manual when providing CRAs with and using credit data. In accordance with the requirements, banks that use the service of a CRA should enter into a formal contractual agreement with the CRA that

---

[1] The Personal Data (Privacy) (Amendment) Ordinance 2012 ("Amendment Ordinance") was passed by the Legislative Council on 27 June 2012. The Amendment Ordinance introduced amendments to the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), inter alia, to provide for regulation over the use of personal data in direct marketing and provision of personal data for use in direct marketing; to create a new offence for disclosure of personal data obtained without consent from data users; to empower the Privacy Commissioner for Personal Data to provide legal assistance to aggrieved data subjects in bringing proceedings to seek compensation from data users under PDPO; to impose a heavier penalty for repeated contravention of enforcement notices; and to create a new offence for repeated contravention of the requirements under PDPO for which enforcement notices have been served.

[2] Four revisions have been made to the Code of Practice on Consumer Credit Data, with the latest revision made in January 2013.

requires the CRA to formulate effective control systems to ensure that relevant provisions of PDPO and the Code of Practice are complied with.

Cyber security

5. According to the Administration, the Office of the Government Chief Information Officer ("OGCIO") and its Government Computer Emergency Response Team have been closely monitoring the overall cyber security situation in Hong Kong. The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") has been established to provide different stakeholders with support in relation to cyber security, including disseminating information on cyber security incidents and security advice, protecting government information systems, nurturing professionals in cyber security, as well as strengthening public education and raising the awareness of public and private organizations through various media and activities. In order to provide appropriate advice on cyber threats and security incidents in a more effective manner, OGCIO launched the Cyber Security Information Sharing and Collaborative Platform ("the Platform") in September 2018 to facilitate the exchange of views among cyber security experts, covering analysis of cyber threats and impact of security incidents, as well as sharing of follow-up strategies, etc. HKCERT also disseminates security advice to the general public through the Platform.

Discussion of relevant Panels

Protection of customers' data by commercial organizations

6. When the FA Panel received briefings on the Chief Executive's 2018 Policy Address on initiatives relating to financial services and on HKMA's work at the meetings on 30 October 2018 and 5 November 2018 respectively, members discussed the e-wallet top-up incident relating to the Faster Payment System ("FPS") happened in October 2018 ('the Incident"). As the Incident might have involved the theft of personal information for setting up e-wallet accounts and making direct debit authorization for account top-up, members enquired about HKMA's follow-up measures in enhancing banks' electronic direct debit authorization ("eDDA") procedure, including whether there was plan to impose requirements on the collection and use of personal data and authentication of eDDA for both physical banks and virtual banks. Members also urged HKMA to learn lessons from the Incident, and stressed the need for HKMA to step up risk assessment measures prior to the launch of other new financial technologies ("Fintech") initiatives.

7. HKMA pointed out that the Incident was related to the authentication controls of e-wallets rather than the security of FPS. HKMA had requested SVF operators and banks to adopt the refined processes to enhance user protection which included (a) sending an SMS notification to the e-wallet user to confirm the setting-up of eDDA through FPS; (b) requiring the user to make a one-time credit transfer from the relevant bank account to his/her e-wallet so as to confirm the wallet user was the same as the bank account owner; or (c) verification of customer identities via two-factor authentication with banks. HKMA stressed that it would assess the risks of e-wallets carefully as banks would rely on third parties to conduct authentication. HKMA would also take measures to strengthen the know-your-client requirements (which involved (a) ascertaining the authenticity of individual clients; and (b) obtaining background information of the clients) for both physical banks and virtual banks, and would adopt a risk-based approach in implementing such requirements.

Enforcement power of the Privacy Commissioner for Personal Data

8. When the CA Panel received a briefing by PCPD on the work of his Office at the meeting on 14 February 2018, some members expressed concern that so far no successful prosecution had been brought against cyber-related contraventions of PDPO and those successful prosecutions were only related to commercial activities. These members considered that there might be a need to grant more power to PCPD in order to strengthen the protection of personal data privacy.

9. PCPD explained that where the occurrence of a security incident involved other criminal elements (e.g. access to a computer with criminal or dishonest intent), it would be referred to the Police for investigation and the criminal(s) would be charged with the more serious offence, even though certain aspects of privacy-related issues were detected in the first instance in some cases.

10. PCPD advised that to enhance personal data privacy protection, his Office had implemented a series of result-oriented promotion and education programmes to raise public awareness in this respect. The Office of PCPD had also taken the initiative to engage organizational data users of various industries with a view to assisting them in complying with PCPO through inspections, compliance checks, round-table discussions, seminars, workshops, talks and lectures.

Need for review of the Personal Data (Privacy) Ordinance to cope with new challenge

11. Members expressed concern about the collection of data and profiles of clients with the aid of advanced data processing and analytics techniques, and enquired whether such activities would be subject to regulation. Members considered that a balance should be struck between promoting businesses and the protection of personal data privacy. PCPD conceded that the rapid development of big data, artificial intelligence and related technologies in recent years had created unanticipated privacy risks and moral implications. The Office of PCPD would focus on engaging the business sector in promoting the protection of personal data privacy, with a view to enhancing the culture of respect for personal data privacy in the sector. The Office of PCPD would also strengthen the working relationship with overseas data protection authorities and explain the newly implemented rules and regulations on data protection of other jurisdictions to the local stakeholders for compliance with the requirements.

12. At the ITB Panel meeting on 12 February 2018, some members enquired whether the Administration had examined if the existing legislation was up-to-date in ensuring protection of privacy and information security in the light of the increasing prevalence of online activities, such as Internet payment and other cyber commercial activities. At the request of the ITB Panel, the Administration has provided a paper on its plan for legislative review in view of privacy and information security issues arising from the development of e-commerce, Internet of Things, Fintech, etc. which is provided through a hyperlink in **Appendix II**.

Relevant Legislative Council questions

13. At the Council meeting of 29 November 2017, Hon Charles MOK raised a written question on measures to enhance information security in local enterprises and industries. Hon Paul TSE asked an oral question on leakage of personal data by commercial organizations, including the TransUnion Limited ("TransUnion") at the Council meeting of 12 December 2018. Details of the questions and the Administration's replies are provided through hyperlinks in **Appendix II**.

Recent developments

14. The Administration will brief the FA Panel on the follow-up actions taken by the relevant government agencies and PCPD in response to the incident concerning security of consumer credit data maintained by TransUnion at the meeting on 7 January 2019. Members of CA Panel and ITB Panel have been invited to join the discussion.

Relevant papers

15. A list of the relevant papers is in **Appendix II**.

Council Business Division 1
Legislative Council Secretariat
3 January 2019

Appendix I

Main features of the Personal Data (Privacy) Ordinance (Cap. 486)

The main features of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") are set out below:

(a) it establishes the Privacy Commissioner for Personal Data ("PCPD"), which is an independent statutory authority, to promote and enforce compliance with PDPO;

(b) it gives statutory effect to internationally-accepted data protection principles[1] ("DPPs"), which provide for the fair collection of personal data; accuracy of personal data; duration for retention of personal data; limits on the use of personal data; security of personal data; openness by data users about the kinds of personal data they hold and purposes to which they are put; as well as data subjects' rights of access and correction with respect to their personal data;

(c) it regulates the use of personal data in direct marketing and the provision of personal data for use in direct marketing;

(d) it provides for offences against the disclosure of personal data obtained without consent from data users;

(e) it gives PCPD powers to approve and issue codes of practice giving guidance on compliance with PDPO; inspect personal data systems and investigate suspected breaches of the requirements under PDPO;

(f) it subjects the automated comparison of personal data to suitable control to protect the privacy interests of data subjects;

(g) it provides for a broad exemption for personal data held for domestic purposes and narrowly defined exemptions from the requirements on subject access and use limitation to cater for a variety of competing

---

[1] Data user must follow the fair information practices stipulated in the six data protection principles ("DPPs") in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486). The Privacy Commissioner for Personal Data is empowered to direct the data user concerned to take corrective actions for non-compliance with the provisions of DPPs by issuing an enforcement notice. With effect from 1 October 2012, if a data user fails to take corrective actions for his contravention by the date specified in an enforcement notice, he will be liable to a fine at level five (at present $50,000) and imprisonment for two years. The data user is liable to a daily penalty of $1,000 if the offence continues. On a second or subsequent conviction, the maximum penalty is a fine at level six (at present $100,000) and imprisonment for two years.

public and social interests, such as human resources management; security, defence and international relations; the prevention and detection of crime; the assessment or collection of taxes; financial regulation; an individual's physical or mental health; news gathering and reporting, legal proceedings, due diligence exercise, and emergency situations; and

(h) it gives PCPD power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user.

Source: LC Paper No. CB(2)222/18-19(03)

Appendix II

List of relevant papers

Date	Event	Papers/Minutes of meeting
29 November 2017	Written question raised by Hon Charles MOK on "Measures to enhance information security"	Hansard (pages 3120 – 3124)
12 February 2018	Meeting of the Panel on Information Technology and Broadcasting ("ITB Panel") (Item V)	Administration's paper (LC Paper No. CB(4)577/17-18(03)) Background brief (LC Paper No. CB(4)577/17-18(04)) Administration's response to issues raised at the meeting on 12 February 2018 (LC Paper No. CB(4)1522/17-18(01)) Minutes (paragraphs 7-35) (LC Paper No. CB(4)832/17-18)
14 February 2018	Meeting of the Panel on Constitutional Affairs ("CA Panel") (Item IV)	Administration's paper (LC Paper No. CB(2)851/17-18(03)) Updated background brief (LC Paper No. CB(2)851/17-18(04)) Minutes (paragraphs 4-25) (LC Paper No. CB(2)1224/17-18)
28 February 2018	Written question raised by Hon LAM Cheuk-ting on "Computer theft incident of the Registration and Electoral Office"	Hansard (pages 7163 – 7166)

Date	Event	Papers/Minutes of meeting
30 October 2018	Meeting of the Panel on Financial Affairs ("FA Panel") (Item I)	Administration's paper (LC Paper No. CB(1)12/18-19(01)) Minutes (LC Paper No. CB(1)306/18-19)
5 November 2018	Meeting of the FA Panel (Item IV)	Administration's paper (LC Paper No. CB(1)101/18-19(02))
14 November 2018	Joint meeting of the CA Panel, the ITB Panel and the Panel on Security	Administration's paper (LC Paper No. CB(2)222/18-19(01)) Background brief (LC Paper No. CB(2)222/18-19(03))
12 December 2018	Oral question raised by Hon Paul TSE on "Leakage of personal data by commercial organizations"	Oral question raised by Hon Paul TSE and Administration's reply