立法會
Legislative Council

LC Paper No. CB(2)512/19-20(04)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

Background brief prepared by the Legislative Council Secretariat for the meeting on 20 January 2020

Review of the Personal Data (Privacy) Ordinance

Purpose

This paper provides background information on the latest review of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"). It also summarizes the major views and concerns expressed by Legislative Council ("LegCo") Members on issues relating to the review of PDPO.

Background

Personal Data (Privacy) Ordinance

2. PDPO, having come into force since 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.

3. The Administration conducted a comprehensive review of PDPO with the support of the Privacy Commissioner for Personal Data ("PCPD"), and consulted the public from August to November 2009 on proposals arising from the review. The Administration published the consultation report in October 2010 [LC Paper No. CB(2) 37/10-11(02)] and further consulted the public on the legislative proposals from October to December 2010. The Report on Further Public Discussions on Review of PDPO was published in April 2011. The Ordinance was amended in mid-2012 and all the amended provisions have already come into operation.[1]

---

[1] The Personal Data (Privacy) (Amendment) Ordinance 2012 ("Amendment Ordinance") was passed by LegCo on 27 June 2012. The Amendment Ordinance introduced amendments to 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

4. The main features of PDPO are as follows:

(a) it establishes 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, 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 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.

---

empower PCPD 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.

Latest review of the Personal Data (Privacy) Ordinance

5. When the Panel on Constitutional Affairs ("CA Panel") received a policy briefing by the Secretary for Constitutional and Mainland Affairs on 16 December 2019 on the policy initiatives of the Constitutional and Mainland Affairs Bureau ("CMAB") as announced in the 2019 Policy Address, the Administration advised that in view of the series of major personal data breach incidents which took place earlier, CMAB was now actively reviewing and studying possible amendments to the PDPO jointly with PCPD to strengthen protection towards personal data privacy.[2] According to the paper provided by the Administration [LC Paper No. CB(2)19/19-20(01)] for the said meeting, PCPD has already put forward preliminary recommendations on amendments to PDPO to the Administration. CMAB is now focusing its study on several amendment directions, including:

(a) establishing a mandatory data breach notification mechanism;

(b) strengthening the regulation on data retention period;

(c) reviewing penalties of non-compliance with PDPO by raising relevant criminal fines and exploring the feasibility of introducing direct administrative fine;

(d) regulating data processors directly to strengthen protection towards personal data being processed; and

(e) amending the definition of "personal data" to cover information relating to an "identifiable" natural person.

6. The Administration informed the CA Panel that it would continue to conduct further in-depth study on the feasibility of the above proposed legislative amendment directions in collaboration with PCPD, and make reference to relevant data protection laws in other jurisdictions and Hong Kong's actual situation. The Administration also advised that it would consult relevant stakeholders in due course, with a view to submitting concrete proposals to amend PDPO and drafting the amendment bill as soon as possible.

---

[2] Major personal data breach incidents in recent years included the incident of leakage of personal data of 9.4 million passengers as announced by Cathay Pacific Airways Limited on 24 October 2018 ("the Cathay Pacific incident") and suspected security loopholes in the TransUnion Limited's online procedures for obtaining personal credit information as reported by the press in November 2018 ("the TransUnion incident").

Discussion of relevant Panels

Enforcement power of the Privacy Commissioner for Personal Data

7. During discussion of the review of PDPO in 2009 by the CA Panel, members had expressed diverse views on PCPD's proposals of granting criminal investigation and prosecution power to PCPD, empowering PCPD to award compensation to aggrieved data subjects, and requiring a data user to pay monetary penalty for serious contravention of Data Protection Principles ("DPPs")[3] of PDPO. Nevertheless, members in general expressed concern that PCPD had inadequate powers for the effective enforcement of PDPO.

8. At the CA Panel meetings on 15 and 20 November 2010, the former PCPD pointed out that the recent serious contraventions of PDPO and unauthorized sale of personal data had reflected the inadequacy of the enforcement power of PCPD. The proposal of granting PCPD criminal investigation and prosecution powers could meet the public expectations for enhancing deterrent measures against serious contravention of PDPO. The former PCPD advised that his team had the knowledge and experience to perform those roles efficiently and effectively. However, the discretion to prosecute or not still vested in the Secretary for Justice.

9. The Administration was of the view that in order to maintain check and balance, PCPD should not be provided with the power to carry out criminal investigations and prosecutions, and the existing arrangement under which criminal investigation and prosecution were vested respectively in the Police and the Department of Justice should be retained. The Government announced in April 2011 that proposals of granting criminal investigation and prosecution power to PCPD, empowering PCPD to award compensation to aggrieved data subjects and requiring data user to pay monetary penalty for serious contravention of DPPs under PDPO would not be implemented.

10. When the CA Panel received a briefing by PCPD on the work of his Office at its meeting on 14 February 2018, some members expressed concern

---

[3] Data users must follow the fair information practices stipulated in the six DPPs in Schedule 1 to PDPO in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, availability of data information, and access to personal data. PCPD 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.

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.

11. 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. To enhance personal data privacy protection, PCPD advised that 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 challenges

12. At various briefings by PCPD given to the CA Panel, some 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. These members considered that a balance should be struck between promoting businesses and the protection of personal data privacy. Some other members were also concerned that the application of biometric technology (including fingerprint recognition, voice authentication, retina scan, facial recognition, finger vein recognition) by banking and financial institutions might pose security risks to their customers' personal data privacy. They considered that PCPD and the Administration should formulate a policy to enhance personal data privacy protection in this regard.

13. In response to members' concern, 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. PCPD's Office 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. PCPD's Office would also strengthen the working relationship with overseas data protection authorities. It would explain the newly implemented rules and regulations on data protection of other jurisdictions to the local stakeholders for compliance with the requirements. As regards the financial industry, PCPD's Office had engaged relevant stakeholders

including monitoring bodies, banking institutions, and card issuing companies through meetings, and had conducted professional workshops, talks and seminars on financial technology. Many recommendations made by PCPD's Office had been adopted and incorporated into the relevant guidelines published by these monitoring bodies/organizations. PCPD also advised that more efforts would be made to strengthen protection of personal data privacy in the business sector.

14. 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. In response to members' concerns, 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, Financial Technology, etc. (in **Appendix I**).

Establishing a mandatory data breach notification mechanism and raising the penality of non-compliance

15. At the meeting jointly held by the CA Panel, the Panel on Information Technology and Broadcasting, and the Panel on Security on 14 November 2018 to discuss the Cathay Pacific incident and issues relating to protection of personal data and cyber security, members urged the Administration to review the relevant provisions in PDPO to introduce requirements for incidents of data breaches to be disclosed within a certain timeframe, say, 72 hours. Members in general also considered that the current regulatory regime lacked deterrent effect and the level of penalty should be enhanced. There was a suggestion that in reviewing the provisions of PDPO, the Administration should make reference to the European Union's General Data Protection Regulation ("GDPR") and other cyber security laws instituted in overseas jurisdictions to safeguard personal data and to prescribe rules on how incidents of personal data breaches should be reported.

16. PCPD advised that while there was no mandatory requirement under the current law for any organization to file a notification in cases of data leakage, PCPD's Office had started reviewing PDPO taking into consideration the provisions in GDPR. Introducing mandatory requirements for notification, the prosecution process as well as the penalty levels were among the areas to be reviewed. The Administration also conceded that there was room for amending PDPO and the Administration would take the results of the compliance investigation of the Cathay Pacific incident into consideration while keeping an open mind about the amendment proposals.

Protection of consumers' data by credit reference agencies

17. At its meeting on 7 January 2019, the Panel on Financial Affairs ("FA Panel") discussed personal data protection issues relating to credit reference agencies ("CRAs") in the wake of the TransUnion incident. Members raised concern about the possible security loopholes in the procedures for TransUnion's customers in obtaining their credit reports through TransUnion's online platform, which had recently enabled an unauthorized party to access credit information and personal data of some customers in TransUnion's database. They enquired whether the Administration would consider introducing a specific regime to regulate CRAs in the handling of personal data including the provision of data to CRAs' business partners for profit.

18. PCPD advised that in the light of the TransUnion incident, his Office would conduct a comprehensive review of the Code of Practice on Consumer Credit Data ("Code of Practice") with reference to the findings of the compliance investigation, and would consider improvements to the operation of the Code of Practice where necessary. According to the Administration, the handling of personal data by CRAs, including the collection, accuracy, use, security, access and correction of data, was regulated by the Code of Practice. With regard to the regulation of CRAs, the Administration and the representative of the Hong Kong Monetary Authority ("HKMA") stressed that PDPO had clear provisions governing the protection of personal data privacy. From the perspectives of financial market regulation and development, the Administration advised that it had no plan to introduce a specific regulatory regime for CRAs, as the TransUnion incident was an issue pertaining to personal data protection. Nevertheless, the Administration agreed to consider in collaboration with PCPD how the regulation of data protection could be further enhanced under the existing legal framework.

19. The representative of HKMA also advised that only about half of the information providers to TransUnion were banks. Apart from CRAs, there were other third-party service providers in the market which would have access to and process personal data of bank customers. These third-party service providers, however, were not regulated by HKMA. Whether these third-party service providers should be regulated was a complicated question. That said, HKMA would make reference to the outcome of PCPD's compliance investigation of the TransUnion incident, and work together with the banking industry to consider ways to further strengthen the arrangements between banks and CRAs.

20. At the same meeting, the FA Panel passed a motion urging the Government to, among others, study the regulation of CRAs, strengthen the monitoring of the collection, holding, handling or use of customers' personal

credit data, and refine the legislation to enhance the community's confidence in credit rating reference services. The wording of the motion and the Administration's written response are in **Appendices II** and **III** respectively.

Relevant motion passed by the Legislative Council

21. At the Council meeting of 22 May 2019, Dr Hon Priscilla LEUNG moved a motion on "Keeping up with technological development and enhancing the protection of people's privacy" urging the Government to, among other things, comprehensively review the policy on personal data privacy protection. The motion as amended by Hon Elizabeth QUAT was passed by the Council. The wording of the motion and the progress report provided by the Administration are in **Appendix IV**.

Recent development

22. The CA Panel will discuss the review of PDPO at its next meeting on 20 January 2020.

Relevant papers

23. A list of the relevant papers on the LegCo website is in **Appendix V**.

Council Business Division 2
Legislative Council Secretariat
13 January 2020

Appendix I

LC Paper No. CB(4)1522/17-18(01)

香港特別行政區政府

創新及科技局

香港添馬添美道二號
政府總部西翼二十樓

INNOVATION AND
TECHNOLOGY BUREAU

THE GOVERNMENT OF THE HONG KONG
SPECIAL ADMINISTRATIVE REGION

20/F, West Wing, Central Government Offices,
2 Tim Mei Avenue, Tamar, Hong Kong

電話 Tel: 3655 5607
圖文傳真 Fax: 3153 2664

By email

31 August 2018

Mr Daniel SIN,
Clerk to Panel,
Panel on Information Technology and Broadcasting,
Legislative Council Complex,
1 Legislative Council Road,
Central, Hong Kong

Dear Daniel,

Information requested at the meeting of
the Panel on Information Technology and Broadcasting on 12 February 2018

At the meeting of the Panel on Information Technology and Broadcasting on 12 February 2018, Members requested supplementary information on the following:

(a) the Government's plan for legislative review in view of the privacy and information security issues arising from the development of e-commerce, Internet of Things (IoT), Financial Technology (FinTech), etc.; and
(b) the Government's assessment on the current cyber security situation in Hong Kong, and whether the Government would conduct victimisation surveys on cyber crimes.

In consultation with the relevant bureaux/departments, our response is set out below.

Legislative review

Regarding information security, Hong Kong has many pieces of legislation tackling computer and Internet-related crimes. For example, the Theft Ordinance (Cap. 210) deals

with offences of destroying, defacing, concealing or falsifying records kept by computer; the Crimes Ordinance (Cap. 200) tackles access to computer with criminal or dishonest intent; and the Telecommunications Ordinance (Cap. 106) prohibits unauthorised access to computer by telecommunications.

Although certain laws do not mention explicitly the cyber environment, they can still apply to the virtual world. For example, the Unsolicited Electronic Messages Ordinance (Cap. 593) prohibits fraud activities related to the sending of multiple commercial electronic messages; and the Personal Data (Privacy) Ordinance (Cap. 486) is applicable to any personal data which is practicable to be accessed and processed. The Government will review the relevant laws from time to time in view of the volatile environment and amend them when necessary.

On protection of privacy, Members expressed concern over the protection of privacy of children on the Internet. The Personal Data (Privacy) Ordinance is a technology-neutral legislation and protects data subjects of all ages including children. The Office of the Privacy Commissioner for Personal Data (PCPD) has also carried out education on children's privacy by, for example, distributing information in relation to protection of personal data privacy on its main website (i.e. pcpd.org.hk) and two thematic websites (i.e. "Be SMART Online" and "Children Privacy"), and publishing guidelines for organisations, parents and teachers.

Concerning the promotion of FinTech, the Government strives to facilitate financial innovation on the one hand and to protect the investing public on the other. To this end, we keep our legislative and regulatory regime under constant review. Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) and Insurance Authority (IA) have established their respective dedicated FinTech liaison platforms to enhance communications with the FinTech industry. HKMA, SFC and IA have also launched their respective regulatory sandboxes to allow financial institutions to test FinTech projects in a confined environment.

Assessment on the current cyber security situation and victimisation surveys on cyber crimes

The Hong Kong Police Force (HKPF) recorded 5 567 cases of technology crime in 2017 with a total financial loss of around $1.4 billion. Both figures have shown a decline when compared with 2016 (5 939 cases and $2.3 billion).

The HKPF have been closely monitoring and analysing the latest trends of technology

crimes in Hong Kong and overseas, as well as maintaining close liaison with relevant law enforcement agencies and industry stakeholders with a view to timely assessing the cyber security situation in Hong Kong. Subject to the availability of resources, the HKPF will prepare and maintain statistics useful to their work depending on operational needs and the level of effectiveness. The HKPF currently has no plan to conduct victimisation surveys on technology crimes.

In addition, the Government studies the surveys and reports prepared by the industry to assess Hong Kong's cyber security situation in comparison to other areas. According to the Microsoft Security Intelligence Report in 2017, about 6.4% of computers in Hong Kong were targeted by malware, which was lower than the global average of 7.8% and much lower than the highest rate of 26.6% in Bangladesh. Furthermore, according to the Safe Cities Index 2017 published by the Economist, among the 60 cities, Hong Kong was ranked fifth in terms of digital security.

We will continue to strengthen information security within the Government and collaborate with different stakeholders to protect the public and businesses against cyber security threats with the aim of promoting Hong Kong's overall information security and cyber resilience.

Yours sincerely,

(Salina MAK)
for Secretary for Innovation and Technology

附錄 II
Appendix II

立法會CB(1)421/18-19(01)號文件
LC Paper No. CB(1)421/18-19(01)

財經事務委員會

在2019年1月7日會議上通過的議案

目前信貸提供者和信貸資料庫的行為只有實務守則規管，對消費者權益保護非常不足。鑒於信貸資料服務機構持有大量消費者信貸紀錄等敏感個人資料，本會促請政府研究對信貸資料服務機構的規管，加強監察收集、持有、處理或使用客戶個人信貸資料的活動，令將來運用創新科技提供個人信貸資料更加透明、安全，完善法例以提升社會對信用評級資料服務的信心。

由莫乃光議員動議並經陳振英議員修正的議案

(Translation)

Panel on Financial Affairs

Motion passed at the meeting on 7 January 2019

Currently, as the conduct of credit providers and credit databases is only regulated under a code of practice, the protection of consumer rights and interests is very inadequate. Given that credit reference agencies are in possession of a large amount of sensitive personal data such as consumer credit records, this Panel urges the Government to study the regulation of credit reference agencies, strengthen the monitoring of the collection, holding, handling or use of customers' personal credit data, increase the transparency and security of using innovative technologies to provide personal credit data in the future, and refine the legislation to enhance the community's confidence in credit rating reference services.

Motion moved by Hon Charles Peter MOK as amended by Hon CHAN Chun-ying

Panel on Financial Affairs
Follow-up to meeting on 7 January 2019

The Personal Data (Privacy) Ordinance ("PDPO") has clear legal provisions governing the protection of personal data privacy. Credit reference agencies ("CRAs") must comply with the PDPO and the Code of Practice on Consumer Credit Data ("Code of Practice") issued by the Privacy Commissioner for Personal Data ("Privacy Commissioner") under the PDPO when providing credit reference services to banks and other organisations in Hong Kong. The Code of Practice covers requirements ranging from the collection, accuracy, use, security to access and correction of data. It stipulates that a CRA shall take appropriate measures to protect 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.

The TransUnion incident involves suspected unauthorised access to customer data, which is an issue pertaining to personal data protection. The Office of the Privacy Commissioner for Personal Data ("PCPD") has commenced a compliance investigation against TransUnion pursuant to the PDPO. The investigation is currently ongoing. The PCPD will conduct a comprehensive review of the Code of Practice having regard to the findings of the compliance investigation, and consider the need for further revisions to improve the operation of the Code. The Government, together with the PCPD, is also reviewing the relevant stipulations and penalties under the PDPO, and will seriously consider how the regulation of data protection could be enhanced. The Hong Kong Monetary Authority will make reference to the outcome of the investigation conducted by the Privacy Commissioner, and assist the Privacy Commissioner in liaising with the banking industry to review whether the contractual arrangements between the banking industry and CRAs can be improved.

Motion on "Keeping up with Technological Development and Enhancing the Protection of People's Privacy" at the Legislative Council meeting of 22 May 2019

Progress Report

Purpose

At the Legislative Council meeting held on 22 May 2019, the motion on "Keeping up with Technological Development and Enhancing the Protection of People's Privacy" moved by Dr Hon Priscilla LEUNG and amended by Hon Elizabeth QUAT was passed. The wording of the motion passed is at **Annex**. This paper reports on the progress of relevant work.

Review of the Personal Data (Privacy) Ordinance

2. The rapid development of information technology, common usage of the internet and mobile communication technology, as well as the advancement in technology have brought a considerable number of new challenges to the protection of personal data privacy. The trend of personal data privacy breaches has shifted from mostly improper collection and use of data and direct marketing in the past to breach of data security, such as data leakage and hacker attacks resulting from security loopholes recently. In addition, the series of major personal data breach incidents which took place earlier attracted public concern on the sufficiency of the Personal Data (Privacy) Ordinance (PDPO) in protecting personal data privacy.

3. The Government highly values the protection of personal data privacy and agrees that the data protection regime has to be up-to-date. We are now reviewing and studying possible amendments to the PDPO jointly with the Privacy Commissioner for Personal Data (PCPD). The PCPD has already put forward preliminary recommendations on

amendments to the PDPO to the Government. We are now focusing our study on several amendment directions which are listed in the following paragraphs.

Mandatory Data Breach Notification Mechanism

4. Data Protection Principle (DPP) 4 under the PDPO states that data users must take all practicable steps to prevent unauthorised or accidental access of personal data. However, there is currently no statutory requirement for a data user to notify the PCPD or the data subject of a data breach. Introducing the mandatory notification mechanism could ensure that the Privacy Commissioner could monitor the handling of these organisations who could seek instructions from the Privacy Commissioner for follow up to mitigate or prevent further damage resulting from the data breach. We are of the view that introducing the mandatory notification mechanism could strengthen the protection towards personal data.

5. In examining the establishment of a mandatory personal data breach notification mechanism, the topics being considered include the definition of "personal data breach" and the notification threshold (i.e. what type and scale of data breach incident would require the organisation to make notification to the PCPD and data subjects, and whether the threshold should be the same for notification to both parties), etc. With reference to overseas experience, in terms of notification threshold, when considering whether to make notification to the PCPD, the organisation should consider various factors, including the type of personal data being leaked, the amount of personal data involved, the likelihood of identity theft, and whether the leaked data is adequately encrypted, etc.

6. In terms of notification timeframe, overseas experience shows that data users may need time to verify the details of a data breach case. We are considering whether it is necessary to allow data users to investigate and verify the suspected data breach incident before making notification

within a specified timeframe.

Data Retention Period

7. DPP2 under the PDPO provides that data users should 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, which is similar to data protection laws in other jurisdictions.

8. However, the longer the data is retained, the higher the risk for data breach and the severity of the impact brought. Unnecessary privacy risk in respect of those data subjects whose personal data should have been purged will persist. In view of different organisations' service nature and unique need, introducing a one-size-fits-all retention period may not be appropriate. Therefore, we are currently considering amending the PDPO to require data users to formulate a clear retention policy which provides for a retention period for the personal data collected.

9. At present, DPP5(a) of the PDPO provides that "all practicable steps shall be taken (by data users) to ensure that a person can ascertain a data user's policies and practices in relation to personal data". We will consider whether DPP5 should be amended to require data users to expressly provide for the retention policy.

Power of Sanction

10. At present, in case of non-compliance of the DPPs under the PDPO, the PCPD may issue an enforcement notice to the data user directing it to remedy. Contravention of DPPs is currently not an offence in itself. Only non-compliance with the enforcement notice is an offence punishable by either a fine or imprisonment. Non-compliance of an enforcement notice attracts a criminal fine at Level 5 (i.e. up to a maximum of HK$50,000 according to Schedule 8 of the Criminal Procedure

Ordinance), and imprisonment up to 2 years on first conviction. As revealed from past experience, the existing levels of criminal fines under the PDPO and its deterrence effect are insufficient to incentivise data users to comply with the PDPO. To raise the deterrence effect of the PDPO, one of our study directions is to raise the relevant criminal fines.

11. Furthermore, we note that a number of overseas data protection authorities are empowered to impose administrative fines for contravention of their data protection legislation. Hence, we are also exploring the feasibility of introducing direct administrative fine in Hong Kong.

Regulation of Data Processors

12. Currently, the PDPO places the obligation to protect personal data on data users, who are required to adopt contractual means to ensure that data processors[1] or sub-contractors adopt measures to ensure the safety of personal data. In other words, the PDPO only imposes indirect regulation over data processors. However, with the advancement in technology, out-sourcing data activities like sub-contracting personal data processing work to other service providers has become more common. In principle, we hold the view that it is necessary to regulate data processors to strengthen protection towards personal data being processed, and to reflect fairer sharing of responsibilities between data users and data processors.

13. We note that a number of overseas regulatory authorities have introduced direct regulation on data processors, or required data processors to observe requirements which are confining to certain circumstances (e.g. in relation to data retention, erasure and security). Hence, our study direction is to regulate data processors directly by imposing legal obligations on data processors or sub-contractors, for instance, to require data processors to be directly accountable for personal data retention and

[1] According to the PDPO, "data processor" means a person who processes personal data on behalf of another person and does not process the data for any of the former's own purposes.

security.

Definition of Personal Data

14. The current definition of "personal data" under the PDPO includes information that relates to an "identified" person. In view of the wide use of tracking and data analysis technology nowadays, expanding the definition of "personal data" under the PDPO to cover information relating to an identifiable natural person would satisfy social needs and expectation. In a number of jurisdictions examined, the definition of "personal data" also includes data that relates to an "identifiable"[2] natural person. We hold the view that amending the definition of "personal data" under the PDPO could raise the protection towards personal data.

Way Forward

15. We will continue to conduct further in-depth study on the feasibility of the above proposed legislative amendment directions in collaboration with the PCPD, and make reference to relevant data protection laws in other jurisdictions and Hong Kong's actual situation. We would consult relevant stakeholders including the relevant Legislative Council Panel in due course, with a view to submitting concrete proposals to amend the PDPO as soon as possible.

Constitutional and Mainland Affairs Bureau
September 2019

[2] An "identificable person" is a living individual who can be identified, directly or indirectly, by reference to an identifier such as name, location or an online identifier.

Annex

Motion on
"Keeping up with technological development and enhancing the protection of people's privacy" moved by Dr Hon Priscilla LEUNG at the Council meeting of 22 May 2019

Motion as amended by Hon Elizabeth QUAT

That Hong Kong's existing legislation on the protection of personal privacy is incomprehensive, particularly there is no legislation to impose targeted regulation on Internet storage of personal privacy and data, and there is also no dedicated legislation for protecting children's Internet privacy, thus failing to deter lawbreakers from collecting, through Internet, children's privacy and data and invading their privacy, and even committing indecent conduct through such acts; serious incidents relating to large-scale leakage of personal privacy and data have occurred many times in Hong Kong, for example the uncovering of the resale of the data of 2.4 million customers by the Octopus Card Limited to other companies for marketing use in 2009, the Registration and Electoral Office's loss of a notebook computer containing the personal data of 3.78 million Geographical Constituencies electors across the territory in 2017, and the leakage of the personal data of 9.4 million passengers by the Cathay Pacific Airways in 2018; the Personal Data (Privacy) Ordinance came into force in 1996 and the Government only amended the Ordinance once in 2012, and given that the rapid technological development of the Internet, social media, big data, artificial intelligence, etc. has created privacy risks and that the General Data Protection Regulation ('GDPR') of the European Union ('EU') has come into force, the Personal Data (Privacy) Ordinance has appeared to be even more lagging behind and its personal data privacy protection is apparently inadequate; in this connection, this Council urges the Government to keep up with technological development and comprehensively review the policy on personal data privacy protection, so as to enhance the protection of people's privacy; the relevant proposals include:

(1) by drawing reference from the various measures and laws on the protection of Internet privacy of other jurisdictions, including the safeguards and requirements on restricting information storage in Internet and the notification regime for incidents, enacting legislation on the protection of Internet privacy applicable to Hong Kong ;

(2) by drawing reference from the laws of other jurisdictions, enacting dedicated legislation for protecting children's Internet privacy, including formulating requirements to restrict network operators' excessive collection and storage of children's privacy and data and prevent the invasion of children's privacy, so as to effectively protect children's personal privacy;

(3) by drawing reference from EU's GDPR and the relevant laws of other jurisdictions, amending the Personal Data (Privacy) Ordinance expeditiously and comprehensively, including requiring data users to notify the Privacy Commissioner for Personal Data ('PCPD') and data subjects of any data leakage incidents within a specified timeframe and raising the penalty of non-compliance with the enforcement notice to enhance the deterrent effect;

(4) regarding serious incidents relating to leakage of personal privacy and data, studying the introduction of more effective mechanisms for awarding compensation, empowering PCPD to exercise administrative penalties (such as fines), etc., so as to protect the rights and interests of members of the public and prompt for greater protection of personal data by data users;

(5) focusing on some enterprises' requirements for clients to provide non-service related personal data before using their services, conducting a review of the existing scope of permissible data collection by data users, including defining the meaning of sensitive personal data, and setting restrictions on the collection and storage of sensitive data, so as to enhance the protection of the people's personal data;

(6) requiring all government departments and public and private organizations to review their policies on processing personal data and security precautions, so as to avoid the recurrence of infringement of people's personal data privacy; and

(7) enhancing public promotion to raise the understanding and awareness of the people as well as of public and private organizations on protecting and respecting personal data privacy.

Appendix V

Relevant documents on
Review of the Personal Data (Privacy) Ordinance

Committee	**Date of meeting**	**Paper**
Panel on Constitutional Affairs ("CA Panel")	15.11.2010 (Item IV)	Agenda Minutes
	20.11.2010 (Item I)	Agenda Minutes
	20.3.2017 (Item V)	Agenda Minutes
Legislative Council ("LegCo")	8.11.2017	Official Record of Proceedings Pages 36 – 40
	29.11.2017	Official Record of Proceedings Pages 116 – 120
Panel on Information Technology and Broadcasting ("ITB Panel")	12.2.2018 (Item V)	Agenda Minutes
CA Panel	14.2.2018 (Item IV)	Agenda Minutes
CA Panel, ITB Panel and Panel on Security	14.11.2018 (Item II)	Agenda Minutes
LegCo	14.11.2018	Official Record of Proceedings Pages 23 – 34
	12.12.2018	Official Record of Proceedings Pages 53 – 63
Panel on Financial Affairs	7.1.2019 (Item V)	Agenda Minutes
LegCo	16.1.2019	Official Record of Proceedings Pages 158 – 162

Committee	**Date of meeting**	**Paper**
CA Panel	18.3.2019 (Item IV)	Agenda Minutes
LegCo	8.5.2019	Official Record of Proceedings Pages 84 – 88
	22.5.2019	Official Record of Proceedings Pages 216 – 270 Motion on "Keeping up with technological development and enhancing the protection of people's privacy" - Progress report
	6.11.2019	Official Record of Proceedings Pages 82 – 100
	13.11.2019	Official Record of Proceedings Pages 46-53

Council Business Division 2
Legislative Council Secretariat
13 January 2020