

立法會
Legislative Council

LC Paper No. CB(2)628/20-21(06)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

**Updated background brief prepared by the Legislative Council Secretariat
for the meeting on 18 January 2021**

Work of the Office of the Privacy Commissioner for Personal Data

Purpose

This paper summarizes previous discussions held by the Panel on Constitutional Affairs ("the Panel")¹ regarding the work of the Office of the Privacy Commissioner for Personal Data ("PCPD").

Background

2. The Office of PCPD is a statutory body responsible for overseeing the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") which protects the privacy of individuals in relation to personal data. The Office of PCPD is headed by PCPD appointed by the Chief Executive. According to section 5(4) of PDPO, PCPD shall hold office for a period of five years and shall be eligible for reappointment for not more than one further period of five years. Section 8 of PDPO prescribes the functions and powers of PCPD as set out in **Appendix I**. The Office of PCPD is funded mainly by recurrent subvention from the Government. Ms Ada CHUNG Lai-ling was appointed in July 2020 as the new PCPD with effect from 4 September 2020 for a term of five years, succeeding Mr Stephen WONG Kai-yi, the former PCPD.

3. Section 11(1) of PDPO provides for the establishment of the Personal Data (Privacy) Advisory Committee ("the Advisory Committee") to advise PCPD on matters relevant to the privacy of individuals in relation to personal data or implementation of PDPO. Chaired by PCPD, the Advisory Committee comprises members appointed by the Secretary for Constitutional and Mainland Affairs.

¹ With effect from the 2008-2009 legislative session, the policy area of personal data protection has been transferred from the Panel on Home Affairs to be placed under the purview of this Panel.

Amendment of the Personal Data (Privacy) Ordinance

4. In June 2012, the Personal Data (Privacy) (Amendment) Ordinance 2012 ("the Amendment Ordinance") was passed by the Legislative Council ("LegCo"). 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 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 ("ENs"); and to create a new offence for repeated contravention of the requirements under PDPO for which ENs have been served. Some of the provisions therein came into operation since 1 October 2012. The remaining provisions relating to the use and provision of personal data for use in direct marketing as well as the new legal assistance scheme were also brought into force on 1 April 2013.

Major issues discussed at Panel meetings

5. It is the usual practice of the Panel to receive a briefing by PCPD on the work of the Office of PCPD in each legislative session. The major issues raised at the relevant meetings are summarized below.

Protection of personal data in developing software/mobile applications and public education on privacy protection

6. In view of the popular use of online videoconferencing software during the coronavirus disease-2019 outbreak, some members expressed concern that certain software was said to have a number of data security loopholes (e.g. lack of end-to-end encryption) and thus be vulnerable to hacking attacks. These members enquired about the measures taken by the Office of PCPD to prevent abuse and misuse of personal data by software developers and operators.

7. The former PCPD advised that the Office of PCPD had issued guidelines on compliance with PDPO in developing software and mobile applications. To promote the adoption of "Privacy by Design" and "Privacy by Default" as core considerations of enterprises when developing information and communications technology ("ICT") systems, the Office of PCPD and Singapore's Personal Data Protection Commission had released a jointly-developed guide to assist enterprises in applying "data protection by design" principles by offering practical guidance for all phases of software development and good practices for data protection for ICT systems. Moreover, the Office of PCPD had provided guidance to users of

videoconferencing software in general through different channels. It had also written to schools to alert them of the risks when using videoconferencing software as an online teaching and learning platform.

8. Some members considered that many of the promotion and education activities conducted by the Office of PCPD could hardly arouse the interest of the general public in personal data protection. They suggested that efforts should be targeted at promoting public awareness of the legal responsibility of doxxing acts and the importance of personal data protection in new and innovative ways.

9. The former PCPD advised that the Office of PCPD had launched new accounts and revamped its page/channel on various social media platforms (e.g. Instagram, Twitter, Facebook and YouTube) in early April 2020, with a view to enhancing the dissemination of updated information on protection of personal data privacy to the general public, particularly the younger generation and those who preferred mobile devices to conventional media channels. Through these platforms, the latest privacy issues of public concern would be explained to the public in a plain language and with the help of visual illustrations and videos.

10. Some members also raised 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. In response to members' concern, the former PCPD conceded that the rapid development of big data, artificial intelligence and related technologies in recent years had created unanticipated privacy risks and 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. It 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.

11. Some members considered that more should be done by the Office of PCPD to educate the local companies and the public regarding the impact of the General Data Protection Regulation ("GDPR") enacted by the European Union ("EU").² These members pointed out that GDPR contained provisions requiring the data user and the data processor to designate a data protection officer and implement appropriate measures to ensure the security of personal

² GDPR became effective in May 2018 and has an extra-territorial application.

data. They enquired whether the aforementioned principle and provisions would be introduced in PDPO.

12. The former PCPD advised that the Office of PCPD had conducted a comparative study on EU GDPR and PDPO with a view to identifying the differences. The Office of PCPD would proactively assist local data users in understanding and complying with data protection regimes overseas. The former PCPD further advised that as GDPR had provided for various specific requirements regarding the appointment of the data protection officer, the feasibility of introducing similar provisions in PDPO would require further study and consultation with stakeholders concerned including small and medium enterprises ("SMEs").

Review of the Personal Data (Privacy) Ordinance

13. Some members took the view that the regulation of data protection should be enhanced through amendments to PDPO, in the wake of the three major incidents of personal data leakage by Cathay Pacific Airways Limited, TransUnion Limited and the Marriot International hotel group respectively in late 2018. These members were particularly concerned that there was no mandatory requirement under PDPO for an organization to file data breach notifications whether to the Office of PCPD or to its affected clients. Concern was also raised about the current lack of regulatory control of the transfer of consumer personal data (including credit data) among credit reference service agencies and their collaborating organizations, or to data processors overseas. In these members' view, the Office of PCPD could make reference to GDPR enacted by EU in proposing necessary amendments to PDPO to address the above issues.

14. The former PCPD advised that the Office of PCPD had drawn up initial recommendations on the review of PDPO regarding the enhancement of data breach notification arrangements, retention and disposal of personal data by data users, penalties for non-compliance with PDPO, and regulation of data processing activities by data processors (such as cloud service providers), etc. In June 2019, the Office of PCPD put forward to the Government its preliminary recommendations on PDPO amendments.³

15. At the briefing by the former PCPD on 20 April 2020, some members urged the Office of PCPD to step up its efforts to initiate investigations into

³ The Administration also embarked on a review of PDPO and studied possible amendments proposed by the Office of PCPD. On 20 January 2020, the Administration consulted the Panel on the preliminary amendment directions put forward by the Government as set out in LC Paper No. CB(2)512/19-20(03).

suspected cases relating to doxxing and cyberbullying and seek new ways to deter people from doxxing police officers.

16. The former PCPD explained that the Office of PCPD was not vested with the powers to conduct criminal investigation and prosecution for criminal offences under PDPO. As such, it had referred suspected criminal doxxing cases, i.e. those cases involving a potential contravention of section 64 of PDPO, to the Police. The former PCPD further advised that in the light of public concerns about doxxing and the difficulties encountered by the Office of PCPD in handling relevant cases, the Government and the Office of PCPD were studying how PDPO should be amended in order to curb doxxing behaviour more effectively.⁴

Enforcement power of the Privacy Commissioner for Personal Data

17. During discussion on review of PDPO, members had expressed diverse views at its various meetings on PCPD's 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 the Data Protection Principles ("DPPs").⁵ Nevertheless, members in general expressed concern that PCPD had inadequate powers for the effective enforcement of PDPO.

18. At the briefing by the then PCPD, Mr Allan CHIANG Yam-wang, on 15 November 2010, members further discussed the enforcement power of PCPD. The then 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

⁴ The Administration informed the Panel in January 2021 that it was studying with the Office of PCPD on concrete legislative amendment proposals, making reference to relevant data protection laws in other jurisdictions and Hong Kong's actual situation, with a view to drafting the amendment bill after consulting stakeholders in due course. The Administration's aim was to endeavour to complete formulation of concrete legislative amendment proposals within 2021 and to consult this Panel.

⁵ 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 EN. With effect from 1 October 2012, if a data user fails to take corrective actions for his contravention by the date specified in an EN, he will be liable to a fine at Level 5 (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 6 (at present \$100,000) and imprisonment for two years.

then 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 of Justice.

19. The Administration was of the view that in order to maintain checks and balances, 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 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.

Implementation of section 33 of the Personal Data (Privacy) Ordinance

20. Some members expressed grave concern about the slow progress in bringing section 33 of PDPO into operation to regulate the transfer of data outside Hong Kong. PCPD advised that his Office had submitted recommendations to the Government in 2014 and remained in close communication with the Administration on the matter. The Administration explained that the implementation of section 33 could bring about significant and substantive impact on businesses. The Administration had commissioned a consultant to study the compliance measures that data users would have to adopt in order to fulfil the requirements under section 33.

21. At the meeting on 15 May 2017, the Panel received a briefing by the Administration on the preliminary findings of the business impact assessment on the implementation of section 33 of PDPO. Some members relayed the concerns expressed by the industrial and commercial sectors about the potential impacts of the implementation of section 33 of PDPO, especially on SMEs, such as the high compliance cost that might be involved as a result of adopting measures to fulfil the requirements under section 33, as well as impacts on their operations and their online business.

22. The Administration advised that the consultant would first consolidate the final business impact assessment report, which was expected to be completed before the end of 2017. The representative of the Office of PCPD informed members that, upon receipt of the business impact assessment report, the Office of PCPD would study a number of issues relating to section 33 of PDPO, such as the Office of PCPD's mechanism for reviewing and updating the "white list" of jurisdictions with privacy protection standards comparable to that of Hong Kong, 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, and the support measures required by SMEs to comply with the relevant requirements. The study would take at least a year's time to complete. The Administration advised that it would then formulate the steps forward in the light of the outcome of the Office of PDPO's study.

23. At the briefing by the former PCPD on 20 April 2020, members were informed that the Office of PCPD engaged a consultant in November 2018 to provide specialist views on the implementation of section 33. The consultant recommended that the Office of PCPD should, amongst others, revise the recommended model clauses in the "Guidance on Personal Data Protection in Cross-border Data Transfer" ("the Guidance"),⁶ in order to enhance practicability and user-friendliness of the Guidance and facilitate organizational data users, including SMEs, to directly adopt the relevant clauses in data transfer agreements according to their business needs. The Office of PCPD had engaged the consultant to also review the Guidance, including to update the recommended model clauses in the Guidance for industries' reference, and to revise the Guidance, including updating the recommended good practices for cross-border data transfer agreements for better protection of personal data.

Recent development

24. PCPD will brief the Panel on an update of the work of the Office of PCPD at the next meeting on 18 January 2021.

Relevant papers

25. A list of relevant papers on the LegCo website is in **Appendix II**.

Council Business Division 2
Legislative Council Secretariat
14 January 2021

⁶ The Guidance was issued by the Office of PCPD in December 2014 to strengthen privacy protection for cross-border personal data transfer.

~~則行政長官可藉書面通知委任一人署理專員職位，直至(視情況所需)——(由 1999 年第 34 號第 3 條修訂)~~

- ~~(i) 新的專員根據第 5(3) 條獲委任為止；或
(ii) 專員回任為止。~~
- ~~(2) 根據第 (1) 款獲委任署理專員職位的人，在他獲委任的期間——~~
- ~~(a) 須執行專員在本條例下的職能；及
(b) 可行使專員在本條例下的權力。~~
- ~~(3) 第 6 條須適用於根據第 (1) 款獲委任署理專員職位的人，猶如該人是專員一樣。~~

8. 專員的職能及權力

- (1) 專員須——
- (a) 就遵守本條例條文作出監察及監管；
- (b) 促進及協助代表資料使用者的團體為第 12 條的施行擬備實務守則，以在遵守本條例條文(尤其是各保障資料原則)方面提供指引；
- (c) 促進對本條例的條文(尤其是各保障資料原則)的認識及理解以及遵守；
- (d) 對他認為可影響在個人資料方面的個人私隱的建議制定的法例(包括附屬法例)加以審核，並向建議制定該法例的人報告其審核結果；
- (e) 進行視察，包括對屬政府部門或法定法團的資料使用者所使用的任何個人資料系統的視察；
- (f) 為更佳地執行他的其他職能而對資料處理及電腦科技進行研究及監察其發展，以顧及該等發展在個人資料方面對個人私隱相當可能有的不利影響；
- (g) 與——
- (i) 在香港以外任何地方執行專員認為與其在本條例下的任何職能相似(不論全部或部分相似)的職能的人，進行聯絡及合作；及

~~then the Chief Executive may, by notice in writing, appoint a person to act as the Commissioner until, as the case requires— (Amended 34 of 1999 s. 3)~~

- ~~(i) a new Commissioner is appointed under section 5(3); or
(ii) the Commissioner resumes his office.~~
- ~~(2) A person appointed under subsection (1) to act as the Commissioner, whilst he is so appointed—~~
- ~~(a) shall perform the functions; and
(b) may exercise the powers,~~
- ~~of the Commissioner under this Ordinance.~~
- ~~(3) Section 6 shall apply to a person appointed under subsection (1) to act as the Commissioner as if that person were the Commissioner.~~

8. Functions and powers of Commissioner

- (1) The Commissioner shall—
- (a) monitor and supervise compliance with the provisions of this Ordinance;
- (b) promote and assist bodies representing data users to prepare, for the purposes of section 12, codes of practice for guidance in complying with the provisions of this Ordinance, in particular the data protection principles;
- (c) promote awareness and understanding of, and compliance with, the provisions of this Ordinance, in particular the data protection principles;
- (d) examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the person proposing the legislation;
- (e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government or statutory corporations;
- (f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and computer technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data;
- (g) liaise and co-operate with any person in any place outside Hong Kong—
- (i) performing in that place any functions which, in the opinion of the Commissioner, are similar (whether in whole or in part) to any of the Commissioner's functions under this Ordinance; and

(ii) 該等人士在某些相互關注的並涉及在個人資料方面的個人私隱的事項方面進行聯絡及合作；及

(h) 執行根據本條例或其他成文法則委予他的其他職能。

(2) 專員可作出所有為更佳地執行其職能而需要作出的或對此有助的所有事情，或為更佳地執行其職能而連帶須作出的所有事情，而在不影響前文的概括性原則下，專員尤可——

(a) 在認為任何類別的財產對——

(i) 為專員或任何訂明人員供給地方；或

(ii) 專員可執行的任何職能的執行，屬必要時，取得及持有該財產，並可在持有該財產所按的條款及條件的規限下，處置該財產；

(b) 訂立、履行、轉讓、更改或撤銷任何合約、協議或其他義務，或接受他人所轉讓的合約、協議或其他義務；

(c) 承辦及執行合法信託，但限於以推動專員在本條例下須予執行或准予執行的職能為宗旨的信託或具有其他類似宗旨的信託；

(d) 接受饋贈及捐贈，不論是否受信託所規限的饋贈或捐贈；

(e) 在獲得行政長官事先批准下，成為任何關注 (不論是全部或部分) 在個人資料方面的個人私隱的國際組織的正式成員或附屬成員； (由 1999 年第 34 號第 3 條修訂)

(f) 行使本條例或其他成文法則賦予他的其他權力。

(3) 專員在執行其職能或行使其權力時，可製備及簽立任何文件；凡任何與他執行職能或行使權力所合理附帶或相應引起的事宜，專員亦可在與該等事宜有關連的情況下，製備及簽立任何文件。

(4) 任何文件如看來是以專員的印章簽立的，須予接納為證據，在沒有相反證據的情況下須當作已妥為簽立。

(5) 為向資料使用者提供指引，專員可不時安排擬備不抵觸本條例的指引以顯示他擬執行其在本條例下任何職能或行使其在本條例下任何權力的方式，並安排將該指引藉憲報公告刊登。

(ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data; and

(h) perform such other functions as are imposed on him under this Ordinance or any other enactment.

(2) The Commissioner may do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and in particular but without prejudice to the generality of the foregoing, may—

(a) acquire and hold property of any description if in the opinion of the Commissioner such property is necessary for—

(i) the accommodation of the Commissioner or of any prescribed officer; or

(ii) the performance of any function which the Commissioner may perform,

and, subject to the terms and conditions upon which such property is held, dispose of it;

(b) enter into, carry out, assign or accept the assignment of, vary or rescind, any contract, agreement or other obligation;

(c) undertake and execute any lawful trust which has as an object the furtherance of any function which the Commissioner is required or is permitted by this Ordinance to perform or any other similar object;

(d) accept gifts and donations, whether subject to any trust or not;

(e) with the prior approval of the Chief Executive, become a member of or affiliate to any international body concerned with (whether in whole or in part) the privacy of individuals in relation to personal data; (Amended 34 of 1999 s. 3)

(f) exercise such other powers as are conferred on him under this Ordinance or any other enactment.

(3) The Commissioner may make and execute any document in the performance of his functions or the exercise of his powers or in connection with any matter reasonably incidental to or consequential upon the performance of his functions or the exercise of his powers.

(4) Any document purporting to be executed under the seal of the Commissioner shall be admitted in evidence and shall, in the absence of evidence to the contrary, be deemed to have been duly executed.

(5) The Commissioner may from time to time cause to be prepared and published by notice in the Gazette, for the guidance of data users, guidelines not inconsistent with this Ordinance, indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under this Ordinance.

**Relevant documents on the Work of
the Office of the Privacy Commissioner for Personal Data**

Committee	Date of meeting	Paper
Panel on Constitutional Affairs	20.3.2017 (Item V)	Agenda Minutes
	15.5.2017 (Item IV)	Agenda Minutes
	14.2.2018 (Item IV)	Agenda Minutes
	18.3.2019 (Item IV)	Agenda Minutes
	20.4.2020 (Item V)	Agenda Minutes