For discussion
on 20 January 2020

Legislative Council Panel on Constitutional Affairs

Review of the Personal Data (Privacy) Ordinance

Purpose

This paper seeks Members' views on the review of the Personal Data (Privacy) Ordinance ("PDPO").

Review of the PDPO

2. Amidst the rapid development of information and communication technologies as well as widespread use of the internet and mobile communication, technological advances have brought about considerable new challenges to the protection of personal data privacy. The cause of incidents of personal data privacy breaches has recently shifted from mostly involving improper collection or use of personal data or direct marketing in the past, to those related to digital platforms and data security, such as personal data breaches, hacker attacks resulting from security loopholes and improper disclosure of personal data of others on online platforms. The spate of major personal data breach incidents last year has also raised public concerns about the adequacy of the PDPO in protecting personal data privacy.

3. The Government is reviewing and studying possible amendments to the PDPO jointly with the Office of the Privacy Commissioner for Personal Data ("PCPD") with a view to strengthening the protection for personal data. We

have referred to the General Data Protection Regulation ("GDPR") of the European Union ("EU"), as well as experience and legislation of other jurisdictions during the review and the directions for legislative amendments. We will also keep in view the development trends in various jurisdictions, especially the EU, regarding privacy protection enhancement and consider the actual situation of Hong Kong in order to bring the proposed amendments up to date. The PCPD has put forward to the Government earlier its preliminary recommendations on PDPO amendments. Our present study focuses on the amendment directions set out below. Members' views on the preliminary amendment directions are welcomed.

Proposed Amendments to the PDPO

(I) <u>Mandatory Data Breach Notification Mechanism</u>

4. Data Protection Principle ("DPP") 4 under the PDPO states that data users shall take all practicable steps to prevent unauthorised or accidental access of personal data. However, there is currently no statutory requirement for the data user to notify the PCPD or the data subject in the case of a data breach. At present, relevant notification is made on a voluntary basis. Introducing a mandatory notification mechanism that requires a data user to notify the PCPD and the relevant data subject of any data breach incident will help ensure that the Privacy Commissioner for Personal Data ("the Commissioner") could monitor the handling of data breaches by the organisations concerned. Such organisations could also seek instructions from the Commissioner for follow-up to mitigate or prevent further damage resulting from the data breach.

5. We are of the initial view that the following should be considered in the establishment of a mandatory data breach notification mechanism:

(a) Definition of "personal data breach": could mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[1];

(b) Notification threshold: A data breach having "a real risk of significant harm" should be reported by the data user to the PCPD and impacted individuals. We are considering whether the same threshold should apply to notification to both the PCPD and to impacted individuals, and what factors the data user should take into account when determining whether a data breach has reached that notification threshold, such as the type and amount of data leaked, the security level of the data involved (e.g. whether the leaked data is encrypted), etc.;

(c) Notification timeframe: When the data user becomes aware of a data breach, the data user should notify the PCPD within a specified timeframe (e.g. as soon as practicable and, under all circumstances, in not more than five business days). The PCPD should also be empowered to direct the data user to give notification to the impacted individuals. We are considering whether it is necessary to allow a specified period for the data user to investigate and verify the suspected data breach incident before making notification within the timeframe; and

(d) Mode of notification: We are considering allowing the data user to make written notification to the PCPD by way of email, fax or post. Possible information to be specified in the notification include a description of the data security incident, the cause of the data breach,

[1] The definition is referenced to Article 4(12) of the GDPR of the EU.

the type and amount of personal data involved, an assessment of the risk of harm, the remedial action taken by the data user to mitigate the risk of harm and the action that the data subjects should take to protect themselves against the risk of harm. The PCPD also plans to provide templates of and guidelines on the notification mechanism to facilitate notification by data users.

(II) Data Retention Period

6. Currently, DPP2 under the PDPO provides that data users shall take all practicable steps to 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. However, DPP2 does not specify when such personal data is "no longer necessary". We note that the approach is similar in the data protection laws of other jurisdictions, in which no definite retention period for personal data is spelt out.

7. The longer the data is retained, the higher the risk for a data breach and the more severe the impact. Retention of personal data that should have been purged would result in unnecessary privacy risks. However, given the diverse service nature and unique needs of different organisations, it is practically infeasible to set uniform retention period under the PDPO and apply it to all types of personal data held by different organisations for different purposes. Therefore, mandating a uniform retention period may be inappropriate.

8. We are currently considering amending the PDPO to require data users to formulate a clear retention policy which specifies a retention period for the personal data collected. A retention policy should cover a number of aspects, such as the maximum retention periods for different categories of personal data; legal requirements which may affect the designated retention periods (e.g. regulations pertaining to taxation, employment and certain professions like legal

and medical); and how the retention period is counted (e.g. upon collection of personal data, cessation of the business of the data user, or end of its membership relationship with the data subjects, etc.).

9. At present, DPP5(a) under the PDPO requires data users to take all practicable steps to ensure that a person can ascertain the data user's policies and practices in relation to personal data. We are considering amending DPP5 to expressly require the personal data policy of data users to include a data retention policy, so that data users must ensure that the persons concerned are clearly informed of the details of the retention policy and that it will be executed effectively. The PCPD also plans to provide templates of and guidelines on retention policies for the industry to refer to in the formulation and clear specification of retention policies.

(III) Sanctioning Powers

10. Depending on the offences, criminal fines under the existing PDPO are set at Level 3 (HK$10,000), Level 5 (HK$50,000) and Level 6 (HK$100,000) pegged to the level of fines for offences specified in Schedule 8 to the Criminal Procedure Ordinance[2].

11. At present, the PCPD may issue an enforcement notice directing a data user to remedy the data user's contravention of DPPs under the PDPO. The data user is liable to a fine or imprisonment if the contravention continues after the enforcement notice is served. The maximum penalty for non-compliance with an enforcement notice is a criminal fine at Level 5 (i.e. HK$50,000[3]) and

[2] Section 35 of the PDPO also provides for criminal fines of HK$500,000 and HK$1,000,000 specifically for offences relating to direct marketing. These penalties of fines target at offences such as providing personal data in direct marketing without the data subject's consent, failure of a data user to notify the data subject when using personal data in direct marketing for the first time, and providing personal data of a data subject for use in direct marketing. In addition, section 64 of the PDPO provides for a criminal fine of HK$1,000,000 specifically for disclosing personal data obtained from data users without consent.

[3] Among the convicted cases of non-compliance with enforcement notices issued under the PDPO, the amount of fines imposed by the court so far ranged from HK$1,000 to HK$5,000.

imprisonment for two years on first conviction. To reflect the severity of the offences and enhance the deterrent effect of the PDPO, one of our study directions is to raise the relevant criminal fine levels.

12. In addition, we note that a number of data protection authorities abroad (such as that in the EU, Singapore and the United Kingdom) are empowered to directly impose administrative fines for contravention of data protection laws. Hence, we are also exploring the feasibility of introducing direct administrative fines in Hong Kong as an administrative penalty.

13. Details currently under consideration include:

(a) Threshold for imposing administrative fines: If empowered to impose administrative fines, the PCPD shall have a set of factors to consider whenever it decides for or against issuing such a fine. The factors may include the data compromised, the severity of the data breach, the data user's intent for the breach and attitude of breach handling, the remedial action taken by the data user and the track record of the data user, etc;

(b) Level of administrative fines: Among the overseas jurisdictions we have made reference to, the maximum administrative fine imposable under the GDPR of the EU is €20 million (equivalent to about HK$178 million) or 4% of the company's global annual turnover in the preceding year, whichever is higher. We are now exploring the feasibility of introducing an administrative fine linked to the annual turnover of the data user, and the possibility of classifying data users of different scales according to their turnovers to match with different levels of administrative fines; and

(c) Mechanism for imposing administrative fines: The PCPD will be required to issue to the data user an administrative fine notice specifying the circumstances of the breach, the investigation findings, the indicative level of fine and the rationale for the penalty so as to ensure transparency of the PCPD's order for administrative fines. To enhance fairness of the administrative fine system, the data user should be given appropriate time to make representation upon receipt of the administrative fine notice and have the right to appeal to the administrative appeals board against the notice.

(IV) Regulation of Data Processors

14. 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[4] or sub-contractors adopt measures to ensure the safety of personal data. The outsourcing of data activities like sub-contracting personal data processing work to other service providers has become more common. However, in the event of data breaches, the absence of direct regulation on data processors under the existing PDPO may render data processors neglect the importance of preventing personal data leakage. Regulating data processors by laws will not only strengthen protection, but also pose a fairer sharing of responsibilities between data users and data processors.

15. Drawing reference from a number of overseas regulatory authorities which introduce direct regulation of data processors or require data processors to observe specific requirements (e.g. in relation to data retention, erasure and security), we have set our study direction towards direct regulation of data processors by imposing legal obligations on them or sub-contractors. For instance, data processors may be required to be directly accountable for personal

[4] As defined in DPP2 of 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.

data retention and security, and to make notification to the PCPD and the data user upon being aware of any data breach.

(V) Definition of Personal Data

16. 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 analytics technology nowadays, expanding the definition of "personal data" under the PDPO to cover information relating to an "identifiable" natural person would better satisfy public expectation towards the protection of personal data. In a number of jurisdictions examined, the definition of "personal data" also includes data that relates to an "identifiable" natural person. We hold the view that amending the definition of "personal data" under the PDPO could raise the protection for personal data.

17. A summary of the overseas regulatory regimes in respect of the above proposed amendment directions is at **Annex 1**.

(VI) Regulation of Disclosure of Personal Data of Other Data Subjects

18. Apart from the major data breach incidents which have given rise to the above legislative amendments, we are deeply concerned about the incidents of doxxing that took place over a recent period of time in the society. The PCPD has received and proactively uncovered over 4 700 doxxing-related complaint and enquiry cases from 14 June 2019, and has referred over 1 400 cases to the Police for further investigation in accordance with the law.

19. The victims of doxxing are from all sorts of backgrounds and all walks of life with various views, including police officers and their family members, Government officials and public servants, members of the public who have stated their support for or disagreement with the Government or the Police, etc.

20. As at 31 December 2019, the PCPD has also approached and written for over 140 times to the operators of relevant websites, online social networking platforms or discussion forums urging them to remove over 2 500 web links, of which close to 70% have been removed. In addition, the PCPD has requested the platforms concerned to publish warnings stating that doxxing or cyberbullying may violate section 64 of the PDPO. As of 31 December 2019, a total of eight persons were arrested by the Police for alleged violation of such provision.

21. Furthermore, on 25 October 2019, the Department of Justice sought an injunction order from the court restraining any person from using, publishing, communicating or disclosing personal data of any police officer(s) or their family members intended or likely to intimidate, molest, harass, threaten or pester any police officer(s) or their family members without consent of the persons concerned; from intimidating, molesting, harassing, threatening or pestering any police officer(s) or their family members; or from assisting, inciting, abetting or authorising others to commit any of these acts. As at 31 December 2019, the PCPD has referred 40 cases it had received and found to have allegedly violated the injunction order of the court to the Department of Justice for follow-up.

22. The Government is studying how to amend the PDPO in order to curb doxing behaviour more effectively. Directions under consideration include to consider introducing legislative amendments to more specifically address doxxing, conferring on the Commissioner statutory powers to request the removal of doxxing contents from social media platforms or websites, as well as the powers to carry out criminal investigation and prosecution, etc.

Advice Sought and Way Forward

23. Members are invited to note the content of this paper and offer views on the above proposed directions.

24. Taking Members' responses into account, we will work with the PCPD to conduct further in-depth study on concrete legislative amendment proposals and consult relevant stakeholders, including this Panel, in due course.

Constitutional and Mainland Affairs Bureau

January 2020

Annex 1

Summary of
Relevant Regulatory Regimes in Other Jurisdictions

Data Breach Notification Mechanism

a. Threshold to notify regulatory authority/impacted individuals

Australia	Threshold to notify regulatory authority: notification must be made when there is unauthorised access to or unauthorised disclosure of information and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to any of the individuals to whom the information relates. Threshold to notify impacted individuals: notification must be made when there is unauthorised access to or unauthorised disclosure of information and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the individuals to whom the information relates.
Canada	Threshold to notify regulatory authority: when the organisation reasonably believes that there exists a "real risk of significant harm" to an individual as a result of a data breach incident. Threshold to notify impacted individuals: when the organisation reasonably believes that there exists a "real risk of significant harm" to an individual as a result of a data breach incident.

European Union ("EU")	Threshold to notify regulatory authority: notification of a data breach shall be made by the organisation to the relevant regulatory authority "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". Threshold to notify impacted individuals: when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.
New Zealand	Threshold to notify regulatory authority/impacted individuals: when it is reasonable to believe that the data breach has caused or is likely to cause serious harm to the impacted individuals. (as proposed in the Privacy Bill before the parliament[1])

b. Notification timeframe

Australia	Timeframe to notify regulatory authority: as soon as practicable. According to the guidelines issued by the regulatory authority, the data user may carry out an assessment within 30 days from first becoming aware of any suspected data breach. Timeframe to notify impacted individuals: as soon as practicable.
Canada	Timeframe to notify regulatory authority: as soon as feasible.

[1] The Privacy Bill 2018 was read a second time in the Parliament on 7 August 2019, subject to further discussion and deliberation in the Committee of Whole House.

	Timeframe to notify impacted individuals: as soon as feasible.
EU	Timeframe to notify regulatory authority: without undue delay and, where feasible, not later than 72 hours after having become aware of the data breach. The General Data Protection Regulation ("GDPR") allows data users to provide the required information in phases, as long as it is done without undue further delay. Timeframe to notify impacted individuals: without undue delay.
New Zealand	Timeframe to notify regulatory authority: as soon as practicable. (as proposed in the Privacy Bill before the parliament) Timeframe to notify impacted individuals: as soon as practicable. (as proposed in the Privacy Bill before the parliament)

c. Mode of notification

Australia	Mode of notifying regulatory authority: the data user must make an online notification to the regulatory authority. Mode of notifying impacted individuals: the data user must notify the impacted individuals directly. If direct notification to the impacted individuals is not practicable, the data user must

	publish a copy of the statement (i.e. the notification made to the regulatory authority) on the data user's website and take reasonable steps to bring the contents of the statement to the attention of individuals at risk of serious harm.
Canada	Mode of notifying regulatory authority: the data user must make a notification in writing or by any secure means of communication. Mode of notifying impacted individuals: the data user must make a direct notification in person or by telephone, mail, email or any other forms of communication. If direct notification is likely to cause further harm to the impacted individuals or undue hardship to the organisation, or if the organisation does not have contact information of the impacted individuals, the organisation can make an indirect notification by public communication or similar measures.
EU	Mode of notifying regulatory authority: Member States may further specify the mode of notification through their own data protection legislation. Mode of notifying impacted individuals: the data user must make a direct notification to the impacted individuals. If direct notification involves disproportionate effort, there must instead be a public communication or similar measure whereby the impacted individuals are informed in an equally effective manner. Acceptable ways of notification include email, SMS, mail, prominent web banners or notices/prominent advertisements on print media.

New Zealand	Mode of notifying regulatory authority: the regulatory authority will provide guidelines on the mode and requirements of notification after the Privacy Bill is passed. Mode of notifying impacted individuals: if it is not reasonably practicable to notify the impacted individuals or members of groups these impacted individuals belong to, the data user must give public notice of the breach. (as proposed in the Privacy Bill before the parliament)

d. Consequences of failure to make notifications

Australia	Interference with the privacy of an individual by a body corporate is liable to civil penalties of up to AU$2.1 million.
Canada	Organisations may be criminally fined up to CA$100,000 by the court.
EU	A fine of up to €10 million or 2% of the organisation's total worldwide annual turnover, whichever is higher. Apart from administrative fines, other corrective measures under Article 58 of the GDPR may be imposed by the authority.
New Zealand	Failure to notify the Privacy Commissioner without reasonable excuse may result in a criminal fine of up to NZ$10,000 imposed by court. (as proposed in the Privacy Bill before the parliament)

Data Retention Period

a. Provisions regarding data retention period

Australia	The organisation must take such steps as are reasonable in the circumstances to destroy the personal data that is "no longer needed" for the allowed purposes.
Canada	Personal data should be retained for only as long as necessary for the fulfilment of the original collection purposes. Organisations (data users) should develop guidelines to specify the minimum and maximum retention periods.
EU	Personal data should be kept for no longer than is necessary for the original processing purposes.
New Zealand	An agency (data user) shall not keep personal data for longer than is required for the purposes for which the data may lawfully be used.
Singapore	An organisation (data user) shall cease to retain personal data as soon as it is reasonable to assume that the personal data is no longer necessary for any legal, business or other collection purposes.

Sanctioning Power

a. Power of regulatory authority to impose administrative fines

Australia	No
Canada	No
EU	Yes. Violations of the GDPR are liable to two levels of administrative fines depending on the nature of the breach. A number of factors for consideration are specified under the GDPR for the determination of whether to impose an administrative fine and the level of the fine. The regulatory authority of Member States have the discretion to decide on the most appropriate corrective measures and whether to impose an administrative fine in respect of the case.
UK	Yes. The Information Commissioner's Office has the power to impose monetary penalties (even before enactment of the GDPR).
New Zealand	No
Singapore	Yes. Financial penalties are reserved only for serious breaches when correction directions alone do not sufficiently reflect the seriousness.

b. Level of Sanctions

Australia	Though not empowered to impose administrative fines, the Australian Information Commissioner may apply to court for civil penalty orders for serious and repeated interferences with privacy. Fines of up to AU$420,000 for an individual and AU$2.1 million for a business organisation may be ordered.
Canada	Not applicable
EU	A data user/data processor failing to comply with the GDPR may be liable to: (i) upper tier: an administrative fine of up to €20 million or up to 4% of the organisation's total worldwide annual turnover of the preceding year, whichever is higher; (ii) lower tier: an administrative fine of up to €10 million or up to 2% of the organisation's total worldwide annual turnover of the preceding year, whichever is higher.
New Zealand	Not applicable
Singapore	The data protection authority is empowered to direct an organisation to pay a financial penalty of up to S$1 million for not complying with the requirements on data collection, use, disclosure, access, correction and care.

Regulation of Data Processors

a. Whether data processors are directly regulated

Australia	Yes
Canada	Yes
EU	Yes
New Zealand	Yes
Singapore	Yes (on requirements for security arrangement for and retention of personal data only)

b. How data processors are regulated

Australia	Entities engaged in processing personal information are subject to the Privacy Act 1988 in the collection, holding, use or disclosure of personal information.
Canada	Data processors are subject to direct and indirect regulation. ● Direct regulation: The data protection law (the Personal Information Protection and Electronic Documents Act) applies to every organisation that collects, uses or discloses personal information in the course of commercial activities. ● Indirect regulation: A data user that transfers personal

	information to a data processor for processing must use contractual or other means to ensure that the information receives a comparable level of protection while it is being processed by a data processor.
EU	Data processors are subject to direct and indirect regulation. ● Direct regulation: Data processors must maintain records of processing activities, process data under the data controllers' instructions, ensure security of personal data, report data breaches to the data controllers promptly, appoint data protection officers and comply with provisions in respect of cross-border data transfer, etc. ● Indirect regulation: The GDPR requires data controllers to appoint or choose data processors that can provide sufficient guarantees in respect of technical and organisational measures which meet the GDPR requirements. Data controllers must use contractual means to include specified provisions in the contracts signed with data processors.
New Zealand	Persons or organisations that hold or process personal information must comply with the Privacy Act 1993.
Singapore	Data processors are subject to direct and indirect regulation. ● Direct regulation: Data protection obligations directly apply to data processors, including reasonable requirements for security arrangement for and retention of personal data. ● Indirect regulation: Data processors are also indirectly regulated through contractual arrangements made with data users. Data users remain legally responsible the personal data processed by data processors and must ensure that the

	processing by the data processors complies with the Personal Data Protection Act 2012.

Definition of Personal Data

Australia	Information or an opinion, whether true or not and whether recorded in a material form or not, about an identified individual or an individual who is reasonably identifiable.
Canada	Information about an identifiable individual.
EU	Any information relating to an identified or identifiable natural person. "An identifiable natural person" refers to a natural person who can be identified, directly or indirectly, in particular by reference to: (a) identifiers such as names, location data or online identifiers; or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
New Zealand	Information about an identifiable individual.
Singapore	Data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.