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.