Legislative Council Panel on Constitutional Affairs
Consultation Document on
Review of the Personal Data (Privacy) Ordinance

INTRODUCTION

On 28 August 2009, we issued the Consultation Document on Review of the Personal Data (Privacy) Ordinance to invite public views on the proposals to amend the Ordinance. Copies of the Consultation Document have been passed to all Members of the Legislative Council. This paper briefs Members on the background of the consultation exercise, and summarizes the major proposals.

BACKGROUND

2. The Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) has been in force since 1996. The major provisions of the PDPO are summarised at the Annex. Over the last decade or so, we have witnessed the rapid advancement in information technology, prevalence of the Internet and exponential growth of e-commerce. Increasing use of information and communications technology has helped enhance Hong Kong's competitiveness and efficiency, and bring more convenient and user-friendly services to the community. At the same time, it has brought new challenges to the protection of personal data privacy. It is important to ascertain the adequacy of the PDPO in the light of these developments.

3. Moreover, having regard to the community's increasing concern about personal data privacy protection, it is important to review whether the regulation of personal data should be tightened in certain circumstances. There is also a need to streamline the operation of the PDPO and address technical problems encountered in the implementation of the Ordinance.

4. We, with the support of the Privacy Commissioner for Personal Data ("PCPD"), has conducted a comprehensive review of the PDPO to examine whether the existing provisions of the Ordinance still afford adequate protection to personal data having regard to developments, including advancement in technology, in the last decade.

PUBLIC CONSULTATION EXERCISE

5. A considerable number of the proposals studied in the review will impact on various sectors of the community, public and private organizations as well as members of the public. For instance, some of the proposals, especially those relating to the regulation of sensitive personal data and data processors and personal data security breach notifications, might lead to additional compliance cost for business operations. On the other hand, enhancing the protection to personal data privacy would safeguard the free flow of personal data involved in financial and economic activities to Hong Kong, which would be in the interests of business operations of Hong Kong. A balance has to be struck between the compliance cost for the community as against the benefits of enhanced personal data protection. It is also important to ensure that any amendments to the PDPO should not be introduced at the expense of Hong Kong's competitiveness.

6. We see the need to conduct a public consultation exercise to gauge public views on the proposals, before deciding on the way forward. We have an open mind on the proposals and welcome the views of the community in this regard. The consultation period will end on 30 November 2009.

GUIDING PRINCIPLES

7. In conducting the review, we are guided by the following :

(a) the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests;

(b) balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology;

(c) any changes to the privacy law should not undermine Hong Kong's competitiveness and economic efficiency as an international city;

(d) the need to avoid putting onerous burden on business operations and individual data users;

(e) due account should be given to local situations;

(f) the PDPO should remain flexible and relevant in spite of technological change;

(g) legislative intervention may not always be the most effective way. In certain circumstances, personal data privacy protection may be achieved by administrative measures; and

(h) consensus in the community about the privacy issues is important.

PROPOSALS

8. In the review, we have studied 12 major proposals concerning sensitive personal data, data security, enforcement powers of the PCPD, and offences and sanctions. They are set out in Chapters Three to Six of the consultation paper. Fifteen other proposals which have considerable impact on the community on which comments are invited are set out in Annex 1 to the consultation paper. They are mainly related to rights of data subjects, rights and obligations of data users, enforcement powers of the PCPD and introducing new exemptions. There are nine proposals which we have considered but are inclined not to pursue, which are set out in Annex 2 to the consultation paper. They mainly involve the scope of regulation under the PDPO, exemptions and powers of the PCPD. There are 16 miscellaneous proposals which include mainly amendments to streamline the operation of the PDPO and address technical and operational problems encountered in the implementation of the PDPO, which are at Annex 3 to the consultation paper.

9. The 12 key proposals covered by Chapters Three to Six of the consultation paper are highlighted in paragraphs 10 to 25 below.

Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

10. At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. More stringent regulation of sensitive personal data is in line with international practices. However, there is no universally agreed set of sensitive personal data and perception of sensitive personal data is culture-bound. Given the challenges posed by the development of biometric technology on an

individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data.

11. To provide a higher degree of protection to sensitive personal data, we have set out in the consultation paper a possible regulatory model to limit the handling of sensitive personal data by data users to specified circumstances in order to narrow down the scope of collection and use of such data.

Data Security

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

12. The rising trend of data users sub-contracting and entrusting data processing work to third parties has increased the risk to which personal data may be exposed. At present, the PDPO does not regulate processors which process personal data for data users. To strengthen security measures governing personal data entrusted to data processors, we have set out possible regulatory options.

13. Under such options, a data user who transfers personal data to a data processor for holding, processing or use, would be required to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the personal data, and to ensure that the data are not misused and are deleted when no longer required for processing.

14. As part of the options, we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted. Recognising that compliance with certain requirements may pose problems for some data processors due to the operational constraints unique to specific industry sectors, we have also included the option of subjecting different categories of data processors to different obligations.

Proposal No. 3: Personal Data Security Breach Notification

15. Following the spate of personal data leakage incidents, questions have been raised on whether a personal data security breach notification ("privacy breach notification") system should be instituted to require data

users to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data so as to mitigate the potential damage to affected individuals. A mandatory notification requirement could impose undue burden on business operations. Bearing in mind that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we consider it more prudent to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community. For this purpose, the PCPD can issue guidelines on voluntary privacy breach notifications.

Enforcement Powers of the PCPD

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

16. At present criminal investigations are conducted by the Police and prosecutions by the Department of Justice. We have considered whether these powers should be conferred on the PCPD. Since some offences proposed in this review are not technical in nature and involve a fine and imprisonment, there could be concern if such powers are delegated to the PCPD. Moreover the existing arrangements have worked well. We do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

17. Under Section 66 of the Ordinance, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user. The PDPO does not empower the PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings. To achieve greater deterrent effect on acts or practices which intrude into personal data privacy and enhance the overall effectiveness of sanctions provided for under the PDPO, views are invited on whether the PCPD should be conferred with the power to provide legal assistance to an aggrieved data subject.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

18. We have considered whether the PCPD should be empowered to determine the amount of compensation to a data subject who suffers

damage by reason of a contravention of a requirement by a data user, as an alternative to the existing redress avenue to seek compensation through the court as provided for under Section 66 of the PDPO. The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC") Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1994. The LRC opined that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the Data Protection Principles ("DPPs"). It would be for a court to determine the appropriate amount of compensation payable. Views are invited on whether it is appropriate to introduce an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

19. The PCPD is empowered to remedy contravention of a DPP by issuing an enforcement notice to direct the data user to take remedial steps. Contravention of the enforcement notice is an offence.

20. One option is to consider making contravention of a DPP an offence. Bearing in mind that DPPs are couched in generic terms and can be subject to a wide range of interpretations, to make contravention of a DPP a criminal offence would have significant impact on civil liberties, if an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether we should make contravention of a DPP an offence.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

21. Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. To curb irresponsible dissemination of leaked personal data, we may consider making it an

offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.

Proposal No. 9: Repeated Contravention of a DPP on Same Facts

22. Under the PDPO, if a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently does the same act or engages in the same practice, the PCPD would issue another enforcement notice. Since the enactment of the PDPO, PCPD has not come across any such case of circumvention. To forestall possible circumvention of the regulatory regime, one option is to consider making it an offence if a data user repeats such contravening act. However, this would be moving away from the original intent of adopting the DPPs in the PDPO. Views are invited on whether this is appropriate.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of DPPs

23. We have considered the option of empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. It is not common for non-judicial bodies to have the statutory power to impose monetary penalties. Under the PDPO, the DPPs are couched in generic terms and can be subject to wide interpretations. Although we may require the PCPD to issue guidance on the circumstances he considers appropriate to issue a monetary penalty notice, whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. Views are invited on whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

24. The PDPO does not provide for heavier sanction for data users who repeatedly contravene an enforcement notice. Since the enactment of the PDPO, there has not been a problem with repeated offenders. We have considered the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect. Views are invited on whether there is a need to impose a heavier penalty for such repeated offenders.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

25. Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of a fine at Level 3 (up to $10,000) may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. To curb misuse of personal data in direct marketing activities, we may consider raising the penalty level for misuse of personal data in direct marketing. Public views are invited on the appropriate level of penalty.

WAY FORWARD

26. Following this round of public consultation, we will consolidate the views received. When we have general directions on the way forward, we will arrange for further public discussions on possible legislative proposals.

CONCLUSION

27. Members are invited to express views on this paper.

Constitutional and Mainland Affairs Bureau
August 2009

Major Provisions of the Personal Data (Privacy) Ordinance

The PDPO applies to any data relating directly or indirectly to a living individual, from which it is reasonably practicable to ascertain the identity of that individual and which are in a form in which access to or processing of is reasonably practicable. The Ordinance binds all data users (i.e. persons who control the collection, holding, processing or use of personal data) in both public and private sectors.

2. The PDPO gives statutory effect to internationally accepted data protection principles, which govern the fair and lawful collection of personal data, data quality, use, disclosure and retention of personal data, data security, openness of personal data policies, and right of data subjects (i.e. persons who are the subjects of the personal data) to access and correct their personal data. The gist of the six DPPs, which must be followed by data users, are set out below :

(a) DPP 1 (purpose and manner of collection of personal data) which provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user who is to use the data. Only personal data that are necessary for or directly related to the purpose should be collected, and that the data collected should be adequate but not excessive for those purposes. In addition, it provides for the lawful and fair means of collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject;

(b) DPP 2 (accuracy and duration of retention of personal data) which requires all practicable steps to be taken to ensure that personal data should be accurate and kept no longer than necessary;

(c) DPP 3 (use of personal data) which provides that unless with the prescribed consent of the data subject, personal data should be used for the purposes for which they were collected or a directly related purpose;

(d) DPP 4 (security of personal data) which requires a data user to take all practicable steps to protect the personal data held against unauthorized or accidental access, processing, erasure or other use;

(e) DPP 5 (information to be generally available) which requires a data user to take all practicable steps to ensure openness about his personal data policies and practices, the kinds of personal data he holds and the main purposes for which personal data are used;

(f) DPP 6 (access to personal data) which provides that a data subject has the right of access to and correction of his personal data.

3. The PDPO gives rights to data subjects. They have the right to confirm with data users whether the latter hold their personal data, to obtain a copy of such data from data users at a fee which is not excessive, and to have their personal data corrected. They may complain to the PCPD about a suspected breach of the requirements of the PDPO and claim compensation for damage caused to them as a result of a contravention of the PDPO through civil proceedings.

4. The PDPO imposes conditions on the use of personal data in automated matching processes. The Ordinance also regulates the use of personal data in direct marketing by data users.

5. The PDPO provides specific exemptions from the requirements of the Ordinance. They include :

(a) a broad exemption from the provisions of the Ordinance for personal data held by an individual for domestic or recreational purposes;

(b) an exemption from DPP 3 (use of personal data principle) for statistics and research purposes;

(c) exemptions from the requirements on subject access (i.e. DPP 6 and Section 18(1)(b) of the Ordinance) for certain employment-related personal data; and

(d) exemptions from the use limitation requirements and subject access (i.e. DPP 3, DPP 6, and Section 18(1)(b)) of the Ordinance to cater for a variety of competing public and social interests, such as security, defence and international relations, prevention or detection of crime, assessment or collection of tax or duty, news activities, and health.

6. Under the PDPO, contravention of a DPP by itself is not an offence. If, following the completion of an investigation, the PCPD is

of the opinion that a data user is contravening a requirement (including a DPP) under the PDPO or has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated, the PCPD may, having regard to the damage or distress caused to the data subject, serve an enforcement notice on the data user, directing him to take such steps as are specified in the notice to remedy the contravention. If the data user fails to comply with the enforcement notice issued by the PCPD, he is liable to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily fine of $1,000.

7. Separately, a variety of offences are provided for under the PDPO for contravention of various requirements under the Ordinance (other than a contravention of a DPP). The penalty levels range from a fine at Level 3 (up to $10,000) to a fine at Level 5 (up to $50,000) and imprisonment for two years. Non-compliance with an enforcement notice attracts the highest level of penalty under the PDPO.

8. The PDPO also provides an avenue for an individual who suffers damage, including injury to feelings, as a result of a contravention of the Ordinance to seek compensation from the data user concerned by instituting civil proceedings.