Legislative Council Panel on Constitutional Affairs

Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance

Introduction

This paper briefs Members on the result of the public consultation on the review of the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) and the legislative proposals drawn up in the light of the views received during the public consultation and recent developments, including cases of transfer of customer personal data by some enterprises to others for direct marketing purposes. The Report on Public Consultation on Review of the PDPO ("consultation report"), which is issued today, is at the **Annex**.

Background

2. The PDPO, enacted in 1995, requires updating in order to afford adequate protection to personal data privacy having regard to technological and other developments in the last decade or so. With the support of the Privacy Commissioner for Personal Data ("PCPD"), we had conducted a review on the PDPO. We then published a consultation document in August 2009 for a three-month public consultation until November 2009 on the proposals arising from the review. A total of 178 submissions were received. We also organised two public forums and two District Council forums to gauge the views of the community and met with representatives of sectors and organisations interested in the review or took part in the forums or seminars organised by them.

Result of Public Consultation

3. The views received during the public consultation showed that most of the proposals in our consultation document are generally supported by the public, while some proposals are more complex and public views on them are diverse. Separately, the recent cases of transfer of customer personal data by some enterprises to others for direct marketing purposes (monetary gains are involved in some cases) have aroused widespread concern. Having carefully considered the views received during the public consultation and the public concerns arising

from these incidents and consulted the PCPD, we intend to take forward 37 proposals, including some new proposals on direct marketing and related matters. A summary of the proposals to be taken forward and those we do not intend to pursue can be found on pages i to xiii of the consultation report at the Annex. The major ones are explained in paragraphs 4 to 36 below.

Proposals to be Taken Forward

(A) Direct Marketing and Related Matters

Collection and Use of Personal Data in Direct Marketing (Proposal (1) in the consultation report)

4. The PDPO already contains provisions regulating the collection and use (whose meaning under the PDPO includes "transfer") of personal data. Data Protection Principle ("DPP") 1(3) provides that a data user (i.e. a person who controls the collection, holding, processing or use of the data) should take all practicable steps to ensure that the data subject (i.e. the individual who is the subject of the data) is explicitly informed, on or before collecting personal data from the data subject, of the purpose (in general or specific terms) for which the data are to be used and the classes of persons to whom the data may be transferred. DPP 3 stipulates that, without the prescribed consent of the data subject, personal data shall not be used for any purpose other than the purposes for which the data were to be used at the time of collection or a directly related purpose[1].

5. A major criticism arising from the recent cases of transfer of customer personal data by enterprises to others for direct marketing purposes is that some enterprises, in collecting personal data, do not explicitly and specifically inform the customers of the purposes for which the data collected are to be used, or the identity of the persons to whom the data may be transferred (the transferees). Moreover, the relevant information is given in small print. In many cases, the application form for the service or the contract is designed in such a way to seek the

[1] Contravention of a DPP by itself is not an offence under the PDPO. Instead, the PCPD is empowered to remedy the breach by issuing an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he/she commits an offence and is liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

applicant's/customer's bundled consent to the terms and conditions of the service, the purposes for which the personal data collected are to be used, and the classes of persons to whom the personal data may be transferred.

6. These business practices have given rise to concerns that the existing legislation is too general and not specific enough to afford adequate protection to personal data privacy. To address these concerns, the PCPD has just issued a new guidance note on the collection and use of personal data for direct marketing, replacing the existing Guidance Note on "Cross Marketing Activities" and Fact Sheet on "Guidelines on Cold-Calling". The new guidance note provides practical guidelines to assist practitioners to comply with the provisions of the PDPO. It will also draw their attention to recommended practices in personal data privacy protection.

7. In addition, we propose to amend the PDPO so that the legislation will, in addition to providing general principles and requirements, stipulate specific requirements on data users if they intend to use (including transfer) the personal data collected for direct marketing purposes. In formulating the legislative amendments, we are mindful that direct marketing has been increasingly popular as a major sales channel in recent years, with many companies and employees directly engaging in such activities. It provides consumers with information on goods and services available on the market. Some consumers may also be interested in receiving information on promotional offers. The general view in the community is not to prohibit enterprises from using customer personal data for direct marketing purposes, but rather customers should be given an informed choice as to whether to allow data users to use their personal data for such purposes.

8. In light of the aforementioned considerations, we propose to introduce in the PDPO the following additional specific requirements on data users <u>who intend to use (including transfer) the personal data collected for direct marketing purposes</u>:

(a) the data user's Personal Information Collection Statement ("PICS") should be <u>reasonably specific</u> about the <u>intended direct marketing activities</u> (whether by the data user himself/herself or the transferee(s)), the <u>classes of persons</u> to whom the data may be transferred for direct marketing purposes and the <u>kinds of data</u> to be transferred for direct marketing purposes, so that the data subjects will have an adequate understanding of how their personal data will be

(b) the presentation of the part of the data user's PICS on the intended direct marketing activities (whether by the data user himself/herself or the transferee(s)), the classes of persons to whom the data may be transferred for direct marketing purposes and the kinds of data to be transferred for direct marketing purposes should be understandable and reasonably readable by the general public; and

(c) regarding the issue of bundled consent, the data user should, on or before collecting the personal data, provide an option for the applicant to choose (e.g. by ticking a checkbox) not to agree to the use (including transfer) of his/her personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees.

9. We propose that non-compliance with any of the new requirements in paragraph 8 above will be subject to the issue of an enforcement notice by the PCPD. Failure to comply with the enforcement notice will be an offence, as currently provided for under the PDPO. We propose that, to tie in with the entry into force of the new requirements, the PCPD should take into account the new requirements and revise the guidance note mentioned in paragraph 6 above or replace it with a Code of Practice to provide guidance on the new requirements. He will consult the relevant stakeholders as appropriate in the preparation of the revised guidance note or Code of Practice. The PCPD will also launch a publicity and public education programme to promote understanding of the new requirements by both data users and data subjects, and assist data users in complying with the new requirements.

10. We also propose that a data user commits an offence and is liable on conviction to a fine of $500,000 and imprisonment for three years, if he/she:

(a) does not comply with any of the requirements in paragraph 8 and subsequently uses (including transfers) the personal data for direct marketing purposes; or

(b) complies with those requirements but uses (including transfers) the personal data collected for a direct marketing activity or transfer the data to a class of transferees to which the data subject has indicated disagreement; or

(c) (i) uses (including transfers) the personal data collected for a direct marketing activity;

(ii) transfers for direct marketing purposes the data to a class of persons; or

(iii) transfers for direct marketing purposes a kind of personal data

not covered in the PICS.

11. In addition, under section 34(1)(b)(ii) of the PDPO, a data user shall not use any personal data for the purpose of carrying out direct marketing activities if the data subject has previously requested the data user to cease to so use his/her personal data. The consultation document proposed to increase the penalty for contravening this requirement. Views received during the public consultation generally supported the proposal. In order to have sufficient deterrent effect and to bring the penalty in line with that for the new offences in paragraph 10 above, we propose to raise it from the existing penalty of Level 3 ($10,000) to a fine of $500,000 and imprisonment for three years.

Unauthorised Sale of Personal Data by Data User
(Proposal (2) in the consultation report)

12. The PDPO currently does not prohibit the sale of personal data. If a data user uses personal data for a purpose (e.g. sale) which is not the purpose for which the data were to be used at the time of collection or a directly related purpose, he/she contravenes DPP 3 and is subject to the issue of an enforcement notice by the PCPD.

13. Following the recent cases of transfer of customer personal data, some of which involved monetary gains, there are calls from some quarters of the community for criminalising the sale of personal data by data users. There are, however, views that the resulting damage does not warrant outright criminalisation. The personal data protection laws of many jurisdictions such as the United Kingdom, Australia and New Zealand do not prohibit or criminalise such sale. On the other hand, some consider that data users should be allowed to sell personal data if the data subjects consent to the sale for various reasons such as there being something in return for them. Having considered the issue, one possible option is as follows:

(a) if a data user is to sell personal data (whether collected from the data subject directly by the data user or obtained from another source) to another person for a monetary or in kind gain, the data user should, before doing so, inform the data subject in writing of the kinds of personal data to be sold and to whom the personal data will be sold;

(b) the presentation of the notice to provide the data subject with the information in (a) above should be understandable and reasonably readable by the general public;

(c) the data user should provide the data subject with an opportunity to indicate whether he/she agrees to ("opt-in model") or disagrees with ("opt-out model") the sale; and

(d) it will be an offence for a data user to sell personal data to another person for a monetary or in kind gain without complying with the requirements in (a) to (c) above or against the wish of the data subject.

14. On paragraph 13(c) above, the merit of the opt-in model is that the explicit consent of the data subject has to be sought, while the opt-out model is in line with that currently adopted under section 34 of the PDPO regarding the use of personal data in direct marketing (see paragraph 11 above) and that under the proposal in paragraph 8(c) above. We welcome public views on which model to prescribe, or other approaches such as allowing flexibility for individual data users to adopt an appropriate model.

15. We also propose that non-compliance with any of the requirements in paragraph 13(a) to (c) above will be subject to the issue of an enforcement notice by the PCPD. As regards the penalty for contravention of the requirement in paragraph 13(d) above, we welcome public views. For reference, the penalty for a broadly similar offence[2]

[2] Section 58(1) of the UEMO provides that a person to whom an unsubscribe request is sent shall not use any information obtained thereby other than for the purpose of complying with the relevant requirements (including the requirement to comply with the unsubscribe request). A person who contravenes section 58(1) commits an offence and is liable on summary conviction to a fine at Level 6 ($100,000). A person who knowingly contravenes section 58(1) commits an offence and is liable upon conviction on indictment to a fine of $1,000,000 and imprisonment for five years.

under section 58(1) of the Unsolicited Electronic Messages Ordinance ("UEMO") (Cap. 593) is cited in the consultation report.

Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent
(Proposal (3) in the consultation report)

16. The consultation document proposed to make it an offence for a person who discloses for profits or malicious purposes personal data which he/she obtained from a data user without the latter's consent. Views received during the public consultation generally supported the proposal but some has raised concerns about the definition of "for malicious purposes". As such, we propose to take forward this proposal, and suggest that a possible formulation is to define "malicious purposes" as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another". On penalty, some suggest that it should be set at a higher level so as to achieve deterrent effect. One option is to set the penalty at the same level as that for the new offence concerning unauthorised sale of personal data as mentioned in paragraph 15 above.

(B) Data Security

Regulation of Data Processors and Sub-contracting Activities
(Proposal (5) in the consultation report)

17. Currently, a data user is held liable under section 65(2) of the PDPO for any act done by the data processor[3] entrusted by him/her. The consultation document invited public views on whether :

(a) we should continue to regulate data processors indirectly through the data users but go one step further to require data users to use contractual or other means to ensure that its data processors comply with the requirements under the PDPO; or

(b) data processors should be regulated directly under the PDPO.

[3] A data processor is an agent which holds, processes or uses personal data solely for a data user and does not hold, process or use the data for his/her own purposes.

18. The views received generally supported the direction of strengthening the regulation of data processors and sub-contracting activities. As regards whether direct or indirect regulation of data processors should be implemented, public views were diverse. For those who supported direct regulation, the majority view was that, if indirect regulation was adopted, an unfair and onerous burden might be put on the data users as the responsibility of overseeing the compliance of data processors with personal data protection requirements would rest with the data users. On the other hand, those opposing direct regulation opined that it was impractical to put data processors under a direct regulatory regime since many data processors only provided a platform for processing of data and might not know whether the data being handled by them contained personal data, or the use purpose of the data. Adopting a direct regulatory regime would increase the burden and operating costs of the industry.

19. Having considered the views received, we propose to continue with indirect regulation but go one step further to require the data user to use contractual or other means to ensure that its data processors and sub-contractors, whether within Hong Kong or offshore, comply with the requirements under the PDPO. Contravention of the requirement will render the data user liable to the issue of an enforcement notice by the PCPD. We also propose that the PCPD should step up publicity and public education on the outsourcing of personal data processing and where necessary, prepare codes of practice to provide guidance on matters such as provisions of contracts between data users and data processors.

Personal Data Security Breach Notification
(Proposal (6) in consultation report)

20. The consultation document examined whether a 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. The consultation document suggested to start with a voluntary notification system first so that we could assess the impact of breach notifications more precisely and fine-tune the notification requirements to make them more reasonable and practicable, without causing onerous burden on the community.

21. The majority of the views received supported a voluntary notification system. The main consideration was that privacy breach notification system was still in the development stage and there were no clear or objective standards for notification or common practices. There were worries about how the system was going to operate and the onerous burden brought to data users if a mandatory notification system was to be implemented. Respondents also suggested that guidelines should be drawn up, covering the circumstances under which notification should be triggered and other details.

22. We intend to adopt a voluntary notification system. In this regard, in June 2010, the PCPD promulgated a guidance note entitled "Data Breach Handling and the Giving of Breach Notifications" to assist data users in handling data breaches and to facilitate them in giving data breach notifications. We will work with the PCPD on the promotional and educational initiatives that can be taken by the PCPD to raise awareness of the guidance note, promote the adoption of a data breach notification system by data users voluntarily and assist data users to make appropriate notification.

(C) Powers of the PCPD

Legal Assistance to Data Subjects under Section 66 (Proposal (7) in the consultation report)

23. The consultation document examined whether the PCPD should be conferred with the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under section 66 of the PDPO, along the lines of the Equal Opportunities Commission ("EOC") model.

24. The views received generally supported this proposal. We intend to take forward this proposal. Along the lines of the EOC model, we propose that the legal assistance should include giving the applicant advice as to whether the evidence for the case is sufficient, arranging for a lawyer from the Office of the PCPD to act as the legal representative of the applicant, arranging for the representation of the applicant by a solicitor of the Office of the PCPD or a solicitor employed outside the Office of the PCPD during the legal proceedings, and providing any form of assistance which the PCPD considers appropriate. To ensure good use of public funds, the PCPD will be required to, when considering whether to accede to a request for legal assistance, take into account whether the case raises a question of principle, or it is difficult for the

applicant to deal with the case unaided, having regard to the complexity of the case or the applicant's position in relation to the respondent or another person involved.

Circumstances for Issue of an Enforcement Notice (Proposal (8) the in consultation report)

25. Under section 50(1) of the PDPO, the PCPD, following completion of an investigation, may serve an enforcement notice on a data user if he is of the opinion that the relevant data user (a) is contravening a requirement under the PDPO, or (b) has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated.

26. There can be situations where the contravention has ended and will unlikely be repeated but the damage or distress caused by the contravention would last. To enhance the effectiveness of the PDPO in the protection of personal data privacy, we propose to amend section 50(1) of the PDPO to provide that the PCPD may serve an enforcement notice on a data user if he is of the opinion that the relevant data user (a) is contravening a requirement under the PDPO, or (b) has contravened such a requirement, irrespective of whether it is likely that the contravention will continue or be repeated.

(D) New Offences and Sanctions

Repeated Contravention of a Data Protection Principle on Same Facts (Proposal (18) in the consultation report)

27. The consultation document invited public views on whether it should be made an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice in breach of a DPP for which the PCPD had issued an enforcement notice.

28. There were both supporting and opposing views on this proposal. Those who opposed considered that as DPPs are couched in general terms, making a breach of a DPP (whether a first-time or repeated breach) an offence would have adverse impact on commercial operations. We consider that, as the wordings of enforcement notices are specific, data users who take proper measures to comply with the enforcement notices should not normally commit the same contravening acts again. Taking

into account the need to forestall deliberate circumvention of the regulatory regime, we propose to take forward the proposal. We propose to set the penalty at a fine at Level 5 ($50,000) and imprisonment of two years, which is the same as the penalty for non-compliance with an enforcement notice.

Repeated Non-compliance with Enforcement Notice
(Proposal (19) in the consultation report)

29. The consultation document examined whether heavier penalty should be imposed for a second or subsequent contravention of enforcement notice. The views received generally supported this proposal. As for the penalty, the fine for a second or subsequent conviction of the same offence under some other legislation such as the Control of Obscene and Indecent Articles Ordinance (Cap. 390) doubles that for the first conviction while the term of imprisonment sentence remains the same. We propose to set the penalty for repeated non-compliance with enforcement notice at a fine at Level 6 ($100,000) (as against a fine at Level 5 ($50,000) for first time contravention) and imprisonment of two years (which is the same as that for first time contravention).

Proposals not to be Taken Forward

Sensitive Personal Data
(Proposal (38) in consultation report)

30. The consultation document examined whether there would be a need to accord better protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances, and whether the possible regulatory regime set out in the consultation document, including coverage of sensitive personal data, related regulatory measures and sanctions, was appropriate. While most of the views received supported the general direction of strengthening the protection for certain types of sensitive personal data, there were diverse views on the coverage of sensitive personal data, mode of regulation and sanctions. There were also strong objections from the information technology ("IT") sector to the proposal to classify biometric data as sensitive personal data.

31. The proposal would have wide impact on the community, and there are no mainstream views in the community on the coverage of

sensitive personal data and the mode of regulation. We, therefore, do not propose to institute a statutory regulatory regime for sensitive personal data at this stage. We will keep in view the community's discussion on the protection of sensitive personal data and the developments in overseas jurisdictions on regulation of sensitive personal data, before we further consider whether to pursue any necessary legislative amendments. We also propose that:

(a) the PCPD should step up promotion and education and where necessary, issue a code of practice or guidelines to suggest good practices on the handling and use of sensitive personal data in general, such as biometric data and health records; and

(b) the PCPD should continue to discuss with the IT sector possible measures to enhance the protection of biometric data.

Granting Criminal Investigation and Prosecution Power to the PCPD (Proposal (39) in consultation report)

32. The consultation document examined whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo of vesting these powers in the Police and the Department of Justice respectively should be maintained.

33. The majority of views received considered it important to have separate organisations to handle investigations and prosecutions in order to ensure checks and balances. They agreed with the view in the consultation document that it would not be appropriate to confer the PCPD with criminal investigation and prosecution powers and that the existing arrangements, which had been working smoothly, should be maintained. We, therefore, do not intend to take forward the proposal.

Empowering the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal (40) in consultation report)

34. The consultation document examined whether it would be appropriate to introduce another redress avenue (in addition to the existing avenue for an aggrieved data subject to seek compensation through the court under section 66 of the PDPO) by empowering the PCPD to award compensation to aggrieved data subjects who suffer

damage by reason of a contravention of a requirement under the PDPO by data users.

35. The majority of views received considered it inappropriate to confer the enforcement power and power to grant compensation to the same organisation. They opposed empowering the PCPD to determine the amount of compensation which, in their view, should be determined by the court. We, therefore, do not intend to take forward the proposal.

Imposing Monetary Penalty on Serious Contravention of DPPs (Proposal (42) in the consultation report)

36. The consultation document examined whether it would be appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs to enhance deterrent effect. The majority of views received considered that the existing sanction against contravention of DPPs should be retained. They also considered it inappropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs as this would put the enforcement power and power to impose penalty in the same organisation. We, therefore, do not intend to take forward the proposal.

Way Forward

37. We are going to launch further public discussions on the legislative proposals contained in the consultation report. Members of the public may submit their views from now until 31 December 2010. We will organise two public forums on 4 and 29 November 2010 and arrange discussion sessions with relevant organisations and stakeholders for in-depth discussions on the details of the proposals planned to be taken forward so as to ensure smooth operation of the amended PDPO.

Constitutional and Mainland Affairs Bureau
18 October 2010