Legislative Council Panel on Constitutional Affairs

Review of the Personal Data (Privacy) Ordinance and Related Matters

Introduction

At the meeting of the Panel on 18 October 2010 and the meeting with deputations on 20 November 2010, Members discussed the proposals set out in the Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance ("PDPO") ("the consultation report"). We have also organised two public forums and attended discussion sessions/forums to solicit the views of the relevant sectors on the proposals. Questions and comments have been raised on the various proposals in the consultation report. This paper elaborates on the major proposals, and sets out the major questions and views raised on those proposals and our responses. This paper also provides information on the related matters of transfer of personal data outside Hong Kong and data user returns.

Collection and Use of Personal Data in Direct Marketing

The proposal

2. The collection and use of personal data for direct marketing activities is subject to the existing provisions of the PDPO on collection and use of personal data. The Privacy Commissioner for Personal Data (PCPD) has also issued a new guidance note on the collection and use of personal data in direct marketing. Details are at the **Appendix**.

3. In addition, the use of personal data for direct marketing purposes is now regulated by section 34 of the PDPO, which adopts an "opt-out" mechanism. Section 34 stipulates that if a data user uses personal data obtained from any source for direct marketing purposes, he/she must, the first time he/she so uses the personal data, inform the data subject that he/she is required to cease to so use the data if the data subject so requests. Section 34(1)(b)(ii) provides that, if the data subject requests the data user not to use his/her personal data for direct marketing purposes, the data user shall cease to so use the data. A data user who, without reasonable excuse, contravenes this requirement commits an offence and is liable on conviction to a fine at Level 3 ($10,000).

4. In the consultation report, we propose to amend the PDPO to stipulate the following additional specific requirements on data users if they intend to use (the meaning of which under the PDPO includes "transfer") the personal data collected for direct marketing purposes -

(a) the data user's Personal Information Collection Statement ("PICS") should be reasonably specific about 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;

(b) the presentation of the information in (a) should be understandable and reasonably readable by the general public; and

(c) the data user should provide an option for the data subject to choose, e.g. by ticking a checkbox, not to agree (i.e. an "opt-out" mechanism) 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.

5. We propose that non-compliance with any of the new requirements in paragraph 4 above will be subject to the issuing of an enforcement notice by the PCPD. Failure to comply with the enforcement notice will be an offence[1].

6. 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 new requirements in paragraph 4 and subsequently uses (including transfers) the personal data for direct marketing purposes; or

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

[1] The penalty for non-compliance with an enforcement notice is a fine of $50,000 and imprisonment for two years.

(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.

7. In brief, the proposal is a two-step approach. The first step involves a breach of the new requirements in paragraph 4 above, which will be subject to the issue of an enforcement notice by the PCPD. The second step involves non-compliance with the new requirements and subsequent use (including transfer) of the personal data for direct marketing purposes as set out in paragraph 6 above, which will be an offence. The data user will be liable on conviction to a fine of $500,000 and imprisonment for three years.

"Opt-in" mechanism versus "opt-out" mechanism

8. The consultation report proposes to adopt the "opt-out" mechanism for the enhanced regulation of collection and use of personal data in direct marketing (paragraph 4(c) above). This is in line with the "opt-out" mechanism currently adopted under section 34 of the PDPO. Separately, the Unsolicited Electronic Messages Ordinance ("UEMO"), which regulates direct marketing activities in the form of electronic communications, adopts an "unsubscribe" regime[2], which is essentially an "opt-out" mechanism.

9. At the meetings on 18 October and 20 November 2010, different views were expressed on whether the "opt-in" or "opt-out" mechanism should be adopted. The direct marketing and some other business sectors oppose the "opt-in" mechanism. Their view is that practically, it is much more difficult to obtain the express consent of customers as many customers may not read in detail the PICS or would not bother to give express consent even if they may not object to direct marketing calls or messages. Adopting the "opt-in" mechanism will affect seriously the

[2] The UEMO requires a sender of commercial electronic messages to provide a "functional unsubscribe facility" to enable the registered user of an electronic address to notify the sender that he/she does not wish to receive further commercial electronic messages from that sender.

business of and employment opportunities in the direct marketing industry. An "opt-out" mechanism will give data subjects a clear channel to opt out if they so wish, thus striking a better balance between protection of rights of data subjects and the continued survival of the direct marketing industry in Hong Kong. The direct marketing sector also pointed out that they were not aware of a single country that universally adopted the "opt-in" mechanism.

10. On the other hand, advocates of the "opt-in" mechanism consider that such a mechanism can better protect the interests of data subjects as data users are allowed to use the personal data only when data subjects have given express consent. The right of deciding how to use their personal data should be left to the data subjects themselves. The advocates also consider it inappropriate to assume data subjects' agreement if they have not expressed disagreement.

11. Members also asked about overseas experience. In this regard, jurisdictions including the United States, Canada, United Kingdom, France, Germany, Australia and New Zealand adopt an "opt-out" mechanism to regulate the use of personal data in direct marketing in general. In some jurisdictions like the United Kingdom, France and Germany, the relevant legislation adopts an "opt-in" mechanism for direct marketing activities conducted through certain channels such as emails, short messages, fax and automated calls. However, all the abovementioned jurisdictions adopt the "opt-out" mechanism for person-to-person telemarketing activities.

12. The Administration attaches great importance to the protection of personal data privacy and at the same time, is committed to maintaining Hong Kong's business-friendly environment. Our consideration is that a data subject should be given an informed choice as to whether to allow the use of his/her personal data for direct marketing purposes and, on the other hand, any changes to the legislation should not undermine Hong Kong's competitiveness and economic efficiency. We will continue to listen to the views of the community and examine the views received carefully before putting forward proposed legislative amendments.

Unauthorised Sale of Personal Data by Data User

<u>The proposal</u>

13. The consultation report proposes that 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 –

(a) 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 information in (a) above should be understandable and reasonably readable by the general public; and

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

14. We also propose to make it an offence for a data user to sell personal data to another person for a monetary or in kind gain without complying with any of the requirements in paragraph 13(a) to (c) above or against the wish of the data subject.

15. The above proposal is a two-step approach. The first step involves non-compliance with the proposed requirements in paragraph 13(a) to (c) above, which will be subject to the issuing of an enforcement notice by the PCPD. The second step involves sale of personal data without complying with the requirements in paragraph 13(a) to (c) above or against the wish of the data subject, which will be an offence. As regards the penalty, we welcome public views and propose to make reference to the penalty for a broadly similar offence under section 58(1) of the UEMO, which is up to a fine of $1,000,000 and imprisonment for five years.

<u>"Opt-in" mechanism versus "opt-out" mechanism</u>

16. The Administration has an open mind on whether to adopt the "opt-in" or "opt-out" mechanism for the proposal concerning unauthorised sale of personal data (paragraph 13(c) above). We welcome public views. The merit of the "opt-in" mechanism is that the explicit consent of the data subject has to be sought, while the "opt-out" mechanism is in line with that currently adopted under section 34 of the PDPO and that proposed for the new requirement in paragraph 4(c) above.

17. The major views received on this particular issue are similar to those on the proposal concerning the collection and use of personal data for direct marketing, as summarised in paragraphs 9 and 10 above. We will continue to listen to the views of the community and examine carefully the views received before putting forward legislative amendments, bearing in mind that confusion may result if different mechanisms are adopted for regulating the collection and use of personal data for direct marketing and unauthorised sale of personal data.

18. For Members' reference, as far as we understand, most overseas jurisdictions such as the United Kingdom, Australia and New Zealand do not criminalise the sale of personal data by data users. A few jurisdictions such as the Mainland, Australia and Denmark prohibit the sale of personal data by certain classes of data users or under certain circumstances.

Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent

19. The consultation report proposes to make it an offence for a person to disclose for profits or malicious purposes personal data which he/she obtained from a data user without the latter's consent. One example is sale of customers' personal data which an employee obtained from his company without the company's consent. This proposal aims to criminalise irresponsible acts of disclosure for profits or malicious purposes of personal data obtained without authorisation which intrude into personal data privacy and/or cause harm to the data subjects. As regards the definition of "malicious purposes", having made reference to relevant legislation, we propose in the consultation report that one possible option is to define it as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another".

20. We have received comments and concerns that activities of web-users might be caught by this proposal with such a definition of "malicious purposes". We would like to point out that this proposal only targets acts involving disclosure for profits or malicious purposes of personal data obtained from data users without the latter's consent. We will continue to listen to public views on the proposal, including the defences to be provided, and fine-tune the proposal where appropriate.

Powers and Functions of the PCPD

Legal assistance for aggrieved data subjects

21. In the consultation report, we propose to empower the PCPD to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings under section 66 of the PDPO against a data user to seek compensation for damage by reason of a contravention of the a requirement under the PDPO. Most of the responses so far are supportive of the proposal. However, there are questions on whether there would be means testing of the financial resources of the applicant, the assistance to be provided and the factors to be considered by the PCPD in granting legal assistance.

22. We have made reference to other legal assistance schemes including that provided by the Equal Opportunities Commission (EOC). We propose that, similar to the EOC's arrangements, there should not be any means test and the PCPD will provide the following assistance -

(a) giving legal advice on the sufficiency of evidence;

(b) arranging for a lawyer from the Office of the PCPD to act as the legal representative of the applicant;

(c) arranging for either a lawyer from the Office of the PCPD or an outside lawyer to represent the applicant in legal proceedings; and

(d) providing any form of assistance which the PCPD considers appropriate.

23. We also propose that the PCPD should consider an application for legal assistance on the basis of the following factors -

(a) the case raises a question of principle; or

(b) 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 or any other matter.

Granting criminal investigation and prosecution power to the PCPD

24. In the consultation report, we indicate that we do not intend to pursue the proposal to confer the PCPD with the power to carry out criminal investigations and prosecutions. We consider it important to retain the existing arrangement, under which the Police conducts criminal investigations and the Department of Justice undertakes prosecutions, in order to maintain checks and balances.

25. Some Members and deputations have suggested that the PCPD should be granted criminal investigation and prosecution power, so that he would have teeth in enforcing the PDPO. There are also views that the PCPD should be conferred with prosecution power, as in the case of such statutory bodies as the Vocational Training Council, Employees Compensation Assistance Fund Board and Construction Workers Registration Authority.

26. On the other hand, some other Members and deputations agree that criminal investigation and prosecution powers should be vested in separate organisations, as is the current case, to maintain checks and balances. They do not see strong justifications for departing from this arrangement for the PDPO.

27. We would like to point out that the PDPO already confers on the PCPD the powers to conduct investigations and inspections, and related powers to discharge these investigative functions, including entry into premises, summoning witnesses and requiring the concerned persons to furnish any information to the PCPD. Our view is that criminal investigation and prosecution powers should be vested in separate organisations to ensure checks and balances. As regards the prosecution power of the statutory bodies mentioned in paragraph 25 above, the offences concerned are mostly minor or of a simple nature, or are under legislation regulating individual trades. The PDPO has a broader coverage and the penalties for offences under it involve fines and imprisonment. Besides, some of the new offences proposed under the current review of the PDPO are of a more complicated nature and the proposed penalties are higher.

28. The PCPD has expressed concern that the Police does not accord priority to investigation into criminal offences under the PDPO. We have taken up the matter with the Police. The Police has stressed that it always attaches importance to handling cases referred by the PCPD. It has issued guidelines to front line officers setting out procedures in

handling cases referred by the PCPD. In addition, a designated police officer at Senior Superintendent level in every Police region will handle the referred case in person and assign it to appropriate unit in a timely manner for investigation. The Police is also open to the PCPD's suggestion of formulating joint policies and guidelines with the Police and the Department of Justice for referral of cases to be investigated and prosecuted under the PDPO. The Police will continue to work with the PCPD to tackle cases involving contraventions of the PDPO.

Empowering the PCPD to award compensation to aggrieved data subjects

29. In the consultation report, we indicate that we do not intend to pursue the proposal to empower the PCPD to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user. We do not consider it desirable to vest in a single authority both enforcement and punitive functions.

30. While some Members and commentators agree with the Administration's stance, individual commentators are of the view that the civil remedy under section 66 of the PDPO is costly to pursue and propose that the PCPD should be empowered to award compensation to aggrieved data subjects.

31. We would like to draw Members' attention to the "Report on Reform of the Law Relating to Protection of Personal Data" issued by the Law Reform Commission (LRC) in August 1994, in which the LRC opined that the PCPD's role should be limited to determining whether there had been a breach of Data Protection Principles (DPPs). It would be for a court to determine the amount of compensation payable and it would be undesirable to vest in a single authority both the enforcement and punitive functions. Our view is that this consideration remains valid.

Empowering the PCPD to impose monetary penalty on serious contravention of DPPs

32. The PCPD proposes to empower him to impose monetary penalty on serious contravention of DPPs so as to achieve the necessary deterrent effect. We do not intend to pursue this proposal. As pointed out by the LRC in its 1994 report, it is undesirable to vest in a single authority both enforcement and punitive functions. In Hong Kong, it is uncommon for non-judicial bodies to have the power to impose monetary penalties.

We do not see sufficient justifications for departure from this arrangement for the PCPD. In addition, we have proposed to make certain serious contraventions offences, such as unauthorised sale of personal data.

Related Matters

Transfer of personal data out of Hong Kong

33. Section 33 of the PDPO, which has not yet come into operation, prohibits the transfer of personal data to a place outside Hong Kong except in specified circumstances, including –

(a) where the place has been specified by the PCPD by notice in the Gazette as having in force a law substantially similar to, or serves the same purposes as, the PDPO;

(b) where the data subject has consented in writing to the transfer; or

(c) where the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data are afforded appropriate protection.

34. Pending the commencement of section 33, transfer of personal data outside Hong Kong is governed by the provisions of the PDPO concerning use (the meaning of which under the PDPO includes "transfer") of data, including DPP3 on use limitation. A data user is not allowed to transfer personal data to a place outside Hong Kong without the consent of the data subject unless the transfer is for a purpose the same as or directly related to the original purpose of the collection of the data. In addition, so long as a data user is able to control, in or from Hong Kong, the holding, processing or use of the personal data outside Hong Kong, the provisions of the PDPO will apply. If a data user outsources the processing of the personal data to an offshore agent, any act done by its offshore agent in breach of the PDPO will be treated as done by the data user and the data user is held liable.

35. Commencement of the operation of section 33 will impose more stringent regulation on the transfer of personal data to places outside Hong Kong and have significant implications on data transfer activities of various sectors such as the banking and telecommunications sectors.

36. We need to take into account the relevant factors, including the need for consulting stakeholders to assess the readiness of the community for the operation of section 33, international developments, and assistance required by the industry, such as guidelines issued by the PCPD. Moreover, the PCPD needs to specify in the Gazette the places with legislation substantially similar to, or serves the same purposes as, the PDPO. We are working with the PCPD to map out the way forward for considering the possibility of bringing section 33 into operation.

Data user returns

37. Sections 14 to 17 of the PDPO provide for a data user returns scheme (DURS), under which the PCPD may by notice in the Gazette specify a class of data users to which the DURS applies, after consultation with such bodies representative of data users belonging to that class and other interested parties. A data user of the specified class shall submit to the PCPD an annual return in the specified form containing information prescribed in Schedule 3 to the PDPO[3] together with a fee prescribed by the PCPD in a regulation in accordance with section 69 of the PDPO. Under sections 15 and 16, the PCPD shall, based on the returns, maintain a register of data users which shall be made available for public inspection without charge.

38. Implementation of the DURS will have implications for different sectors, in particular small and medium enterprises. It would be prudent for the PCPD to consider carefully the implementation arrangements such as the classes of data users to be specified and the need for guidelines to facilitate data users to comply with the requirements. Before specifying a class of data users, the PCPD has to consult the stakeholders as well. The PCPD is considering the arrangements to take the matter forward. We will continue to liaise with the PCPD on the arrangements.

Advice Sought and Way Forward

39. Members are invited to give views on the proposals in the consultation report and the related matters set out in this paper. The

[3] The prescribed information includes (a) the name and address of the data user; (b) a description of the kind of personal data in respect of which the data user is a data user; (c) a description of the purpose or purposes for which the personal data are or are to be collected, held, processed or used by the data user; (d) a description of any classes of persons to whom the data user discloses, intends to disclose or may wish to disclose the personal data; and (e) the names or a description of any places outside Hong Kong to which the data user transfers, intends to transfer or may wish to transfer, the personal data.

further public discussion on the proposals arising from the review of the PDPO will last until the end of December 2010. We will examine the views received carefully and then finalise our legislative proposals. We will report to the Panel the views received and our legislative proposals, before introducing an amendment bill into the Legislative Council.

Constitutional and Mainland Affairs Bureau
December 2010

Existing provisions of the PDPO concerning collection and use of personal data and PCPD's guidance note on collection and use of personal data in direct marketing

The PDPO 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].

2. To address various concerns of the community on use of personal data in direct marketing, the PCPD issued in October 2010 a new guidance note in October 2010 on the collection and use of personal data in direct marketing, replacing the previous 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 also draws their attention to recommended practices in personal data privacy protection.

[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.