Legislative Council Panel on Constitutional Affairs

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

Introduction

This paper briefs Members on the result of the further public discussions on review of the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) conducted from October to December 2010 and the legislative proposals drawn up in the light of the views received. The "Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance" ("further public discussions report") is at **Annex A**.

Background

2. The PDPO was enacted in 1995. To ensure that the PDPO still affords adequate protection to personal data privacy and meets present day requirements, we have conducted a comprehensive review of it with the support of the Privacy Commissioner for Personal Data ("PCPD"). We conducted a public consultation from August to November 2009. We then published in October 2010 the "Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance" ("consultation report"), setting out our legislative proposals drawn up in the light of the views received and a few new proposals in response to cases of transfer of customer personal data by some enterprises for direct marketing purposes. Further public discussions on the proposals ended in December 2010. A total of 284 submissions were received. We consulted Members, organised two public forums, met with representatives of the direct marketing, financial services, information technology ("IT"), commercial and social services sectors, attended the seminars and forums organised by interested organisations and briefed the Chairmen and Vice-Chairmen of District Councils, the Human Rights Forum and Children's Rights Forum.

Proposals to be Implemented

3. In the consultation report, we set out over thirty proposals which we intended to take forward. The majority of views received during the further public discussions generally support these proposals. Having considered the

comments received, we have refined some of these proposals. The major revisions are highlighted below.

Collection and Use of Personal Data in Direct Marketing

Proposal in the consultation report

4. Section 34(1)(ii) of the PDPO provides that, if a data subject requests the data user not to use his personal data for direct marketing purposes, the data user shall cease to so use the data. Contravention of this requirement is subject to a fine at Level 3 ($10,000). We proposed in the consultation report to raise the penalty to a fine of $500,000 and imprisonment for three years to enhance the deterrent effect.

5. To address concerns over the use (the meaning of which under the PDPO includes transfer) of the personal data collected for direct marketing purposes, we proposed to stipulate in the PDPO additional specific requirements on data users who intend to so use the data. These include providing the data subject with information on the intended direct marketing activities, 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. The presentation of such information should be understandable and reasonably readable. The data user should also provide an option for the data subject to choose not to agree (i.e. an opt-out mechanism) to the use of his personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees. Non-compliance with any of the abovementioned requirements will be subject to the issue of an enforcement notice by the PCPD. It will be an offence for a data user to use personal data for direct marketing purposes without complying with any of the abovementioned requirements or against the wish of the data subject.

Views received and proposed way forward

6. Most of the views received support the proposal to raise the penalty for contravention of section 34(1)(ii) of the PDPO. We will implement this proposal.

7. Most of the views received also support the proposal to introduce additional specific requirements on data users who intend to use personal data for direct marketing. Some offered suggestions on the wording of the new requirements. Of those who expressed views on whether the opt-out or opt-in mechanism should be adopted, about 60%, including the marketing/direct

marketing, banking and exhibition and convention industries, support the former. They point out that consumers tend not to read the information provided to them and when they are undecided, they tend to take a conservative approach. The opt-in mechanism will kill the direct marketing industry which has been creating employment opportunities. In addition, other jurisdictions generally have chosen to adopt the opt-out mechanism[1]. Those who support the opt-in mechanism, including the Office of the PCPD, consider that it can best protect the consumers' right of self-determination on the use of their personal data by requiring the consumers to provide express consent.

8. We intend to adopt the opt-out mechanism, as proposed in the consultation report, so as to strike a balance between the protection of personal data privacy and allowing room for businesses to operate while providing data subjects with an informed choice as to whether to allow the use of their personal data for direct marketing. This is also in line with the approach adopted under section 34 of the PDPO and that under the Unsolicited Electronic Messages Ordinance (Cap. 593) ("UEMO")[2], which regulates the sending of unsolicited commercial electronic messages.

9. In the light of the comments received and making reference to the guidance note entitled "Guidance on the Collection and Use of Personal Data in Direct Marketing" published by the PCPD in October 2010, we propose to refine the requirements to the effect that a data user intending to use the personal data to be collected for direct marketing should, before or at the time of data collection –

(a) inform the data subject of (i) the classes of goods, facilities or services (e.g. beauty products, financial services, telecommunications services or healthcare services) to be offered or advertised and/or the purposes (e.g. charitable, cultural or recreational) for which donations or contributions may be solicited, whether by the data user himself or the transferee(s); (ii) the classes of persons (e.g. financial services companies or telecommunications services providers) to whom the data may be transferred; and (iii) the kinds of personal data to be

[1] The personal data protection regulations of the United States, Canada, the United Kingdom ("UK"), France and Australia generally adopt the opt-out principle to regulate the use of personal data in direct marketing. In some jurisdictions like the UK and France, the relevant regulations adopt an opt-in mechanism for direct marketing activities conducted through certain channels such as email, fax or automated calls and an opt-out mechanism for person-to-person telemarketing activities. In Germany, prior express consent from the consumer is needed for person-to-person telemarketing activities.

[2] The UEMO regulates the sending of commercial electronic messages including e-mail, facsimile and pre-recorded telephone messages. The Office of the Telecommunications Authority has established three do-not-call registers for fax, short messages and pre-recorded telephone messages respectively under the UEMO.

transferred. The layout and presentation of the information, if in written form, should be easily readable to individuals with normal eyesight and the language easily understandable; and

(b) provide an option, without charge, for the data subject to choose not to agree (i.e. an opt-out mechanism) to the use (including transfer) of his personal data for the direct marketing purposes stated by the data user. The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the various classes of goods/facilities/services to be offered or advertised, purposes for which donations or contributions may be sought, classes of transferees and kinds of personal data to be transferred stated by the data user. The data user will be allowed to adopt the opt-in mechanism, instead of the opt-out mechanism, if he so chooses.

10. If a data user intends to use (including transfer) personal data already collected ("pre-existing data") (whether before or after the entry into force of the new requirements) for direct marketing purposes, he should, before the use (or transfer), comply with the requirements in paragraph 9(a) and (b) above. However, the requirements will not apply to the pre-existing data which the data user has, before the entry into force of the new requirements, used for direct marketing in compliance with the existing requirements under the PDPO, and which he continues to use (but not transfers) for offering or advertising the same class(es) of goods, facilities or services, or solicitation of donations or contributions for the same purpose(s). There is a case to provide for this arrangement as the data subjects are aware of such direct marketing activities of the data user and could have requested the data user to cease to so use their personal data if they so wished. This will also help avoid a huge number of notices providing the required information and option to be sent to data subjects to cover data being used for such activities when the new requirements come into effect.

11. If, after the provision of the information and option required, the data subject provides a response to the data user indicating that he does not opt out, the data user may proceed to use and/or transfer the personal data for the direct marketing activities stated by him. If the data subject does not respond to the data user, the data user may deem that the data subject has not opted out if no opt-out request is received within 30 days after the information and option are given to the data subject.

12. A data subject may opt out any time and if he so requests, the data user has to cease to use his personal data for direct marketing as currently required under section 34(1)(ii) of the PDPO. We further propose that, if a data

subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 9(b) above, the data subject may request the data user to notify the classes of persons to whom his personal data have been transferred for direct marketing to cease to so use the data. Upon receipt of the notification, the transferees have to cease to so use the data. As regards erasure of such data, section 26 of the PDPO already stipulates that a data user shall erase personal data held by him where the data are no longer required for the purpose (including any directly related purpose) for which the data were used[3] and it is an offence for a data user to contravene this requirement.

13. The PCPD will be requested to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements. As proposed in the consultation report, non-compliance with any of the requirements in paragraph 9(a) and (b) will be subject to the issue of an enforcement notice by the PCPD. Using the personal data collected for direct marketing without complying with any of the specific requirements or against the wish of the data subject will be an offence and the penalty a fine of $500,000 and imprisonment for three years. A transferee referred to in paragraph 12 who, upon receipt of the notification, does not cease to use the personal data for direct marketing will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years.
In order not to criminalise inadvertent acts, we propose that it shall be a defence for a data user to prove that he has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

<u>Exemption for Essential Social and Healthcare Services from Provisions relating to Direct Marketing</u>

Proposal in the consultation report

14. Pursuant to section 34 of the PDPO, if an individual contacted by a social worker requests the social worker to cease to use his personal data for offering social services or facilities (which falls under the definition of direct marketing in that section), the social worker has to cease to so use the data. The consultation report proposed to exclude from the definition of "direct marketing" the offering of essential social services and facilities by social workers to individuals in need of such services and facilities, so that social

[3] Under section 26 of the PDPO, a data user shall erase personal data held by him where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless (a) any such erasure is prohibited under any law; or (b) it is in the public interest for the data not to be erased. A data user who, without reasonable excuse, contravenes section 26 commits an offence and is liable on conviction to a fine at level 3 ($10,000).

workers may, in the proper interest of the client and of the society at large, continue to "knock at the door" of the client, even against his wish.

Views received and proposed way forward

15. The majority of the submissions that commented on this proposal agree to the rationale of this proposal. There are suggestions for this exemption to cover social services that are run, subvented or subsidised by the Social Welfare Department ("SWD") or provided by non-governmental organisations. There are also suggestions that the Hospital Authority ("HA") and the Department of Health ("DH") should be exempted since they provide hospital and related healthcare services to the public, the importance of which is similar to that of social services. It will be onerous for HA and DH, which together have over eight million patients, to comply with the requirements in paragraphs 9 to 12 above. Modern delivery of medical services puts great emphasis on a multidisciplinary approach and cross-sectoral collaboration and patients need to be informed of the availability of various services. A respondent suggests that medical services provided by private medical practitioners should be exempted as well. On the other hand, some respondents consider that the proposed exemption would remove the right of citizens to refuse services provided by social services organisations. Some comment that all organisations, be they commercial enterprises, charitable organisations or government bodies, should be subject to the same set of regulations and penalties.

16. Having carefully considered the views received, we propose that –

(a) social services run, subvented or subsidised by SWD;

(b) healthcare services provided by HA or DH; or

(c) social or healthcare services not covered by (a) or (b) above which, if not provided, would be likely to cause serious harm to the physical or mental health of the data subject or any other individual

should be exempted from the provisions relating to direct marketing activities (i.e. section 34 of the PDPO and those in paragraphs 9 to 12 above).

Unauthorised Sale of Personal Data by Data User

Proposal in the consultation report

17. We proposed in the consultation report to stipulate in the PDPO that a data user who intends to sell personal data to another person for a monetary or in kind gain should, before doing so, provide the data subject with information in writing, which should be understandable and reasonably readable, on the kinds of personal data to be sold and to whom the personal data would be sold; as well as an opportunity for the data subject to indicate whether he agrees to (i.e. an opt-in mechanism) or disagrees with (i.e. an opt-out mechanism) the sale. Non-compliance with any of the abovementioned requirements will be subject to the issue of an enforcement notice by the PCPD. It will be an offence for a data user to sell personal data for monetary or in kind gain without complying with any of the abovementioned requirements or against the wish of the data subject.

Views received and proposed way forward

18. Of the submissions that expressed views on this proposal, most are in support. However, some business corporations and associations are against it. Respondents from the direct marketing industry, in particular, object to the application of the term "sale" to sharing and temporary transfer of data in exchange for fees or commissions, which is generally referred to as "list rental" and "data licensing". Some respondents from the direct marketing, financial services and IT sectors consider that these are legitimate commercial activities and should not be criminalised. Views on whether the opt-in or opt-out mechanism should be adopted are similar to those in paragraph 6 above. Some offered suggestions on the wording of the new requirements.

19. Having regard to the views received on the term "sell" and as a result the types of activities covered by this proposal, we propose to define the term "sell" as –

> "to make available, whether for a defined or indefinite period, to another person personal data for gain, including but not limited to monetary gain,
>
> (a) whether or not parting with possession of the personal data; and
> (b) whether or not the gain is contingent on other conditions".

In other words, the types of activities in paragraph 18 referred to as "list rental" and "data licensing" in exchange for fees or commissions will be covered.

These are the activities that have aroused widespread community concerns and calls for criminalisation.

20. We also propose to adopt the opt-out mechanism to help avoid confusion with the requirements relating to collection and use of personal data for direct marketing and to facilitate compliance. In the light of the comments received, we propose to fine-tune the requirements to the effect that if a data user is to sell personal data to be collected, the data user should, before or at the time of data collection –

(a) inform the data subject in writing of (i) the kinds of personal data to be sold and (ii) to which classes of persons the personal data may be sold. The layout and presentation of the information should be easily readable to individuals with normal eyesight and the language easily understandable; and

(b) provide an option, without charge, for the data subject to choose not to agree to the sale (i.e. an opt-out mechanism). The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the kinds of personal data to be sold and the classes of persons to whom the data may be sold stated by the data user. The data user will be allowed to adopt the opt-in mechanism, instead of the opt-out mechanism, if he so chooses.

21. If a data user intends to sell personal data already collected (whether before or after the entry into force of the new requirements), he should, before the sale, comply with the requirements in paragraph 20(a) and (b) above. The deeming arrangement in cases where no opt-out request is received within 30 days in paragraph 11 will similarly apply to this proposal.

22. We propose to stipulate that a data subject may opt out any time and the data user has to cease to sell the personal data upon receipt of the opt-out request. We further propose that, if a data subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 20(b), the data subject may request the data user to notify the classes of persons to whom his personal data have been sold to cease to use the data. Upon receipt of the notification, the buyers have to cease to use the data.

23. The PCPD will be requested to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements. As proposed in the consultation report, non-compliance with any of the specific requirements in paragraph 20(a) and (b)

will be subject to the issue of an enforcement notice by the PCPD. In view of community concern about unauthorised sale of personal data and to provide sufficient deterrence, we propose that the penalty for a data user who sells personal data without complying with any of the requirements in paragraph 20(a) and (b) or against the wish of the data subject should be a fine of $1,000,000 and imprisonment for five years. A buyer referred to in paragraph 22 who, upon receipt of the notification, does not cease to use the personal data will commit an offence and be liable on conviction to a fine of $1,000,000 and imprisonment for five years. A defence same as the one in paragraph 13 above will be provided.

<u>Disclosure with a view to Gain or Cause Loss of Personal Data Obtained without the Data User's Consent</u>

Proposal in the consultation report

24. The consultation report proposed that it should be an offence for a person (e.g. an employee of a data user) to disclose for profits or malicious purposes personal data which he obtained from a data user without the latter's consent. The phrase "for malicious purposes" may be defined as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another". It was proposed that the penalty should be set at the same level as that for the new offence of unauthorised sale of personal data by data users.

Views received and proposed way forward

25. The majority of the submissions that commented on this proposal are supportive. Some respondents consider the term "for malicious purposes", particularly the phrase "injury to feelings" in the proposed definition, a wide and subjective concept. Some respondents suggest providing for defences. Having regard to the comments received, we intend to refine the proposal to the effect that it will be an offence for a person to disclose personal data which he obtained from a data user without the latter's consent –

(a) with a view to gain in money or other property for himself or another; or

(b) with an intent to cause loss in money or other property or psychological harm to the data subject.

The term "injury to feelings" is replaced with "psychological harm" as the scope of "psychological harm" is more concrete. In view of the seriousness of the offence, the penalty will be set at the same level as that for the new offence of unauthorised sale of personal data by data users, i.e. liable on conviction to a fine of $1,000,000 and imprisonment for five years. Defences, as set out in paragraph 3.73 of the further public discussions report, will be provided.

Legal Assistance to Data Subjects

Proposal in the consultation report

26. The consultation report proposed empowering the PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings against the data user to seek compensation under section 66 of the PDPO. Such assistance will include giving legal advice on the sufficiency of evidence and arranging for a lawyer to represent the applicant in legal proceedings. To ensure proper use of public funds, applications for legal assistance would only be considered if 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 or any other matter. This is similar to the existing arrangements for the Equal Opportunities Commission ("EOC") to provide legal assistance to complainants under the anti-discrimination ordinances.

Views received and proposed way forward

27. As the majority of those who commented on this proposal are supportive, we will implement it. We further propose to, following the EOC model, stipulate that proceedings under section 66 shall be brought in the District Court and that each party (i.e. the claimant and the respondent) has to each bear his own costs unless the District Court otherwise orders on the ground that the proceedings were brought maliciously or frivolously or there are special circumstances which warrant an award of costs. This is to remove fear of the victim having to bear possibly huge legal fees in the event he loses the case.

Time Limit for Responding to PCPD's Investigation / Inspection Report

Proposal in the consultation report

28. Under section 46(4) of the PDPO, before the PCPD publishes an inspection or investigation report, he has to provide a copy of the report to the

relevant data user for him to advise within 28 days whether he objects to the disclosure in the report of any personal data that are exempted from the provisions of Data Protection Principle ("DPP") 6. The PCPD has proposed to shorten the period to 14 days. In the consultation report, we stated that we did not intend to pursue this as data users may need time to seek legal advice before they can provide a formal response to the PCPD.

Views received and proposed way forward

29. The PCPD, however, urges the Administration to reconsider it, since in cases involving public interest, a swift response should be given to address the public concern. Moreover, if no personal data are mentioned in the report, it would be a waste of time to wait for 28 days. Having considered the PCPD's latest submission, we agree that the PDPO should be amended so that the requirement in section 46(4) should only apply to investigation and inspection reports that contain personal data.

Proposals not to be implemented

30. The consultation report also set out some proposals that we did not intend to pursue. The majority of views received agree to our position. We, therefore, maintain our stance of not taking forward these proposals. The major ones are highlighted at **Annex B**.

Way Forward

31. We will prepare proposed amendments to the PDPO on the basis of the proposals in the further public discussions report. We aim at introducing an amendment bill into the Legislative Council in July 2011.

Constitutional and Mainland Affairs Bureau
April 2011

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

April 2011

Contents

Summary of Proposals

Proposals to be Implemented

Collection and Use of Personal Data in Direct Marketing

1. To raise the penalty for contravention of section 34(1)(ii) of the Personal Data (Privacy) Ordinance ("PDPO") (which stipulates that a data user has to cease using the personal data of a data subject for direct marketing purposes if the data subject so requests) from a fine at Level 3 ($10,000) to a fine of $500,000 and imprisonment for three years.

2. To introduce the following new requirements : if a data user intends to use (including transfer) for direct marketing purposes the personal data to be collected, he should, before or at the time of data collection –

   (a) inform the data subject of (i) the classes of goods, facilities or services (e.g. beauty products, financial services, telecommunications services or healthcare services) to be offered or advertised and/or the purposes (e.g. charitable, cultural or recreational) for which donations or contributions may be solicited, whether by the data user himself or the transferee(s); (ii) the classes of persons (e.g. financial services companies or telecommunications services providers) to whom the data may be transferred; and (iii) the kinds of personal data to be transferred. The layout and presentation of the information, if in written form, should be easily readable to individuals with normal eyesight and the language easily understandable; and

   (b) provide an option, without charge, for the data subject to choose not to agree (i.e. an opt-out mechanism) to the use (including transfer) of his personal data for the direct marketing purposes stated by the data user. The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the various classes of goods/facilities/services to be offered or advertised, purposes for which donations or contributions may be sought, classes of transferees and kinds of personal data to be

transferred stated by the data user. The data user will be allowed to adopt the opt-in mechanism instead of the opt-out mechanism, if he so chooses.

3. To stipulate that, if a data user intends to use (including transfer) personal data already collected ("pre-existing data") (whether before or after the entry into force of the new requirements) for direct marketing purposes, and if the requirements in paragraph 2 (a) and (b) were not complied with before or at the time of data collection, the data user should, before the use (or transfer), comply with the requirements therein. A data user who has, before the entry into force of the new requirements, used pre-existing data for offering or advertising one or more classes of goods, facilities or services and/or solicitation of donations or contributions for one or more purposes in compliance with the existing requirements under the PDPO, will be allowed to continue to use (but not transfer) the personal data for offering or advertising the same class(es) of goods, facilities or services, or solicitation of donations or contributions for the same purpose(s) without complying with the requirements in paragraph 2 (a) and (b).

4. To stipulate that, if, after the information and option required under paragraph 2 (a) and (b) are provided to the data subject, the data subject provides a response to the data user indicating that he does not opt out, the data user may proceed to use and/or transfer the personal data for the direct marketing activities stated by him. If the data subject does not respond to the data user, the data user may deem that the data subject has not opted out if no opt-out request is received within 30 days after the information and option are given to the data subject.

5. To stipulate that, if a data subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 2(b), the data subject may request the data user to notify the classes of persons to whom his personal data have been transferred for direct marketing to cease to so use the data. Upon receipt of the notification, the transferees have to cease to so use the data. As regards erasure of such data, section 26 of the PDPO already stipulates that a data user shall erase personal data no longer required and it is an offence to contravene this requirement.

6. To stipulate that non-compliance with any of the requirements in paragraph 2 (a) and (b) will be subject to the issue of an enforcement notice by the Privacy Commissioner for Personal Data ("PCPD"). A data user will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years, if he uses the personal data collected for direct marketing without complying with any of the requirements, or against the wish of the data subject. A transferee referred to in paragraph 5 who, upon receipt of the notification, does not cease to use the personal data for direct marketing will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years. It shall be a defence for a data user to prove that he has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

7. To request the PCPD to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements.

Exemption for Essential Social and Healthcare Services from Provisions relating to Direct Marketing

8. To exempt from the provisions relating to direct marketing activities (i.e. section 34 of the PDPO and those in paragraphs 2 to 6 above) –

   (a) social services run, subvented or subsidised by the Social Welfare Department;

   (b) healthcare services provided by the Hospital Authority or Department of Health; or

   (c) social or healthcare services not covered by (a) or (b) above which, if not provided, would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

Unauthorised Sale of Personal Data by Data User

9. To define the term "sell" as –

"to make available, whether for a defined or indefinite period, to another person personal data for gain, including but not limited to monetary gain,

(a) whether or not parting with possession of the personal data; and

(b) whether or not the gain is contingent on other conditions."

10. To introduce the following new requirements : if a data user is to sell personal data to be collected, he should, before or at the time of data collection –

(a) inform the data subject in writing of (i) the kinds of personal data to be sold and (ii) to which classes of persons the personal data may be sold. The layout and presentation of the information should be easily readable to individuals with normal eyesight and the language easily understandable; and

(b) provide an option, without charge, for the data subject to choose not to agree to the sale (i.e. an opt-out mechanism). The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the kinds of personal data to be sold and the classes of persons to whom the data may be sold stated by the data user. The data user will be allowed to adopt the opt-in mechanism instead of the opt-out mechanism, if he so chooses.

11. To stipulate that, if a data user intends to sell personal data already collected (whether before or after the entry into force of the new requirements) and if the requirements in paragraph 10 (a) and (b) were not complied with before or at the time of data collection, the data user should, before the sale, comply with the requirements therein.

12. To stipulate that, if, after the information and option required under paragraph 10 (a) and (b) are provided to the data subject, the data subject provides a response to the data user indicating that he does not opt out, the data user may proceed to sell the kind(s) of personal data to the class(es) of persons as stated by him. If the

data subject does not respond to the data user, the data user may deem that the data subject has not opted out if no opt-out request is received within 30 days after the information and option are given to the data subject.

13. To stipulate explicitly that a data subject may opt out any time, even if he has not opted out before or is deemed to have not opted out, and the data user has to cease to sell the personal data upon receipt of the opt-out request. If a data subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 10(b), the data subject may request the data user to notify the classes of persons to whom his personal data have been sold to cease to use the data. Upon receipt of the notification, the buyers have to cease to use the data.

14. To stipulate that non-compliance with any of the requirements in paragraph 10 (a) and (b) will be subject to the issue of an enforcement notice by the PCPD. A data user will commit an offence and be liable on conviction to a fine of $1,000,000 and imprisonment for five years if he sells the personal data to another person without complying with any of the new requirements or against the wish of the data subject. A buyer referred to in paragraph 13 who, upon receipt of the notification, does not cease to use the personal data will commit an offence and be liable on conviction to a fine of $1,000,000 and imprisonment for five years. It shall be a defence for a data user to prove that he has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

15. To request the PCPD to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements.

Disclosure with a view to Gain or Cause Loss of Personal Data Obtained without the Data User's Consent

16. To make it an offence for a person to disclose personal data, which he obtained from a data user without the latter's consent –

(a) with a view to gain in money or other property for himself or another; or

(b) with an intent to cause loss in money or other property or psychological harm to the data subject.

The penalty will be a fine of $1,000,000 and imprisonment for five years. Defences will be provided.

Regulation of Data Processors and Sub-contracting Activities

17. To amend the PDPO to require data users to use contractual or other means to ensure that their data processors and sub-contractors, whether within Hong Kong or offshore, comply with the requirements under the PDPO. Contravention of the new requirement will render the data user liable to the issue of an enforcement notice by the PCPD.

Personal Data Security Breach Notification

18. To start with a voluntary personal data security breach notification system, under which organisations would notify the PCPD and affected individuals when a breach of data security leads to the leakage of personal data, so that we can adjust the detailed arrangements, if necessary, having regard to actual operational experience and assessment on the impact of leakage notification, with a view to making the system reasonable and practicable.

19. To request the Office of the PCPD to undertake promotional and educational initiatives to raise awareness of the guidance note on this subject issued by it, promote adoption of a privacy breach notification system by data users voluntarily and assist data users to make appropriate notifications.

Legal Assistance to Data Subjects

20. To empower the PCPD 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.

Time Limit for Responding to PCPD's Investigation/Inspection Report

21. To amend the PDPO to the effect that the requirement in section 46(4) should only apply to investigation and inspection reports that contain personal data.

Others

22. To pursue the other proposals set out in **Appendix D**.

Proposals NOT to be Implemented

Sensitive Personal Data

23. Not to pursue the proposal to subject sensitive personal data to more stringent regulation. Instead, we will take the following measures to enhance the protection for sensitive personal data –

    (a) to request the Office of the PCPD to step up promotion and education and, where necessary, issue codes of practice or guidelines to suggest best practices on the handling and use of sensitive personal data, such as biometric data and health record; and

    (b) to request the Office of the PCPD to continue to discuss with the information technology sector possible measures to enhance the protection of biometric data.

Granting Criminal Investigation and Prosecution Powers to the PCPD

24. Not to pursue the proposal to grant criminal investigation and prosecution powers to the PCPD.

Empowering the PCPD to Award Compensation to Aggrieved Data Subjects

25. Not to pursue the proposal to empower the PCPD to award compensation to aggrieved data subjects.

Empowering the PCPD to Impose Monetary Penalty for Serious Contravention of Data Protection Principles

26. Not to pursue the proposal to empower the PCPD to impose monetary penalty for serious contravention of data protection principles.

Others

27. Not to pursue the other proposals set out in Chapter Four.

Chapter One : Introduction

1.1 The Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) (an overview of the PDPO is at **Appendix A**), 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"), the Constitutional and Mainland Affairs Bureau ("CMAB") had conducted a review on the PDPO and then published a consultation document in August 2009 for a three-month public consultation on the proposals arising from the review.

1.2 Subsequently, we published the Report on Public Consultation on Review of the PDPO ("consultation report") on 18 October 2010, setting out the views on the proposals submitted by the public and the proposals drawn up in the light of the views received and related developments, including cases of transfer or sale of customer personal data by some enterprises to others for direct marketing purposes, for further public discussions until 31 December 2010.

1.3 This report sets out the views received during the further public discussions and the Government's proposed way forward. Chapter Two of this report gives a brief account of the further public discussions. Chapter Three sets out the proposals to be implemented and Chapter Four sets out the proposals not to be implemented, having regard to the public views received.

Chapter Two : The Further Public Discussions

2.1 During the further public discussions, we organised two public forums on 4 and 29 November 2010 to gauge the views of the community on the proposals. Over 180 people attended the two forums. Summaries of views expressed by the participants are at **Appendix B**. We consulted the Legislative Council Panel on Constitutional Affairs ("LegCo CA Panel") on 18 October, 15 November and 20 December 2010. At its meeting on 20 November, the LegCo CA Panel received views from deputations on the proposals. We have also met with representatives of the sectors and organisations interested in the proposals. A list of the forums and seminars we attended is at **Appendix C**.

2.2 The further public discussions ended on 31 December 2010. A total of 284 submissions were received, including a few that were received after the end of the further public discussions. Save those kept confidential at the request of the submitting parties, the submissions are available at the CMAB's website (http://www.cmab.gov.hk).

Chapter Three : Proposals to be Implemented

Collection and Use of Personal Data in Direct Marketing (Proposal (1) in the Consultation Report)

Proposal in the Consultation Report

3.1 Section 34(1)(ii) of the PDPO provides that, if a data subject requests the data user not to use his personal data for direct marketing purposes, the data user shall cease to so use the data (i.e. an opt-out mechanism). 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). To more effectively curb the misuse of personal data in direct marketing, we proposed in the consultation report to raise the penalty to a fine of $500,000 and imprisonment for three years.

3.2 The recent cases of transfer of massive customer personal data by some enterprises to others for direct marketing purposes without explicitly and specifically informing the customers of the purpose of the transfer and the identity of the transferees and seeking the customer's consent have aroused widespread community concerns. To address these concerns, we proposed to stipulate in the PDPO additional specific requirements on data users who intend to use (the meaning of which under the PDPO includes "transfer") the personal data to be collected for direct marketing purposes[1]. It was also proposed that the data user should provide an option for the data subject to choose not to agree (i.e. an opt-out mechanism) to the use (including transfer) of his personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees.

3.3 Under the proposal, non-compliance with any of the additional specific requirements should be subject to the issue of an enforcement notice by the PCPD. Failure to comply with the enforcement notice is an offence as currently provided for under

[1] These requirements include providing the data subject with information, which should be understandable and reasonably readable, on the intended direct marketing activities, 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.

the PDPO[2].

3.4 The consultation report also proposed that a data user would commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years, if he used (including transferred) the personal data collected for direct marketing purposes without complying with any of the additional specific requirements or against the wish of the data subject.

Views Received

3.5 Around 30% of the submissions received expressed views on this proposal. The majority support the principle of tightening the regulation of the collection and use of personal data in direct marketing. Only a few consider that the current regulatory regime has already provided sufficient protection and oppose the introduction of new requirements and the proposed criminal offence.

Raising the penalty for contravention of section 34(1)(ii) of the PDPO

3.6 More than 70% of the submissions that commented on the proposed increase of penalty for contravening section 34(1)(ii) of the PDPO supported the proposal as this could increase the deterrent effect. However, a minority of the submissions, mainly from the business sector, consider imprisonment disproportionate as the actual material damage to the data subject may not be substantial.

Additional specific requirements on the collection and use of personal data for direct marketing purposes

3.7 The majority of the submissions that commented on the proposed introduction of additional specific requirements on the collection and use of personal data for direct marketing purposes support the proposal.

3.8 There are, however, views that some of the terms in the proposed

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

additional specific requirements, such as "intended direct marketing activities" and "reasonably readable", are ambiguous and subject to wide interpretation. They urge the PCPD to, in consultation with stakeholders, prepare guidelines or codes of practice to facilitate compliance.

3.9 Of those who expressed views on the proposal to adopt the opt-out instead of the opt-in mechanism, about 60% are supportive. They generally consider that this can strike a balance between the protection of personal data privacy and the business operation of the direct marketing industry by offering data subjects an informed option.

3.10 The marketing industry points out that consumers tend not to read the information provided to them for a variety of reasons, most of which relate to human nature. Moreover, when consumers are undecided on whether to indicate agreement or not, they tend to take a conservative approach. For these reasons, if the opt-in mechanism is adopted, the opt-in percentage will be extremely low. This will kill the direct marketing industry which has been creating employment opportunities and contributing much to the Hong Kong economy. The direct marketing industry stresses that other jurisdictions generally have chosen to adopt the opt-out mechanism.

3.11 The direct marketing industry also points out that the current discussion on direct marketing focuses only on telemarketing but ignores other media that can be used to deliver sales messages directly to the consumer, including direct mail, short messages and email. If the opt-in mechanism is adopted, it would have a ripple effect throughout the entire industry and its supply chain including printers, production houses and delivery companies and thousands of jobs will be at stake. The direct marketing industry considers that both the opt-out and opt-in mechanisms provide the same protection and powers to consumers, and differ only in the manner of indicating choice. They urge that efforts should be stepped up to educate the general consuming public to understand the powers and rights that are available to them.

3.12 The banking industry also prefers the opt-out mechanism. The industry considers the opt-in mechanism unduly burdensome on

the operations of data users. Data subjects must actively engage in an opt-in model. Some data subjects may prefer a hassle-free opt-out approach. Other data subjects may fail to respond for other reasons including that they may not understand the opt-in model and confirmation process. This will result in a lose-lose situation where data subjects lose the benefit and convenience of receiving marketing information that may interest them and data users lose the opportunity to market their products and services to potential customers. Moreover, requiring a data subject to opt-in from the start without trying out a data user's products or services first may not facilitate an informed choice.

3.13 The exhibition and convention industry supports the opt-out mechanism. A respondent from the industry stresses that while it advocates better protection and usage of personal data, any new regulation must also strike a balance to leave the industry a reasonable and effective way to continue its business and services.

3.14 Of those who expressed views on the proposal to adopt the opt-out instead of the opt-in mechanism, less than 30% support the opt-in mechanism, while some others propose a hybrid approach that adopts different mechanisms in different situations. Respondents who support the opt-in mechanism, including the Office of the PCPD, a political party, individual LegCo members and some civil society organisations, consider that the opt-in mechanism, which requires the express consent of consumers, can best protect the consumers' right of self-determination on the use of their personal data.

3.15 On the detailed arrangements for the opt-out mechanism, there are views from the business sector, including the banking industry, that allowing data subjects to opt out from using their personal data for any of the intended direct marketing activities or transfer of their personal data to any of the intended classes of transferees will require data users to provide custom-made service to data subjects individually. This will be extremely difficult if not totally impracticable as different customers might have different combinations of options. This is particularly the case when the data user holds personal data of a very large number of data subjects. It should be a simple all-or-nothing opt-out right.

3.16 Only a few respondents commented on the proposed penalty level. Some respondents from the business sector consider that while unsolicited marketing can be annoying, the actual damage caused may not be that substantial. Criminal sanction for violating the proposed additional requirements is too harsh. A respondent considers that the fine should be proportional to the profits generated by the relevant act. Some suggest that defences should be provided to avoid criminalising inadvertent or careless acts, and it should also be a defence if a data user has already exercised all due diligence to avoid the commission of the offence.

3.17 Some respondents enquire if personal data collected before the entry into force of the new requirements will be grandfathered and if not, whether a grace period will be provided for data users to comply with the new requirements for such data. Another respondent remarks that there may be a time gap between the making of the opt-out request by the data subject and the receipt of the request by the data user, during which time the data user may have made direct marketing approach to the data subject.

Do-not-call ("DNC") register for person-to-person telemarketing calls ("P2P calls")

3.18 Around 10% of the submissions received expressed views on whether a DNC register for P2P calls should be set up. About half are against, with a slightly smaller number in support. Respondents who oppose, including those from the direct marketing industry, consider that consumers already have the right to opt out from telemarketing calls on a company-by-company basis and the economic value of direct marketing activities should not be overlooked.

3.19 Those who are supportive consider that unsolicited P2P calls bring the same level of nuisance as pre-recorded messages. Some of them, including the Office of the PCPD, consider that the DNC registers administered by the Office of the Telecommunications Authority ("OFTA") under the Unsolicited Electronic Messages

Ordinance[3] ("UEMO") (Cap. 593) should be extended to regulate such calls.

3.20 To solicit views on a number of proposals, including the DNC register for P2P calls, the Office of the PCPD has conducted an online survey targeted at the general public and sent a questionnaire to 95 parties and individuals who had made submissions to the Administration during the 2009 public consultation and/or had given views to the LegCo CA Panel or approached the PCPD during the further public discussions. The two surveys revealed different opinions[4].

Way Forward

Raising the penalty for contravention of section 34(1)(ii) of the PDPO

3.21 Most of the views received support the proposal to raise the penalty for contravention of section 34(1)(ii) of the PDPO from a fine at Level 3 ($10,000) to a fine of $500,000 and imprisonment for three years. We will introduce amendments to the PDPO to implement this proposal.

Additional specific requirements on the collection and use of personal data for direct marketing purposes

3.22 Most of the views received support the introduction of additional specific requirements on the collection and use of personal data for direct marketing purposes. We will take forward this proposal. In the light of the comments on some of the terms and specifics in the additional requirements, we have refined the requirements, as set out in paragraph 3.24 below.

3.23 As regards our proposal to adopt the opt-out mechanism, having

[3] The UEMO regulates the sending of commercial electronic messages including e-mail, facsimile and pre-recorded telephone message generated electronically by machines. The OFTA has established three do-not-call registers for fax, short messages and pre-recorded telephone messages respectively under the UEMO.

[4] For the online survey, of the 1 210 respondents, 464 (38%) support the setting up of a do-not-call register for person-to-person telemarketing activities, 711 (59%) object while 35 (3%) have no comment. According to the Office of the PCPD, 292 of the objecting responses were submitted by a call centre. For the questionnaire survey, of the 43 respondents, 18 (42%) support the proposal, 11 (26%) object and 14 (32%) have other views or no comment.

considered the views received and making reference to overseas practices[5], we maintain the proposal for the opt-out mechanism so as to strike a balance between the protection of personal data privacy and allowing room for businesses to operate while providing data subjects with an informed choice as to whether to allow the use of their personal data for direct marketing. This is also in line with the approach adopted under section 34 of the PDPO and that under the UEMO, which regulates the sending of commercial electronic messages.

3.24 Our proposal is as follows : if a data user intends to use (including transfer) for direct marketing[6] purposes the personal data to be collected, he should, before or at the time of data collection –

(a) inform the data subject of (i) the classes of goods, facilities or services (e.g. beauty products, financial services, telecommunications services or healthcare services) to be offered or advertised and/or the purposes (e.g. charitable, cultural or recreational) for which donations or contributions may be solicited, whether by the data user himself or the transferee(s); (ii) the classes of persons (e.g. financial services companies or telecommunications services providers) to whom the data may be transferred; and (iii) the kinds of personal data to be transferred. The layout and presentation of the information, if in written form, should be easily readable to individuals with normal eyesight and the language easily understandable; and

---

[5] The personal data protection regulations of the United States, Canada, the United Kingdom ("UK"), France and Australia generally adopt the opt-out principle to regulate the use of personal data in direct marketing. In some jurisdictions like the UK and France, the relevant regulations adopt an opt-in mechanism for direct marketing activities conducted through certain channels such as email, fax or automated calls and an opt-out mechanism for person-to-person telemarketing activities. In Germany, prior express consent from the consumer is needed for person-to-person telemarketing activities.

[6] Under section 34 of the PDPO, direct marketing means –
(a) the offering of goods, facilities or services;
(b) the advertising of the availability of goods, facilities or services; or
(c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,
by means of –
(i) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or
(ii) telephone calls made to specific persons.

(b) provide an option, without charge, for the data subject to choose not to agree (i.e. an opt-out mechanism) to the use (including transfer) of his personal data for the direct marketing purposes stated by the data user. The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the various classes of goods/facilities/services to be offered or advertised, purposes for which donations or contributions may be sought, classes of transferees and kinds of personal data to be transferred stated by the data user. The data user will be allowed to adopt the opt-in mechanism instead of the opt-out mechanism, if he so chooses.

3.25 If a data user intends to use (including transfer) personal data already collected ("pre-existing data") (whether before or after the entry into force of the new requirements) for direct marketing purposes, and if the requirements in paragraph 3.24 (a) and (b) were not complied with before or at the time of data collection, the data user should, before the use (or transfer), comply with the requirements therein, except as set out in paragraph 3.26 below.

3.26 We propose to allow a data user, who has, before the entry into force of the new requirements, used pre-existing data for offering or advertising one or more classes of goods, facilities or services and/or solicitation of donations or contributions for one or more purposes in compliance with the existing requirements under the PDPO, to continue to use (but not transfer) the personal data for offering or advertising the same class(es) of goods, facilities or services, or solicitation of donations or contributions for the same purpose(s) without complying with the requirements in paragraph 3.24 (a) and (b). We consider that there is a case to provide for this arrangement as the data subjects are aware of such direct marketing activities of the data user and could have requested the data user to cease to so use their personal data if they so wished. This will also help avoid a huge number of notices providing the required information and option to be sent to data subjects to cover data being used for such activities when the new requirements come into effect.

3.27 If, after the information and option required under paragraph 3.24 (a) and (b) are provided to the data subject, the data subject

provides a response to the data user indicating that he does not opt out, the data user may proceed to use and/or transfer the personal data for the direct marketing activities stated by him. If the data subject does not respond to the data user, the data user may deem that the data subject has not opted out if no opt-out request is received within 30 days after the information and option are given to the data subject.

3.28 Section 34 of the PDPO already provides that a data user has to cease using the personal data of a data subject for direct marketing purposes if the data subject so requests. This will remain the case after the entry into force of the new requirements above. That is, a data subject may opt out any time, even if he has not opted out before or is deemed to have not opted out, and the data user has to cease using the personal data for direct marketing purposes upon receipt of the opt-out request. We further propose that, if a data subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 3.24(b), the data subject may request the data user to notify the classes of persons to whom his personal data have been transferred for direct marketing to cease to so use the data. Upon receipt of the notification, the transferees have to cease to so use the data. As regards erasure of such data, section 26 of the PDPO already stipulates that a data user shall erase personal data held by him where the data are no longer required for the purpose (including any directly related purpose) for which the data were used[7] and it is an offence for a data user to contravene this requirement.

3.29 Non-compliance with any of the requirements in paragraph 3.24 (a) and (b) when the data user provides the information and option to the data subject will be subject to the issue of an enforcement notice, through which the PCPD can direct the data user to take remedial steps. Failure to comply with the enforcement notice will be an offence, as currently provided for under the PDPO.

---

[7] Under section 26 of the PDPO, a data user shall erase personal data held by him where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless (a) any such erasure is prohibited under any law; or (b) it is in the public interest for the data not to be erased. A data user who, without reasonable excuse, contravenes section 26 commits an offence and is liable on conviction to a fine at level 3 ($10,000).

3.30 A data user will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years, if he –

(a) does not comply with any of the requirements in paragraph 3.24 (a) and (b) and subsequently uses (including transfers) the personal data collected for offering or advertising goods, facilities or services or soliciting donations or contributions; or

(b) uses (including transfers) a kind of personal data collected for offering or advertising a class of goods, facilities or services, or for soliciting donations or contributions for a purpose, or transfers the data to a class of transferees, from which the data subject has opted out; or

(c) (i) uses (including transfers) the personal data collected for offering or advertising a class of goods, facilities or services; or

(ii) uses (including transfers) the personal data collected for soliciting donations or contributions for a purpose; or

(iii) transfers the data for offering or advertising goods, facilities or services to a class of persons; or

(iv) transfers, for offering or advertising goods, facilities or services, a kind of personal data

not covered in the information given to the data subject pursuant to the requirement in paragraph 3.24(a) above; or

(d) uses (including transfers) the personal data collected for offering or advertising goods, facilities or services, or soliciting donations or contributions during the 30-day period mentioned in paragraph 3.27 before receiving the data subject's response, whether or not he subsequently receives a response from the data subject indicating that the latter does not opt out; or

(e) fails to comply with a data subject's request to notify the transferee(s) to cease to use the data subject's personal data

for direct marketing as required under paragraph 3.28.

A transferee referred to in paragraph 3.28 who, upon receipt of the notification, does not cease to use the personal data for direct marketing will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years.

3.31 As regards the suggestion of some respondents to provide defences, considering that data users engaged in direct marketing activities may need to handle huge amount of personal data and data subjects may make or withdraw opt-out requests from time to time, we agree that a defence should be provided so as not to criminalise inadvertent acts. We propose that it shall be a defence for a data user to prove that he has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence. In proposing this defence, we have made reference to the UEMO, which provides for a similar defence.

3.32 The PCPD will be requested to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements.

DNC register for P2P calls

3.33 According to the two surveys (an industry survey and a public opinion survey) conducted by OFTA in 2008 and 2009, around half of the P2P calls did not involve the recipients' personal data. If measures are to be introduced to regulate these calls, they should cover all such calls, including those that do not involve the recipients' personal data, so as to make the regulation more comprehensive and effective, and to avoid confusion and dispute over whether the use of personal data is involved. This goes beyond the ambit of the PDPO.

3.34 Furthermore, according to the industry survey, 31% of the respondent companies reported success rates of over 10% in selling goods/services through P2P calls. 13% of the respondents of the public opinion survey said that they had gained benefits from P2P calls, for example, lower prices or discounts. Establishing a DNC for P2P calls appears disproportionate and not

directly relevant to the personal data privacy issue at hand.

3.35 To enhance the protection for call recipients while still allowing legitimate telemarketing, an industry self-regulation scheme was rolled out in 2010. Industry associations of the finance, insurance, telecommunications service and call centre sectors accounting for most of such calls are supportive of the scheme.

Exemption for Essential Social and Healthcare Services from Provisions relating to Direct Marketing
(Proposal (4) in the Consultation Report)

Proposal in the Consultation Report

3.36 Pursuant to section 34 of the PDPO, if an individual contacted by a social worker requests the social worker to cease to use his personal data for offering social services or facilities (which falls under the definition of direct marketing in that section), the social worker has to cease to so use the data. The consultation report proposed to exclude from the definition of "direct marketing" the offering of essential social services and facilities by social workers to individuals in need of such services and facilities, so that social workers may, in the proper interest of the client and of the society at large, continue to "knock at the door" of the client, even against his wish.

Views Received

3.37 Of the submissions received, less than 10% commented on this proposal. More than 60% of them agree to the rationale of this proposal. Some suggest that to genuinely safeguard the interests of the client, the exemption should be extended to cover non-governmental organisations which also provide many essential social welfare services. There is a suggestion that the exemption should cover social services that are run, subvented or subsidised by the Social Welfare Department ("SWD"). A respondent suggests that career counselling and placement services should be exempted as well.

3.38 Another respondent asks that the exemption be extended to cover private medical practitioners. The Hospital Authority ("HA")

also urges that it be exempted since it provides hospital and related healthcare services to the public, the importance of which is similar to that of social services. There is a suggestion that the public healthcare services provided by the Department of Health ("DH") should be exempted as well. It will be onerous for HA and DH, which together have over eight million patients, to comply with the requirements in paragraphs 3.24, 3.25, 3.27 and 3.28 above. Furthermore, modern delivery of healthcare services puts great emphasis on a multidisciplinary approach and cross-sectoral collaboration and patients need to be informed of the availability of various services.

3.39 On the other hand, some respondents consider that the proposed exemption would remove the right of citizens to refuse services provided by social services organisations. Some, including some from the direct marketing industry, comment that all organisations, be they commercial enterprises, charitable organisations or government bodies, should be subject to the same set of regulations and penalties.

Way Forward

3.40 Having carefully considered the views received, we propose that –

(a) social services run, subvented or subsidised by SWD;

(b) healthcare services provided by HA or DH; or

(c) social or healthcare services not covered by (a) or (b) above which, if not provided, would be likely to cause serious harm to the physical or mental health of the data subject or any other individual[8]

should be exempted from the provisions relating to direct marketing activities (i.e. section 34 of the PDPO and those in paragraphs 3.24 to 3.31 above).

[8] Reference is made to section 59 of PDPO which provides that personal data relating to the physical or mental health of the data subject are exempt from the provisions of either or both of (a) Data Protection Principle ("DPP") 6 and section 18(1)(b); (b) DPP3, in any case in which the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

Unauthorised Sale of Personal Data by Data User (Proposal (2) in the Consultation Report)

Proposal in the Consultation Report

3.41 Recent cases of transfer of customer personal data by enterprises for direct marketing purposes, some of which involving monetary gains, have aroused widespread community concerns. There are calls for criminalising such acts. We proposed in the consultation report that if a data user was to sell personal data to another person for a monetary or in kind gain, he should, before doing so, provide the data subject with information, which should be understandable and reasonably readable, on the kinds of personal data to be sold and to whom the personal data would be sold. The data user should also provide the data subject with an opportunity to indicate whether he agrees to (i.e. an opt-in mechanism) or disagrees with (i.e. an opt-out mechanism) the sale.

3.42 Non-compliance with any of the abovementioned requirements will be subject to the issue of an enforcement notice by the PCPD. The consultation report invited public views on whether the opt-in or opt-out mechanism should be adopted.

3.43 The consultation report proposed that it be 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 abovementioned requirements or against the wish of the data subject.

3.44 In the consultation report, we invited public views on the penalty, citing as reference the penalty for a broadly similar offence under section 58(1) of the UEMO, which is a fine of $1,000,000 and imprisonment for five years[9].

[9] 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) of the UEMO 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.

Views Received

3.45 Of the submissions received, around a quarter expressed views on this proposal. Most are in support. However, some business corporations and associations consider that there is no persuasive argument for such regulation and criminalising the sale of personal data is not consistent with international practices.

3.46 Respondents from the direct marketing industry, in particular, object to the application of the term "sale" to sharing and temporary transfer of data in exchange for fees or commissions, which is generally referred to as "list rental" and "data licensing". The data user has not parted with possession of the customers' personal data but merely "shared"/"licensed" them with/to its business partners, including through cooperative marketing activities. Some respondents from the direct marketing, financial services and information technology ("IT") sectors consider that these are legitimate commercial activities and should not be criminalised. Some respondents from the business sector also consider that business activities such as joint promotional or marketing activities should not be caught under the proposed offence.

3.47 Some other respondents, including the Office of the PCPD, consider that the proposed offence should cover such activities, if they involve monetary or in kind gain, so as not to create a loophole. The Office of the PCPD urges the Administration to specify clearly whether commission-based gains which are contingent upon successful engagement of customers would be covered.

3.48 Some respondents consider that some of the terms in the new requirements, such as "reasonably readable", are subject to wide interpretation. They also urge the PCPD to, in consultation with stakeholders, draw up guidelines or codes of practice to facilitate compliance.

3.49 Some respondents from the IT sector suggest that data users should be required to specify the type of companies to which data users may sell the personal data, rather than the names of individual companies. They consider it not practicable to spell

out the identity of the companies to which the data may be sold at the time of data collection.

3.50 Regarding whether the opt-in or opt-out mechanism should be adopted, almost 60% of those who expressed views on this support the opt-out mechanism. Less than 40% support the opt-in mechanism.

3.51 Supporters of the opt-out mechanism consider that, in addition to the considerations in paragraphs 3.9 to 3.13 above, an opt-out mechanism for the sale of personal data is consistent with the current PDPO and UEMO. It will also be in line with the opt-out mechanism proposed for the new requirements on collection and use of personal data for direct marketing activities and facilitate the understanding and implementation of the new requirements for sale of personal data by the industry and the general public.

3.52 Supporters of the opt-in mechanism, on the other hand, consider that it could offer better protection for personal data privacy as explicit consent of the data subject has to be sought for the sale of his personal data.

3.53 Only a few respondents expressed views on the penalty level of the proposed offence. Their views are diverse. Some agree to draw reference to the broadly similar offence under the UEMO. Some consider that the level of fine should be linked with the gain generated from the sale. Some respondents from the business sector consider the proposed imprisonment for five years disproportionate, while an individual respondent believes that the issue of an enforcement notice is sufficient as non-compliance of an enforcement notice is already a criminal offence.

3.54 Finally, some respondents suggest that defences similar to those in paragraph 3.16 should be provided if the proposal is to be taken forward.

<u>Way Forward</u>

3.55 Most of the views received support the introduction of the new offence against unauthorised sale of personal data by data user. We will take forward this proposal. Having regard to the views

received on the term "sell" and as a result the types of activities covered by this proposal, we propose to define the term "sell" as –

> "to make available, whether for a defined or indefinite period, to another person personal data for gain, including but not limited to monetary gain,
>
> (a) whether or not parting with possession of the personal data; and
>
> (b) whether or not the gain is contingent on other conditions."

In other words, the types of activities in paragraph 3.46 above referred to as "list rental" and "data licensing" in exchange for fees or commissions will be covered. These are the activities that have aroused widespread community concerns and calls for criminalisation. It should be noted that, in determining whether an act is a sale of personal data as defined above, the purpose for which the personal data are sold (whether for direct marketing or other purposes) is not a factor.

3.56 We also propose to adopt the opt-out mechanism to help avoid confusion with the requirements relating to collection and use of personal data for direct marketing and to facilitate compliance. In the light of the comments received, we propose to fine-tune the requirement to the effect that if a data user intends to sell personal data to be collected, he should, before or at the time of data collection –

(a) inform the data subject in writing of (i) the kinds of personal data to be sold and (ii) to which classes of persons the personal data may be sold. The layout and presentation of the information should be easily readable to individuals with normal eyesight and the language easily understandable; and

(b) provide an option, without charge, for the data subject to choose not to agree to the sale (i.e. an opt-out mechanism). The opt-out choice can be an all-or-nothing choice or the data user may allow the data subject to pick and choose among the kinds of personal data to be sold and the classes of persons to

whom the data may be sold stated by the data user. The data user will be allowed to adopt the opt-in mechanism instead of the opt-out mechanism, if he so chooses.

3.57 If a data user intends to sell personal data already collected (whether before or after the entry into force of the new requirements) and if any of the requirements in paragraph 3.56 (a) and (b) were not complied with before or at the time of data collection, the data user should, before the sale, comply with the requirements therein.

3.58 If, after the information and option required under paragraph 3.56 (a) and (b) are provided to the data subject, the data subject provides a response to the data user indicating that he does not opt out, the data user may proceed to sell the kind(s) of personal data to the class(es) of persons as stated by him. If the data subject does not respond to the data user, the data user may deem that the data subject has not opted out if no opt-out request is received within 30 days after the information and option are given to the data subject.

3.59 We propose to stipulate explicitly in the PDPO that a data subject may opt out any time, even if he has not opted out before or is deemed to have not opted out, and the data user has to cease to sell the personal data upon receipt of the opt-out request. We further propose that, if a data subject who has not opted out before or is deemed to have not opted out subsequently exercises the opt-out option provided by the data user as required under paragraph 3.56(b), the data subject may request the data user to notify the classes of persons to whom his personal data have been sold to cease to use the data. Upon receipt of the notification, the buyers have to cease to use the data. As regards erasure of such data, section 26 of the PDPO already stipulates the relevant requirement (see footnote 7).

3.60 Non-compliance with any of the requirements in paragraph 3.56(a) and (b) when the data user provides the information and option to the data subject will be subject to the issue of an enforcement notice, through which the PCPD can direct the data user to take remedial steps. Failure to comply with the enforcement notice will be an offence, as currently provided for under the PDPO. A

data user will commit an offence if he –

(a) does not comply with any of the requirements in paragraph 3.56 (a) and (b) and subsequently sells the personal data; or

(b) sells a kind of personal data or to a class of persons from which the data subject has opted out; or

(c) sells a kind of personal data or to a class of persons not covered in the information given to the data subject pursuant to the requirement in paragraph 3.56(a) above; or

(d) sells the personal data during the 30-day period mentioned in paragraph 3.58, before receiving the data subject's response, whether or not he subsequently receives a response from the data subject indicating that the latter does not opt out; or

(e) fails to comply with a data subject's request to notify the buyers to cease to use the personal data as required under paragraph 3.59.

A buyer referred to in paragraph 3.59 who, upon receipt of the notification, does not cease to use the personal data will commit an offence and be liable on conviction to a fine of $1,000,000 and imprisonment for five years.

3.61 In view of the community concern about unauthorised sale of personal data and to provide sufficient deterrent effect, we propose that the penalty should be a fine of $1,000,000 and imprisonment for five years. In order not to criminalise inadvertent acts, we propose that it shall be a defence for a data user to prove that he has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence. The PCPD will be requested to prepare guidelines or a code of practice in consultation with stakeholders to provide practical guidance on compliance with the new requirements.

Disclosure with a view to Gain or Cause Loss of Personal Data Obtained without the Data User's Consent
(Proposal (3) in the Consultation Report)

Proposal in the Consultation Report

3.62 The consultation report proposed that it should be an offence for a person (e.g. an employee of a data user) to disclose for profits or malicious purposes personal data which he obtained from a data user without the latter's consent. Examples of such acts cited in the consultation report include (a) sale to a third party by an employee of a company of customers' personal data which the employee obtained without the company's consent; and (b) disclosure to a third party by hospital staff of a patient's sensitive health records which the staff obtained without the hospital's consent. As regards the definition of "for malicious purposes", the consultation report suggested that one possible formulation was 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". It was proposed that the penalty should be set at the same level as that for the new offence of unauthorised sale of personal data by data users.

Views Received

3.63 Around 20% of the submissions received commented on this proposal. The majority are supportive.

3.64 Supporters consider that the proposal will help deter the inappropriate conduct of disclosure of personal data obtained without the data user's consent. There are, on the other hand, a few respondents from the direct marketing sector who consider that the existing PDPO already provides for sufficient protection and there is no need for extra regulation.

3.65 Some respondents consider the proposed definition of "for malicious purposes" appropriate. Some others, including both supporting and opposing respondents, express concerns and consider "for malicious purposes", particularly the phrase "injury to feelings" in the proposed definition, a wide and subjective concept.

3.66 Some respondents stress that it is important to avoid criminalising legitimate, unintentional or negligent activities so as not to unnecessarily hinder normal commercial operations. The IT sector argues that in most cases, the harm (especially injury to feelings) caused by the disclosure may be outside the intent or expectation of the person who discloses the data. In addition to the defences in the UK Data Protection Act ("UK Act")[10], some respondents suggest adding further defences including "without willful intent", "in accordance with the data subject's instruction" and "in reasonable belief". Some point out that the behaviors to which many Internet users are currently accustomed may come very close to being caught by the proposed offence. Clear guidelines must be issued.

3.67 On the other hand, the Office of the PCPD considers that the proposed offence is much narrower in scope than that provided for under section 55 of the UK Act (see footnote 10). The scope of protection will therefore be limited.

3.68 Only a few respondents commented on the penalty. More than half support the proposed penalty. Individual organisations from the financial services sector and legal sector propose a lower penalty level while another organisation from the legal sector considers a higher penalty more appropriate.

3.69 The Office of the PCPD suggests that the right to claim civil remedy, such as injunction order, should be clearly and explicitly spelt out in the PDPO.

Way Forward

3.70 The views received generally agree to the direction that the

[10] Section 55(1) of the UK Act provides that a person must not knowingly or recklessly, without the consent of the data controller – (a) obtain or disclose personal data or the information contained in personal data, or (b) procure the disclosure to another person of the information contained in personal data. The Act provides that section 55(1) does not apply to cases where (a) the obtaining, disclosing or procuring was necessary for preventing or detecting crime; (b) the obtaining, disclosing or procuring was required or authorised by any enactment, rule of law or order of a court; (c) the person acted in the reasonable belief that he had in law the right to obtain, disclose or procure the disclosure; (d) the person acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; (e) in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest; and (f) the person acted for the special purposes, with a view to the publication by any person of any journalistic, literary or artistic material and in the reasonable belief that such act was justified as being in the public interest.

irresponsible act of disclosing for profits or malicious purposes personal data obtained without the data user's consent should be made an offence.

3.71 Having regard to the comments received on the proposed definition of "for malicious purposes" and the concerns over criminalising unintentional activities, we have refined our proposal. We now propose that it will be an offence for a person to disclose personal data, which he obtained from a data user without the latter's consent –

(a) with a view to gain in money or other property for himself or another; or

(b) with an intent to cause loss in money or other property or psychological harm to the data subject.

3.72 In particular, we have replaced the term "injury to feelings" in the earlier proposal set out in the consultation report with "psychological harm" in the current proposal. There are references to both the terms "psychological harm" and "injury to feelings" in the laws of Hong Kong[11], though there are no definitions of the two terms in those ordinances. According to the dictionary, "injury to feelings" may mean injury to one's sensation, desire and emotion, while "psychological harm" may mean harm done to the mind, mental aspect of a person. The scope of "psychological harm" seems more limited than that of "injury to feelings" and it is more likely than not that expert evidence will be relied on to prove that harm has been caused to the psychological aspect of a person. As the current proposal involves a criminal offence, we propose to adopt the term "psychological harm", the scope of which is more concrete.

3.73 Regarding defences, taking into account the views received and making reference to the UK Act while heeding the much narrower

[11] There are references to the term "psychological harm" in section 2 of the Organized and Serious Crimes Ordinance (Cap. 455) and Schedule 1 to the Child Abduction and Custody Ordinance (Cap. 512). There are references to the term "injury to feelings" in the following provisions on civil claims : section 66 of the PDPO (Cap. 486), section 76 of the Sex Discrimination Ordinance (Cap. 480), section 72 of the Disability Discrimination Ordinance (Cap. 487), section 54 of the Family Status Discrimination Ordinance (Cap. 527) and section 70 of the Race Discrimination Ordinance (Cap. 602).

scope of our proposed offence than that under the UK Act, we propose to provide for the following defences –

(a) the person making the disclosure acted in the reasonable belief that the disclosure was necessary for the purpose of preventing or detecting crime;

(b) the disclosure was required or authorised by any enactment, rule of law or order of a court;

(c) the person making the disclosure acted in the reasonable belief that he had the consent of the data user; and

(d) the disclosure was for the purpose of news activity or any directly related activity and the person making it had reasonable grounds to believe that the publishing or broadcasting of the data was in the public interest.

3.74 On penalty, in view of the seriousness of the offence, the penalty will be set at the same level as that for the new offence of unauthorised sale of personal data by data users, i.e. liable on conviction to a fine of $1,000,000 and imprisonment for five years.

3.75 As regards the suggestion of the Office of the PCPD that the right to claim civil remedy, such as injunction order, should be explicitly spelt out in the PDPO, the right is in fact provided for under section 21L of the High Court Ordinance (Cap. 4). Pursuant to that section, the Court of First Instance may by order (whether interlocutory or final) grant an injunction or appoint a receiver in all cases in which it appears to the Court of First Instance to be just or convenient to do so.

Regulation of Data Processors and Sub-contracting Activities (Proposal (5) in the Consultation Report)

Proposal in the Consultation Report

3.76 To strengthen the regulation of data processors and sub-contracting activities, the consultation report proposed continuing with the existing indirect regulation approach but

going 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 be subject to the issue of an enforcement notice by the PCPD.

3.77 The consultation report also proposed that the Office of the PCPD should step up publicity and education in relation to sub-contracted data processing, and issue codes of practice or guidelines as and when necessary to provide practical guidelines on the terms and conditions to be included in a contract between the data user and its data processor.

3.78 Under section 2(12) of the PDPO, a person is not taken to be a data user if he holds, processes[12] or uses personal data solely on behalf of another person, and not for any of his own purposes. Not being a data user, a data processor is not required to comply with the requirements of the PDPO, including the data protection principles ("DPPs"). By virtue of section 65(2) of the PDPO, a data user who engages an agent to process the personal data shall be held liable for any acts done by its agent with its authority (whether express or implied, whether precedent or subsequent). In other words, data processors are regulated indirectly through the data users that engage them.

3.79 The consultation report did not propose to adopt the option of directly regulating data processors. The IT sector opposed direct regulation as many data processors only provide a platform for processing of data and may not know whether the data being handled by them contain personal data, or the use purpose of the data. Direct regulation of data processors is impractical and will increase the burden and operating costs of the industry.

Views Received

3.80 Of the submissions received, close to 20% commented on this proposal. The majority supports the general direction of strengthening the regulation of data processors and

[12] Under section 2 of the PDPO, "processing", in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.

sub-contracting activities and agrees that the Office of the PCPD should step up publicity and education efforts in relation to sub-contracted data processing and provide practical guidelines to data users.

3.81 Of the respondents who support strengthening the regulation of data processors and sub-contracting activities, more than 40% support the proposed indirect regulation of data processors and sub-contractors. They also agree that the PCPD should provide practical guidance on the drafting of the terms and conditions of contracts between data users and their data processors. However, there are also views that the PCPD should allow flexibility to data users to craft appropriate contractual provisions and should not mandate specific model clauses for inclusion in the contracts.

3.82 Around one-third of those who support strengthening regulation of data processors and sub-contracting activities, including the Office of the PCPD[13], consider it more appropriate to regulate data processors and sub-contractors directly. They consider this more effective and it is unfair for data users to bear all the responsibilities for the wrongdoings of their data processors and sub-contractors.

3.83 However, some respondents from the IT sector express concerns on the possible effects of direct regulation on Internet-related businesses since it is not uncommon that these data processors have no knowledge of the details or even the nature of the data they are processing. They consider that indirect regulation can strike a balance between the protection offered to data subjects and the operations of Internet-related businesses. Besides, some respondents consider that while data users should use contractual means to ensure that their data processors comply with the requirements under the PDPO, the data processors should also be subject to the enforcement actions of the PCPD if they contravene the requirements under the PDPO.

3.84 Some respondents from the business and financial services sector

[13] The PCPD has sent a questionnaire on this proposal to 10 IT bodies and Internet-related associations which had made submissions during the 2009 public consultation and/or approached the PCPD during the further public discussions. Of the five respondents, four support adopting direct regulation and the other one indicates that there are pros and cons.

consider that defences should be provided. It should be a defence if the data user can demonstrate that appropriate contractual provisions are in place and that he has already taken reasonable and practicable steps to enforce these provisions.

Way Forward

3.85 The practical concerns about subjecting data processors to direct regulatory regime are valid since many data processors only provide a platform for processing of data and may not know whether the data being handled by them contain personal data, or the use purpose of the data. Adopting a direct regulatory regime would impose onerous burden on the industry.

3.86 We will introduce amendments to the PDPO to require data users to use contractual or other means to ensure that their data processors and sub-contractors, whether within Hong Kong or offshore, comply with the requirements under the PDPO. This requirement is modeled on a similar provision in the Personal Information Protection and Electronic Documents Act of Canada[14]. The Privacy Commissioner of Canada has issued guidelines to facilitate compliance[15].

3.87 We consider that the primary means by which data users comply with the new requirement is through contracts. If this is not practicable or feasible, the data user should use other means to ensure compliance by his data processors. For example, he has to be satisfied that his data processor has policies and processes in place, including training for its staff and effective security measures, to ensure that the personal data in its care are properly

[14] Clause 4.1.3 of Schedule 1 to the Personal Information Protection and Electronic Documents Act of Canada provides that: "[a]n organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party".

[15] The "Guidelines for Processing Personal Data Across Borders" issued by the Office of the Privacy Commissioner of Canada provide that "[r]egardless of where the information is being processed – whether in Canada or in a foreign country – the organisation must take all reasonable steps to protect it from unauthorised uses and disclosures while it is in the hands of the third party processor. The organisation must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores personal information, and exercise the right to audit and inspect when warranted".

safeguarded at all times. These are similar to the guidelines issued by the Privacy Commissioner of Canada.

3.88 The PCPD will be requested to issue guidelines to provide practical guidance to data users to facilitate their compliance with the new requirement, including, for reference purpose, guidelines on the terms and conditions to be included in a contract between the data user and its data processor, and guidelines on other means to comply with the new requirement. The Office of the PCPD will also be requested to step up publicity and education efforts in relation to sub-contracted data processing activities.

3.89 Contravention of the new requirement will render the data user liable to the issue of an enforcement notice by the PCPD, through which the PCPD can direct the data user to take remedial actions. Failure to comply with the enforcement notice will be an offence as currently provided for under the PDPO.

Personal Data Security Breach Notification (Proposal (6) in the Consultation Report)

Proposal in the Consultation Report

3.90 The consultation report proposed to start with that a voluntary personal data security breach notification system, under which organisations would notify the PCPD and affected individuals when a breach of data security leads to the leakage of personal data, so as to mitigate the potential damage to affected individuals.

3.91 It is also proposed that the Office of the PCPD should undertake promotional and educational initiatives to raise awareness of its guidance note entitled "Data Breach Handling and the Giving of Breach Notifications", promote adoption of a privacy breach notification system by data users voluntarily and assist data users in making appropriate notifications.

3.92 The consultation report did not propose to make the notification system mandatory. The main consideration is that privacy breach notification system is still in the development stage and there are no clear or objective standards for notification or

common practices[16]. There are worries about how the system is going to operate and the onerous burden brought to data users if a mandatory notification system is to be implemented. The impact of a mandatory privacy breach notification cannot be underestimated. It would be more prudent to start with a voluntary notification system first, 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 imposing onerous burden on the community.

Views Received

3.93 Around 13% of the submissions received commented on this proposal. They generally agree that guidance from the PCPD on privacy breach notification and promotional and educational initiatives are useful and necessary to assist data users in making appropriate notifications. Of these submissions, about half support a voluntary system while around a quarter support a mandatory system. Some propose a mixed system under which mandatory notification would be required only for breaches involving certain types of data or data users.

3.94 Respondents who support a voluntary system consider that making it mandatory will impose undue burden on data users. On the other hand, respondents who support a mandatory system consider a voluntary one ineffective as it may not provide sufficient incentive for businesses or institutions to act accordingly. Some respondents, including the Office of the PCPD, suggest that the mandatory system can be introduced by phases to minimise disruption to commercial operation.

Way Forward

3.95 Starting with a voluntary privacy breach notification system will

[16] A number of overseas jurisdictions such as many states in the United States of America and the European Parliament have set up a mandatory privacy breach notification system, while other jurisdictions such as the UK and New Zealand do not have a mandatory privacy breach notification system. Privacy authorities in those jurisdictions have promulgated voluntary guidelines for data users to follow in the event of privacy breach. Canada is moving towards a mandatory notification approach. Moreover, during the public consultation in 2009 on the consultation document, there was a wide divergence in the views received on the particulars of the notification system, including the time limit for issuing and the recipients of notifications.

allow us to adjust and fine-tune as necessary the detailed arrangements for notification, having regard to actual operational experience and assessment on the impact of leakage notification. This can help make the privacy breach notification system more reasonable and practicable, without causing onerous burden on the community. This has gained support during the further public discussions. We will proceed accordingly.

3.96 To facilitate data users in giving breach notifications, the PCPD promulgated a guidance note in June 2010. The guidance note provides step-by-step guidance and assistance to data users in handling data breaches together with a sample data breach notification form for data users to notify the PCPD in case of data breaches.

3.97 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 privacy breach notification system and assist data users to make appropriate notifications. We will also, together with the PCPD, keep the guidance note under review and the PCPD will make appropriate revisions where necessary.

Legal Assistance to Data Subjects (Proposal (7) in the Consultation Report)

Proposal in the Consultation Report

3.98 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 under section 66 of the PDPO to compensation from the data user for that damage. The consultation report proposed empowering the PCPD 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.

3.99 Such assistance will include giving legal advice on the sufficiency of evidence and arranging for a lawyer to represent the applicant in legal proceedings. To ensure proper use of public funds, applications for legal assistance would only be considered if 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 or any other matter.

Views Received

3.100 Of the submissions received, around 15% expressed views on this proposal. Around two-thirds are supportive.

3.101 Those in support consider that the proposal can offer better assistance to aggrieved data subjects to seek redress under the PDPO. Some respondents also comment that the PCPD, similar to the Equal Opportunities Commission ("EOC"), should be conferred the power to provide legal assistance and sufficient financial resources should be provided to the PCPD to exercise the new power. They also support the factors to be considered in granting legal assistance as set out in paragraph 3.99 above.

3.102 Those who object to the proposal consider that the PCPD should retain his current independent role and the aggrieved data subjects can, if needed, seek legal assistance through the existing channels such as the Legal Aid Department. Some respondents consider it inappropriate to compare the PDPO regime to that of the EOC as they deal with issues of different nature.

Way Forward

3.103 The views received generally support empowering the PCPD to provide legal assistance to aggrieved data subjects. We will introduce amendments to the PDPO accordingly.

3.104 We further propose to, following the EOC model, add a provision to the PDPO stipulating that proceedings under section 66 shall be brought in the District Court and amend the District Court Ordinance (Cap. 336) to provide that each party (i.e. the claimant and the respondent) has to each bear his own costs unless the District Court otherwise orders on the ground that the proceedings were brought maliciously or frivolously or there are special circumstances which warrant an award of costs. This is to remove fear of the victim having to bear possibly huge legal fees

in the event he loses the case.

Time Limit for Responding to PCPD's Investigation / Inspection Report
(Pages 177-178 of the Consultation Report)

The Proposal

3.105 Under section 46(4) of the PDPO, before the PCPD publishes an inspection or investigation report, he has to provide a copy of the report to the relevant data user and invite the data user to advise within 28 days whether he objects to the disclosure in the report of any personal data that are exempted from the provisions of DPP 6 by virtue of an exemption under Part VIII of the PDPO. The Office of the PCPD has proposed to shorten the period from 28 days to 14 days on the ground that the present response period hinders timely reporting of matters of public interest.

3.106 In the consultation report, we stated that we did not intend to take forward the proposal, as data users may need to circulate the report for comments and seek legal advice before they can provide a formal response to the PCPD. A response period of 14 days is unreasonably tight for such a course of action.

Views Received

3.107 During the public consultation in 2009, only a handful of respondents expressed views on this proposal. The majority agree that the proposal should not be pursued. The Office of the PCPD, however, urges the Administration to reconsider it since in cases involving public interest, a swift response should be given to address the public concern. Moreover, it is a waste of time for the PCPD to, as currently required under section 46(4) of the PDPO, invite the data user to advise within 28 days whether he has any objection even if there are no personal data mentioned in the report.

Way Forward

3.108 We have carefully considered the PCPD's latest submission. We agree that, if an investigation or inspection report does not contain

any personal data, there should not be a need for the PCPD to invite the data user to advise within 28 days whether he has any objection. The requirement in section 46(4) should only apply to investigation and inspection reports that contain personal data. We will introduce amendments to the PDPO to this effect.

Others

3.109 The consultation report also set out some other proposals that we intended to take forward. These proposals attracted not many comments during the further public discussions.

3.110 In general, most of the submissions are supportive of those proposals. Some of them offered suggestions or comments on implementation details of individual proposals or the drafting of legislative amendments. We will proceed with these proposals and take these suggestions and comments into account carefully when drafting the legislative amendments. These proposals are summarised at **Appendix D**.

Chapter Four : Proposals Not to be Implemented

4.1 The consultation report also set out the proposals which the Administration had considered but did not intend to pursue. Having considered the views received during the further public discussions, we maintain our stance of not taking forward these proposals.

Sensitive Personal Data
(Proposal (38) in the Consultation Report)

The Proposal

4.2 In the consultation report, we stated that we did not intend to introduce a more stringent regulatory regime for sensitive personal data, such as prohibiting the collection, holding, processing and use of such data except under specific circumstances. The reason is that there are no mainstream views in the community on the coverage of sensitive personal data, the regulatory model or sanctions. The IT sector has also raised strong objection to classifying biometric data as sensitive personal data.

4.3 Instead, we proposed that –

(a) the Office of the PCPD should step up promotion and education and, where necessary, issue codes of practice or guidelines to suggest best practices on the handling and use of sensitive personal data, such as biometric data and health record; and

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

Views Received

4.4 Around 15% of the submissions received expressed views on this proposal. About half are against the introduction of a more stringent regulatory regime for sensitive personal data, with a slightly smaller number in support.

4.5 Of those against classifying personal data into different categories and introducing different regulatory regimes for them, some consider it inflexible to treat certain categories of personal data as sensitive in all circumstances. It may not be possible to categorise data by sensitivity and whether certain data are sensitive depends on how the data are used. Instead of singling out certain types of personal data for more stringent regulation, the Government should aim at strengthening protection for all kinds of personal data.

4.6 There are also views that without consensus in the community, any legislative amendments that would lead to uncertainty and potentially increase the burden on commercial operations should not be pursued. Some respondents suggest that higher degree of protection for sensitive personal data can equally be achieved through the issue of codes of practice or guidelines.

4.7 During the public consultation in 2009, the IT sector raised strong objection to classifying biometric data as sensitive data, for it would affect the daily operation and development of the sector. During the further public discussions, quite a number of respondents from the IT sector welcomed the Government's position of not pursuing this proposal.

4.8 On the other hand, some respondents, including the Office of the PCPD[17] consider that, to provide better protection for personal data privacy, more stringent regulation should be imposed on the handling of sensitive personal data in line with the European standards. If not, Hong Kong will be lagging behind these jurisdictions.

Way Forward

4.9 Implementation of this proposal will have a wide impact on the community. There are no mainstream views in the community on the coverage of sensitive personal data, the regulatory model or

[17] The Office of the PCPD has solicited public views on this proposal as part of the two surveys mentioned in paragraph 3.20. For the online survey, of the 1 208 respondents, 443 (37%) support imposing stringent regulation on sensitive personal data, 701 (58%) object while 64 (5%) have no comment. According to the Office of the PCPD, 293 of the objecting responses were submitted by a call centre. For the questionnaire survey, of the 43 respondents, 20 (47%) support the proposal, 10 (23%) object and 13 (30%) have other views or no comment.

sanctions. We, therefore, do not intend to pursue the proposal at this stage. Instead, the measures stated in paragraph 4.3 above will be taken to enhance the protection for sensitive personal data.

Granting Criminal Investigation and Prosecution Powers to the PCPD
(Proposal (39) in the Consultation Report)

The Proposal

4.10 In the consultation report, we stated that we did not intend to pursue the proposal to confer on the PCPD the power to carry out criminal investigations and prosecutions. We consider it important to retain the existing arrangement, under which the Police conduct criminal investigation and Department of Justice initiates and undertakes prosecution, in order to maintain checks and balances.

Views Received

4.11 More than 65% of the submissions received expressed views on this proposal, most of which were against the proposal to grant criminal investigation and prosecution powers to the PCPD, as opposed to a few in support.

4.12 Most respondents consider that the PCPD will have excessive power if enforcement and prosecution powers are conferred on him. It will also cause confusion over his role and deter data users from seeking help from him to comply with the requirements of the PDPO. They agree that criminal investigation and prosecution powers should be vested in different organisations to maintain checks and balances.

4.13 The Office of the PCPD, among the few in support of the proposal, reiterates that, with such powers, the PCPD will be more effective and efficient in enforcing the PDPO. Also, the proposal to grant prosecution power to the PCPD will not prejudice the Secretary for Justice's discretion to prosecute. Any prosecution will be subject to the consent of the Secretary for Justice. The proposal will only entail the carrying out of prosecution work by the PCPD.

Way Forward

4.14 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 remains that criminal investigation and prosecution powers should continue to be vested in separate organisations to ensure checks and balances.

4.15 For cases referred by the PCPD, the Police have issued guidelines to frontline officers setting out the procedures in handling such cases. 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 an appropriate unit in a timely manner for investigation. The Police and the Department of Justice are also working with the PCPD with a view to enhancing investigation and prosecution work.

Empowering the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal (40) in the Consultation Report)

The Proposal

4.16 In the consultation report, we stated that we did 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.

4.17 The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC")'s "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 had been a breach of the DPPs. It would be for a court to determine the appropriate amount of

compensation payable. Our view is that these considerations remain valid. The data subjects concerned can seek compensation through the court as provided for under section 66 of the PDPO.

Views Received

4.18 Almost half of the submissions received expressed views on this proposal, most of which consider it undesirable to vest in a single authority a combination of enforcement and punitive functions and are against the proposal to empower the PCPD to award compensation to aggrieved data subjects. Some respondents consider that there is no strong evidence showing that the present system is not working effectively to serve its purpose and therefore a drastic expansion of the PCPD's powers is not justified.

4.19 Only a few, including the Office of the PCPD[18], support this proposal. The Office of the PCPD suggests that the proposal will generate direct and effective deterrent effect on data users against infringement of the PDPO.

Way Forward

4.20 In the light of the comments received, our views remain as that stated in paragraph 4.17 above. We do not consider it appropriate to pursue the proposal to empower the PCPD to award compensation to aggrieved data subjects.

[18] The Office of the PCPD has solicited public views on this proposal as part of the two surveys mentioned in paragraph 3.20. For the online survey, of the 1 207 respondents, 319 (26%) support empowering the PCPD to award compensation to aggrieved data subjects and to encourage settlement by reconciliation, 799 (66%) object while 89 (8%) have no comment on the proposal. According to the Office of the PCPD, 292 of the objecting responses were submitted by a call centre. For the questionnaire survey, of the 43 respondents, 10 (23%) support the proposal, 13 (30%) object and 20 (47%) have other views or no comment.

Empowering the PCPD to Impose Monetary Penalty for Serious Contravention of Data Protection Principles
(Proposal (42) in the Consultation Report)

The Proposal

4.21 In the consultation report, we stated that we did not intend to pursue the proposal to empower the PCPD to impose monetary penalty on data users for serious contravention of DPPs.

4.22 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.

Views Received

4.23 Almost half of the submissions received expressed views on this proposal, most of which consider it undesirable to vest in a single authority a combination of enforcement and punitive functions and are against the proposal to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. Some respondents consider that there is no strong evidence showing that the present system is not working effectively to serve its purpose and therefore a drastic expansion of the PCPD's powers is not justified.

4.24 Only a few, including the Office of the PCPD[19], support this proposal. The Office of the PCPD suggests that the proposal will generate direct and effective deterrent effect on data users against infringement of the PDPO.

Way Forward

4.25 Having regard to the comments received, our views remain as

[19] The Office of the PCPD has solicited public views on this proposal as part of the two surveys mentioned in paragraph 3.20. For the online survey, of the 1 214 respondents, 389 (32%) support empowering the PCPD to impose monetary penalty to serious contravention of DPPs, 778 (64%) object while 47 (4%) have no comment. According to the PCPD, 291 of the objecting responses were submitted by a call centre. For the questionnaire survey, of the 43 respondents, 13 (30%) support the proposal, 12 (28%) object and 18 (42%) have other views or no comment.

stated in paragraph 4.22 above. We do not consider it appropriate to pursue the proposal to empower the PCPD to impose monetary penalty on data users for serious contravention of DPPs.

Others

4.26 We also set out in the consultation report some other proposals that we did not intend to take forward. These proposals are –

(a) to make contravention of a DPP an offence (Proposal (41) in the consultation report);

(b) to permit a data user to refuse a data access request made by a "relevant person" (i.e. a person who has parental responsibility for a minor) on behalf of a minor in order to protect the interests of minors (Proposal (43) in the consultation report);

(c) for the purpose of imposition of a fee for complying with a data access request, to provide in the PDPO a fee schedule and to require data users not to charge fees in excess of the maximum level prescribed in the fee schedule (Proposal (44) in the consultation report); and

(d) those in Annex 5 to the consultation report (except the one on time limit for responding to PCPD's investigation or inspection report, which we will now pursue in a revised form, as set out in Chapter Three of this report) which we have considered but do not intend to pursue[20].

4.27 These proposals attracted few comments during the further public discussions. We maintain our stance of not taking forward these proposals.

[20] The proposals relate to: Internet protocol address as personal data, territorial scope of the PDPO, public interest determination, public domain exemption, the PCPD's power to search and seize evidence, the PCPD's power to call upon public officers for assistance and the PCPD's power to conduct hearing in public.

Chapter Five : Conclusion

5.1 During the further public discussions, we engaged the community through a variety of channels in discussing the legislative proposals set out in the consultation report. The public generally support strengthening regulatory measures and promotion and public education efforts to enhance protection of personal data privacy.

5.2 In the light of the views received, we have revised and refined the details of some of the proposals and will implement the proposals outlined in Chapter Three of and **Appendix D** to this report. We are preparing a bill to amend the PDPO to implement these proposals. Our aim is to introduce it into the LegCo in July 2011.

Appendix A

Overview of the Personal Data (Privacy) Ordinance

1. The PDPO was enacted in August 1995 in response to the general recognition of a need to protect the privacy of individuals in relation to personal data by legislative means. The Ordinance seeks to ensure proper protection of an individual's right to privacy with regard to personal data, and obviate the risk of restrictions imposed by other jurisdictions on the free flow of personal data to Hong Kong. Its provisions were largely based on the recommendations of the LRC Report on Reform to the Law Relating to the Protection of Personal Data, which was released in August 1994 following the conduct of a thorough and extensive public consultation exercise. In a nutshell, the LRC recommended that the internationally agreed data protection guidelines should be given statutory force in both the public and private sectors.

2. 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.

3. The PDPO gives statutory effect to internationally accepted DPPs, 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 unauthorised 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.

4. The PDPO gives certain 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.

5. The PDPO imposes conditions on the use of personal data in automated matching processes and conditions on transfer of personal data to places outside Hong Kong (the relevant provisions have not come into operation). The Ordinance also regulates the

use of personal data in direct marketing by data users.

6. 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 access by data subjects (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 access by data subjects requirements (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.

7. 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 or the matters occasioning it. If the data user fails to comply with the enforcement notice issued by the PCPD, he is liable to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily fine of $1,000.

8. 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 ($10,000) to a fine at Level 5 ($50,000) and imprisonment for two years. Non-compliance with an enforcement notice attracts the highest level of penalty under the PDPO.

9. "Data user" is defined in section 2 of the PDPO as a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. A company may also be guilty of an offence. As to whether the directors or other officers of the company may also be guilty of the same offence, it will depend on the available evidence against each individual separately.

10. 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.

Appendix B

Summary of Views Expressed at Public Forums

First Forum

Date: 4 November 2010 (Thursday)
Time: 7:00 – 9:00 p.m.
Venue: Youth Square, Chai Wan
Organiser: Constitutional and Mainland Affairs Bureau

Direct Marketing and Related Matters

1. Some participants raised concern over the transfer of personal data among different departments of the same company or its subsidiaries for a purpose different from the purpose at the time of data collection. A participant suggested that these activities should be regulated under the PDPO.

2. A participant considered that data subjects should be given the right to decide how their personal data would be used. Data users should not include any hidden terms and conditions in the service contracts that would mislead data subjects to give consent to unintended use or transfer of their personal data.

3. A participant suggested that the new requirements to be introduced in the PDPO should have retrospective effect. Data users should be required to review their existing privacy policies and remove any misleading terms and conditions.

4. Regarding whether the opt-in or opt-out mechanism should be adopted, a participant said that if the opt-in mechanism was adopted, data users who had collected data and given an opt-out choice to data subjects before the new requirements came into force would be required to seek consent from data subjects again, even if they had not exercised their opt-out right before. This would be burdensome to data users.

5. A participant expressed his support for the establishment of a central register for use of personal data for direct marketing purposes. However, another participant opined that if the personal data of an individual were transferred to different data

users for direct marking purposes, it would be a hassle for the data subject to update his records in the central register.

6. As regards the unauthorised sale of personal data by data users, a participant suggested that buyers of personal data for direct marketing purposes should also be regulated under the legislative proposals.

7. A participant expressed support to exclude from the definition of "direct marketing" the offering of social services and facilities. Another participant enquired if medical services should also be excluded from the regulations on direct marketing.

Erasure of Personal Data

8. A participant was of view that once a data subject opted to terminate the service, his personal data should be deleted from the active account. However, he did not oppose the data user's retention of the personal data for a period of time in a dummy or other account to which third-party access would be prohibited.

Sensitive Personal Data

9. A participant enquired whether a person's criminal record would be considered as sensitive personal data. He also enquired whether overseas offence records or records of offence committed many years before would be governed by the PDPO.

10. Since finger print data are normally regarded as sensitive, one participant enquired whether finger print data should continue to be used to verify individual's identity at border control points.

Statutory Powers and Functions of the PCPD

11. A participant raised concern that if the PCPD were to be given additional power, he might have excessive power to freely access personal data of individuals at his own will. On the other hand, a participant pointed out that some corporations did not strictly follow the guidelines issued by the PCPD and considered that the PCPD's sanctioning power should be increased.

Strengthening of Education and Publicity

12. A participant opined that more education and promotion programmes on personal data privacy should be introduced, in particular on the subject of the use of identity card number.

Others

13. Some participants enquired how personal data privacy was monitored and protected under the current legislation under certain circumstances, for example the use of personal data collected by closed-circuit television system and measures to mitigate damage caused by leakages of patients' personal data by hospitals.

Second Forum

Date: 29 November 2010 (Monday)
Time: 7:00 – 9:00 p.m.
Venue: Cultural Activities Hall Tsuen Wan Town Hall
Organiser: Constitutional and Mainland Affairs Bureau

Direct Marketing and Related Matters

1. Several participants quoted their personal experience of receiving direct marketing calls from telecommunications companies, banks and financial institutions. They found these calls annoying. Some suggested that tighter regulations and heavier penalty should be imposed on unauthorised use of personal data in direct marketing activities and unauthorised sale of personal data.

2. A participant suggested that data subjects should be allowed to indicate consent in a central register to the use of their personal data in direct marketing activities.

3. A participant pointed out that a common business practice was to require data subjects to give bundled consent to the terms and conditions of the service and the purposes for which the personal data collected were to be used. He considered that there should be some regulation over this business practice.

4. A participant enquired whether the definition of direct marketing would be limited to marketing of services or goods, or also other purposes, such as persuading individuals to sell their properties. He also enquired whether transfer of personal data for gain other than monetary gain would be regulated.

5. On the exclusion of the offering of social services and facilities by social workers from the definition of "direct marketing" under section 34 of the PDPO, a participant expressed support for this proposal as it would be beneficial to clients receiving or in need of such services. He also opined that the scope of the proposed exemption should be set out clearly to prevent abuse.

Statutory Powers and Functions of the PCPD

6. On the proposal to grant the PCPD criminal investigation and prosecution powers, a majority of participants raised concerns that the PCPD might have excessive power. It was uncertain how checks and balance could be maintained.

7. In particular, a participant objected to the granting of prosecution power to the PCPD. He considered that prosecution work should continue to be carried out by the Department of Justice to maintain checks and balance.

8. On the other hand, a participant indicated support, on the ground that time and resources would be saved if preliminary investigation and criminal investigation were conducted by the same organisation.

Implementation and Implications of the Proposed Legislative amendments

9. A participant was concerned whether the proposed legislative amendments would have retrospective effect, in particular whether data users would be required to make personal data security breach notification for incidents occurring before the implementation and whether customers would be given the opportunity to indicate disagreement with the use of personal data which were given before the implementation, for direct marketing purpose. Another participant also enquired about the financial implications on data users and the PCPD after the implementation of the proposed legislative amendments.

Others

10. Some participants enquired how personal data privacy was monitored and protected by the current legislation under certain circumstances, for example the use of identity card number for security purpose and why some companies were not penalised even a large number of personal data were involved in various incidents.

11. A participant expressed concern that some limited companies might try to escape from their legal liabilities by appointing directors to

bear the criminal liabilities. He was of the view that there should be heavier punishment on the company, such as imposing suspension on operation for a certain period of time.

Appendix C

Forums and Seminars Attended by the Administration

	Date	Forums/Seminars
1.	21 Oct	Briefing for Chairmen and Vice Chairmen of District Councils
2.	19 Nov	Children's Rights Forum
3.	23 Nov	Briefing for Hong Kong Retail Management Association
4.	24 Nov	Consultation forum on the review of the PDPO organised by the Electronics Division and Information Technology Division of the Hong Kong Institution of Engineers
5.	25 Nov	Roundtable on the legislative proposals arising from the review of the PDPO organised by: - Internet Professional Association - Information Systems Audit and Control Association, China Hong Kong Chapter - Office of the Hon. Samson Tam
6.	26 Nov	Seminar on "Personal Data Privacy Protection – How Will the Latest Proposals Affect Your Business?" organised by Hong Kong General Chamber of Commerce
7.	7 Dec	Roundtable discussion with: - Hong Kong Chamber of Small and Medium Business - Hong Kong Promotion Association for Small and Medium Enterprises - Hong Kong Small and Medium Enterprises Association - Hong Kong Small and Medium Enterprises Development Association - SME Global Alliance - SME Mentorship Association
8.	8 Dec	Working Group on Advocacy, The Boys' and Girls' Clubs Association of Hong Kong
9.	9 Dec	Open Forum on Legislative Proposals of PDPO co-organised / supported by: - The Professional Commons - IT Voice - Internet Society Hong Kong - Hong Kong Internet Service Providers Association - Hong Kong Information Technology Federation - Information Systems Audit and Control Association, China Hong Kong Chapter

	Date	Forums/Seminars
		- Professional Information Security Association - Communications Association of Hong Kong - Association for Computing Machinery – Hong Kong Chapter - Hong Kong Association of Interactive Marketing - Institute of Electrical and Electronics Engineers, Hong Kong Section Computer Society Chapter - Information Security and Forensics Society
10.	10 Dec	Dialogue between Citizens and Official – Forum on the Review of the PDPO organised by: - Community Development Initiative - Roundtable Community - Power for Democracy
11.	13 Dec	Roundtable discussion with: - Hong Kong Monetary Authority - Hong Kong Association of Banks - Hong Kong Association of Restricted Licence Banks and Deposit-taking Companies - Securities and Futures Commission - Chinese Securities Association of Hong Kong - Hong Kong Association of Online Brokers - Hong Kong Securities Association - Hong Kong Securities Professionals Association - Institute of Financial Planners of Hong Kong - Office of the Commissioner of Insurance - Hong Kong Federation of Insurers - Mandatory Provident Fund Schemes Authority - Hong Kong Investment Funds Association
12.	14 Dec	Human Rights Forum
13.	14 Dec	Roundtable discussion with Hong Kong Institute of Marketing
14.	16 Dec	Roundtable discussion with: - Asia Digital Marketing Association - Hong Kong Call Centre Association - Hong Kong Direct Marketing Association - Hong Kong Retail Management Association - Hong Kong Telemarketers Association

Appendix D

Other Proposals to be Implemented

Statutory Powers and Functions of the PCPD

Circumstances for Issue of an Enforcement Notice (Proposal (8) in the Consultation Report)

- To amend the circumstances under which the PCPD may, following the completion of an investigation, issue an enforcement notice to a data user, so that an enforcement notice may be issued in situations where the data user has contravened a requirement under the PDPO, irrespective of whether there is evidence to show that the contravention will likely be repeated.

- In deciding whether to serve an enforcement notice, the PCPD still has to follow the existing requirement to consider whether the contravention has caused or is likely to cause damage or distress to the data subject.

Clarifying Power to Direct Remedial Steps in an Enforcement Notice (Proposal (9) in the Consultation Report)

- To specify in the PDPO that, when the remedial actions directed by the PCPD in an enforcement notice to be taken within the specified period include desisting from doing a certain act or engaging in a certain practice, the data user should desist from doing so even after the expiration of the specified period.

Removing the Time Limit to Discontinue an Investigation (Proposal (10) in the Consultation Report)

- To remove the 45-day time limit within which the PCPD has to notify the complainant if the PCPD refuses to continue an investigation.

Additional Grounds for Refusing to Investigate (Proposal (11) in the Consultation Report)

- To include "the primary cause of the complaint is not related to personal data privacy" in section 39(2) of the PDPO as an additional ground for the PCPD to refuse to carry out or continue an investigation.

Relieving the PCPD's Obligation to Notify the Complainant who has Withdrawn his Complaint of Investigation Result
(Proposal (12) in the Consultation Report)

- To remove the obligation of the PCPD to inform the complainant of the PCPD's investigation result and the related matters under section 47(3) of the PDPO where the complainant has withdrawn his complaint.

PCPD to Serve an Enforcement Notice together with the Result of Investigation
(Proposal (13) in the Consultation Report)

- To amend section 47 of the PDPO to allow the PCPD to serve an enforcement notice on the relevant data user at the same time when he notifies the relevant parties of the investigation result.

PCPD to Disclose Information in the Performance of Functions
(Proposal (14) in the Consultation Report)

- To allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of their functions and exercise of their powers.

Immunity for the PCPD and his Prescribed Officers from being Personally Liable to Lawsuit
(Proposal (15) in the Consultation Report)

- To stipulate in the PDPO that the PCPD and his prescribed officers would not be held personally liable for any civil liability for any act done or omission made in good faith in the exercise or purported exercise of the PCPD's functions and powers under the PDPO.

Power to Impose Charges for Educational or Promotional Activities
(Proposal (16) in the Consultation Report)

- To expressly provide the PCPD with power to impose reasonable charges for undertaking educational or promotional activities or services.

Power to Obtain Information to Verify a Data User Return
(Proposal (17) in the Consultation Report)

- To empower the PCPD to obtain information from any person in order to verify the information in a data user return filed under section 14 of the PDPO.

Offence and Sanctions

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

- To make it 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 for which the PCPD had previously issued an enforcement notice.

- The penalty for this offence should be the same as that for breaching an enforcement notice, i.e. liable upon 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 fine of $1,000.

Repeated Non-compliance with Enforcement Notice
(Proposal (19) in the Consultation Report)

- To impose heavier penalty on data users for repeated non-compliance with enforcement notice, i.e. a fine at Level 6 ($100,000) and in the case of a continuing offence, a daily fine of $2,000, while the term of imprisonment would remain at two years, the same as that for first-time non-compliance with enforcement notice.

Rights of Data Subjects

Empowering "Relevant Person" to Give Prescribed Consent to Change of Use of Personal Data
(Proposal (20) in the Consultation Report)

- To empower a "relevant person" to give consent to the change of use of personal data of certain classes of data subjects when it is in their

best interests to do so. "Relevant person" is currently defined as follows and the definition will be expanded under Proposal (36) below :

(a) where the individual is a minor, a person who has parental responsibility for the minor;

(b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs.

Access to Personal Data in Dispute
(Proposal (21) in the Consultation Report)

- To add a provision to prohibit the disclosure of document containing the data in dispute to the data requestor and other parties bound by the decision of the Administrative Appeals Board ("AAB"), the court or magistrate by way of disclosure or otherwise before the AAB, the court or magistrate determines in favour of the applicant.

Rights and Obligations of Data Users

Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation
(Proposal (22) in the Consultation Report)

- To add a provision to the PDPO so that a data user can refuse to comply with a data access request where the data user is obliged or entitled under any other ordinances not to disclose the personal data.

Response to Data Access Requests in Writing and within 40 Days
(Proposal (23) in the Consultation Report)

- To require a data user to inform a requestor in writing in 40 days if he does not hold the requested personal data. As regards the handling of data access requests in respect of criminal conviction records by the Police, if the requestor has a clear record, the Police will be exempted from complying with the requirement to reply in writing, though it will still be required to make a verbal response within 40 days.

Contact Information about the Individual who Receives Data Access or Correction Requests
(Proposal (24) in the Consultation Report)

- To amend DPP 1(3) to permit a data user to provide the job title or the name of the individual to whom data access or correction requests may be made.

Erasure of Personal Data
(Proposal (25) in the Consultation Report)

- To amend the PDPO to the effect that the duty to erase personal data would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase obsolete personal data.

Duty to Prevent Loss of Personal Data
(Proposal (26) in the Consultation Report)

- To amend DPP 4 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.

New Exemptions

Transfer of Personal Data in Business Mergers or Acquisition
(Proposal (27) in the Consultation Report)

- To grant an exemption from DPP 3 for the transfer or disclosure of personal data in merger, acquisition or transfer of businesses subject to certain conditions, with a fine at Level 5 ($50,000) and imprisonment for two years for contravention of the requirements on the retention and restriction on the use of the personal data concerned.

Provision of Identity and Location Data on Health Grounds
(Proposal (28) in the Consultation Report)

- To broaden the scope of application of the exemption under section 59 of the PDPO to cover personal data relating to the identity and location of the data subject on health grounds.

Handling Personal Data in Emergency Situations
(Proposal (29) in the Consultation Report)

- To exempt personal data for the purpose of conducting rescue and relief work from DPP 1(3) and DPP 3 subject to some conditions.

Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship
(Proposal (30) in the Consultation Report)

- To grant an exemption from DPP 3 for personal data of minors under the following conditions :

  (a) the transfer or disclosure of the data to the relevant person of the minor is to facilitate the former to better discharge his responsibility to exercise proper care and guardianship, and is in the best interests of the minor; and

  (b) the data are held by the Police or the Customs and Excise Department and are to be transferred or disclosed by the Police or the Customs and Excise Department to the relevant person of the minor.

Use of Personal Data Required or Authorised by Law or Related to Legal Proceedings
(Proposal (31) in the Consultation Report)

- To create an exemption from DPP 3 for use of personal data required or authorised by or under law, by court orders, or in connection with any legal proceedings in Hong Kong or otherwise for establishing, exercising or defending legal rights.

Transfer of Records for Archival Purpose
(Proposal (32) in the Consultation Report)

- To create an exemption from DPP 3 for the transfer of records of historical, research, educational or cultural interests, which contain personal data, to the Government Records Service for archival purpose.

Refusal to Comply with a Data Access Request on Ground of Self-Incrimination
(Proposal (33) in the Consultation Report)

- To create a new exemption for data users from complying with a data access request on the ground of self-incrimination.

Exemption for Personal Data Held by the Court or Judicial Officer
(Proposal (34) in the Consultation Report)

- To add a new provision to the PDPO so that the PDPO shall not apply to personal data held by the court or judicial officer in the course of the exercise of judicial functions.

Miscellaneous Proposed Amendments

Definition of Crime under Section 58
(Proposal (35) in the Consultation Report)

- To add a definition of "crime" in order to clarify the scope of the application of section 58 of the PDPO, which provides that personal data used for the purposes of the prevention or detection of crime are exempted from DPP 3.

Expanding the Definition of "Relevant Person"
(Proposal (36) in the Consultation Report)

- To expand the definition of "relevant person" under section 2 of the PDPO to include the guardians of data subjects with mental incapacity, who are appointed under sections 44A, 59O or 59Q of the Mental Health Ordinance (Cap. 136), so that they may lodge complaints and make data access and data correction requests on behalf of the data subjects concerned.

Extending the Time Limit for Laying Information for Prosecution
(Proposal (37) in the Consultation Report)

- To extend the time limit for laying information for prosecution of an offence under the PDPO from six months to two years from the date of commission of the offence.

Annex B

Major Proposals Not to be Implemented

Do-not-call ("DNC") Register for Person-to-person Telemarketing Calls ("P2P calls")

During the further public discussions, we have received divergent views on whether a DNC register for P2P calls should be set up. Respondents who oppose consider that consumers already have the right to opt out from telemarketing calls on a company-by-company basis and the economic value of direct marketing activities should not be overlooked. Those who are supportive consider that unsolicited P2P calls bring the same level of nuisance as pre-recorded messages. Some of them consider that the DNC registers administered by the Office of the Telecommunications Authority ("OFTA") under the UEMO should be extended to regulate such calls.

2. Surveys conducted by OFTA in 2008 and 2009 (an industry survey and a public opinion survey) showed that around half of P2P calls did not involve personal data. Any regulation of P2P calls should cover all such calls, including those that do not involve the recipients' personal data, so as to make the regulation more comprehensive and effective, and to avoid confusion or dispute over whether personal data are involved. This goes beyond the ambit of the PDPO. Furthermore, according to the industry survey, 31% of the respondent companies reported success rates of over 10% in selling goods/services through P2P calls. 13% of the respondents of the public opinion survey said that they had gained benefits from P2P calls, for example, lower price or discounts. Establishing a DNC for P2P calls appears disproportionate and not directly relevant to the personal data privacy issue at hand. To enhance the protection for call recipients while still allowing legitimate telemarketing, an industry self-regulation scheme was rolled out in 2010. Industry associations of the finance, insurance, telecommunications service and call centre sectors accounting for most of such calls are supportive of the scheme.

Granting Additional Powers to the PCPD

3. The PCPD has proposed to confer on him the powers to conduct criminal investigations and prosecutions, award compensation to aggrieved data subjects and impose monetary penalty on data users for serious contravention of DPPs, so as to enhance his effectiveness and efficiency in enforcing the PDPO.

We indicated in the consultation report that we did not consider it appropriate to pursue these proposals.

4. Most respondents consider that criminal investigation and prosecution powers should be vested in the Police and the Department of Justice respectively to maintain checks and balances. Granting these powers to the PCPD will also cause confusion over his role and deter data users from seeking help from him to comply with the requirements of the PDPO. Most respondents also share the view of the Law Reform Commission in its "Report on Reform of the Law Relating to the Protection of Personal Data" issued in August 1994 that it was undesirable to vest in a single authority both enforcement and punitive functions. They are, therefore, against the proposals to empower the PCPD to award compensation to aggrieved data subjects and to require data users to pay monetary penalty for serious contravention of DPPs.

5. Considering that it is important to vest criminal investigation and prosecution powers and punitive functions in different organisations to maintain checks and balances, we maintain our stance of not taking forward these proposals.