Legislative Council Panel on Constitutional Affairs

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

Introduction

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

Background

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

Result of Public Consultation

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

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

Proposals to be Taken Forward

(A) Direct Marketing and Related Matters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

not covered in the PICS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) Data Security

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

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

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

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

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

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

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

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

20. The consultation document examined whether a system should be instituted to require data users to notify the PCPD and affected individuals when a breach of data security leads to the leakage or loss of personal data, so as to mitigate the potential damage to affected individuals. The consultation document suggested to start with a voluntary notification system first so that we could assess the impact of breach notifications more precisely and fine-tune the notification requirements to make them more reasonable and practicable, without causing onerous burden on the community.

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

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

(C) Powers of the PCPD

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

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

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

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

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

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

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

(D) New Offences and Sanctions

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

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

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

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

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

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

Proposals not to be Taken Forward

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Way Forward

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

Constitutional and Mainland Affairs Bureau
18 October 2010

Annex

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

October 2010

Contents

		Page
Summary of Proposals		i
Chapter One :	**Introduction**	1
Chapter Two :	**The Public Consultation Exercise**	5
Chapter Three :	**Proposals to be Taken Forward**	
	Direct Marketing and Related Matters	
	(1) Collection and Use of Personal Data in Direct Marketing	7
	(2) Unauthorised Sale of Personal Data by Data User	18
	(3) Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent	21
	(4) Excluding Social Services from the Definition of "Direct Marketing"	27
	Data Security	
	(5) Regulation of Data Processors and Sub-contracting Activities	28
	(6) Personal Data Security Breach Notification	40
	Statutory Powers and Functions of the Privacy Commissioner for Personal Data ("PCPD")	
	(7) Legal Assistance to Data Subjects under Section 66	48
	(8) Circumstances for Issue of an Enforcement Notice	52
	(9) Clarifying Power to Direct Remedial Steps in an Enforcement Notice	54
	(10) Removing the Time Limit to Discontinue an Investigation	56
	(11) Additional Grounds for Refusing to Investigate	57

		Page
(12)	Relieving the PCPD's Obligation to Notify the Complainant who has Withdrawn his Complaint of Investigation Result	61
(13)	PCPD to Serve an Enforcement Notice together with the Result of Investigation	62
(14)	PCPD to Disclose Information in the Performance of Functions	63
(15)	Immunity for the PCPD and his Prescribed Officers from being Personally Liable to Lawsuit	65
(16)	Power to Impose Charges for Educational and Promotional Activities	66
(17)	Power to Obtain Information to Verify a Data User Return	68
Offences and Sanctions		
(18)	Repeated Contravention of a Data Protection Principle on Same Facts	69
(19)	Repeated Non-compliance with Enforcement Notice	74
Rights of Data Subjects		
(20)	Third Party to Give Prescribed Consent to Change of Use of Personal Data	77
(21)	Access to Personal Data in Dispute	81
Rights and Obligations of Data Users		
(22)	Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation	84
(23)	Response to Data Access Requests in Writing and within 40 Days	86
(24)	Contact Information about the Individual who Receives Data Access or Correction Requests	88
(25)	Erasure of Personal Data	89
(26)	Duty to Prevent Loss of Personal Data	90

			Page
		Introducing New Exemptions	
	(27)	Transfer of Personal Data in Business Mergers or Acquisition	91
	(28)	Provision of Identity and Location Data on Health Grounds	94
	(29)	Handling Personal Data in Emergency Situations	96
	(30)	Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship	98
	(31)	Use of Personal Data Required or Authorised by Law or Related to Legal Proceedings	104
	(32)	Transfer of Records for Archival Purpose	105
	(33)	Refusal to Comply with a Data Access Request on Ground of Self-Incrimination	107
	(34)	Exemption for Personal Data Held by the Court or Judicial Officer	108
		Miscellaneous Proposed Amendments	
	(35)	Definition of Crime under Section 58	110
	(36)	Expanding the Definition of "Relevant Person"	112
	(37)	Extending the Time Limit for Laying Information for Prosecution	113
Chapter Four :		**Proposals Not to be Taken Forward**	
		Sensitive Personal Data	
	(38)	Sensitive Personal Data	115
		Statutory Powers and Functions of the PCPD	
	(39)	Granting Criminal Investigation and Prosecution Power to the PCPD	124
	(40)	Empowering the PCPD to Award Compensation to Aggrieved Data Subjects	131

		Page
	Offences and Sanctions	
	(41) Making Contravention of a Data Protection Principle an Offence	133
	(42) Imposing Monetary Penalty on Serious Contravention of Data Protection Principles	137
	Access to Personal Data	
	(43) Parents' Right to Access Personal Data of Minors	140
	(44) Fee Charging for Handling Data Access Requests	146
Chapter Five :	**Conclusion**	151
Annex 1	**An Overview of the Personal Data (Privacy) Ordinance**	153
Annex 2	**Summary of Views Expressed at Public Forums**	157
Annex 3	**List of Organisations Met by the Administration**	163
Annex 4	**Written Submissions** *(not enclosed with this report)*	164
Annex 5	**Proposals Not to be Pursued as Indicated in the Consultation Document**	165

Summary of Proposals

(A) Proposals to be Taken Forward

Direct Marketing and Related Matters

Proposal (1): Collection and Use of Personal Data in Direct Marketing

1. To raise the penalty for contravention of the requirement in section 34(1)(b)(ii) of the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) (i.e. if the data subject requests the data user not to use his/her personal data for direct marketing purposes, the data user shall cease to so use the data) from a fine at Level 3 ($10,000) to a fine of $500,000 and imprisonment for three years.

2. To introduce in the PDPO the following additional specific requirements on data users who intend to use (including transfer) the personal data collected for direct marketing purposes :

   (a) the data user's Personal Information Collection Statement ("PICS") should be reasonably specific about the intended marketing activities (whether by the data user himself/herself or the transferee(s)), the classes of persons to whom the data may be transferred for direct marketing purposes and the kinds of data to be transferred for direct marketing purposes;

   (b) the presentation of the information in (a) above in the data user's PICS should be understandable and reasonably readable by the general public; and

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

3. Non-compliance with any of the requirements in paragraph 2 above

will be subject to the issue of an enforcement notice by the Privacy Commissioner for Personal Data ("PCPD")[Note].

4. The PCPD to revise the guidance note on the collection and use of personal data for direct marketing or replace it with a Code of Practice to provide practical guidance on the new requirements in paragraph 2, and to launch a publicity and public education programme to promote understanding of the new requirements.

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

(a) does not comply with any of the requirements in paragraph 2 and subsequently uses (including "transfers") the personal data for direct marketing purposes; or

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

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

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

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

not covered in the PICS.

Proposal (2) : Unauthorised Sale of Personal Data by Data User

6. To introduce the following requirements and offence:

(a) if a data user is to sell personal data (whether collected from the data subject direct by the data user or obtained from

---

Note As currently provided for under the PDPO, if a data user contravenes a requirement under the PDPO, the PCPD may issue an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he/she commits an offence under section 64(7), and is liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

another source) to another person for a monetary or in kind gain, the data user should, before doing so, inform the data subject in writing of the kinds of personal data to be sold and to whom the personal data will be sold;

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

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

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

7. Non-compliance with any of the requirements in (a) to (c) above will be subject to the issue of an enforcement notice by the PCPD.

8. We welcome public views on the penalty for the offence in (d) above. For reference, section 58(1) of the Unsolicited Electronic Messages Ordinance ("UEMO") (Cap. 593) provides that a person to whom an unsubscribe request is sent shall not use any information obtained thereby other than for the purpose of complying with the relevant requirements (including the requirement to comply with the unsubscribe request). A person who contravenes section 58(1) commits an offence and is liable on summary conviction to a fine at Level 6 ($100,000). A person who knowingly contravenes section 58(1) commits an offence and is liable upon conviction on indictment to a fine of $1,000,000 and imprisonment for five years.

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

9. To make it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent.

10. A possible formulation is to define "malicious purposes" as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another".

11. To set the penalty at the same level as that for the offence proposed paragraph 6(d).

Proposal (4) : Excluding Social Services from the Definition of "Direct Marketing"

12. To amend section 34 of the PDPO to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.

Data Security

Proposal (5) : Regulation of Data Processors and Sub-contracting Activities

13. To require a 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 will be subject to the issue of an enforcement notice by the PCPD.

14. The Office of the Privacy Commissioner for Personal Data, Hong Kong ("Office of the PCPD") to 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.

Proposal (6) : Personal Data Security Breach Notification

15. 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.

16. 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.

Statutory Powers and Functions of the PCPD

Proposal (7) : Legal Assistance to Data Subjects under Section 66

17. 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.

Proposal (8) : Circumstances for Issue of an Enforcement Notice

18. 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.

Proposal (9) : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

19. 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.

Proposal (10) : Removing the Time Limit to Discontinue an Investigation

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

Proposal (11) : Additional Grounds for Refusing to Investigate

21. 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.

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

22. 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.

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

23. 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.

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

24. 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.

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

25. 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.

Proposal (16) : Power to Impose Charges for Educational and Promotional Activities

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

Proposal (17) : Power to Obtain Information to Verify a Data User Return

27. 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.

Offences and Sanctions

Proposal (18) : Repeated Contravention of a Data Protection Principle on Same Facts

28. 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.

29. The penalty should be the same as that for breaching an enforcement notice, i.e. a fine at Level 5 ($50,000) and imprisonment for two years.

Proposal (19) : Repeated Non-compliance with Enforcement Notice

30. 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

Proposal (20) : Third Party to Give Prescribed Consent to Change of Use of Personal Data

31. To empower a specified third party 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. The specified third parties include, where the individual is a minor, a person who has parental responsibility for the minor, and where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs.

Proposal (21) : Access to Personal Data in Dispute

32. 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 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

Proposal (22) : Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

33. 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.

Proposal (23) : Response to Data Access Requests in Writing and within 40 Days

34. 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 exempt from complying with the requirement to reply in writing, though it will still be required to make a verbal response within 40 days.

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

35. To amend Data Protection Principle ("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.

Proposal (25) : Erasure of Personal Data

36. 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.

Proposal (26) : Duty to Prevent Loss of Personal Data

37. 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.

Introducing New Exemptions

Proposal (27) : Transfer of Personal Data in Business Mergers or Acquisition

38. 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. To prevent abuse of the exemption and possible harm to data subjects, we propose to impose 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.

Proposal (28) : Provision of Identity and Location Data on Health Grounds

39. 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.

Proposal (29) : Handling Personal Data in Emergency Situations

40. To exempt the law enforcement agencies ("LEAs"), rescue and relief agencies, and individuals and organisations holding relevant personal data from DPP 1(3) and DPP 3 to:

(a) identify individuals who are or may reasonably be suspected to be involved in an accident or other life-threatening situations;

(b) inform family members of the individuals under (a) of the latter's involvement in the accident, etc; and

(c) generally to facilitate the provision of rescue or relief services to the individuals under (a).

Proposal (30) : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

41. 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 parents or guardians of the minor is to facilitate the latter to better discharge their responsibility to exercise proper care and guardianship, and is in the best interests of the minor; and

(b) the data are held by LEAs and are to be transferred or disclosed by LEAs to the parents or guardians of the minor.

Proposal (31) : Use of Personal Data Required or Authorised by Law or Related to Legal Proceedings

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

Proposal (32) : Transfer of Records for Archival Purpose

43. To create an exemption from DPP 3 for the transfer of records containing personal data of historical, research, educational or

cultural interests to the Government Records Service ("GRS") for archival purpose.

Proposal (33) : Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

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

Proposal (34) : Exemption for Personal Data Held by the Court or Judicial Officer

45. 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

Proposal (35) : Definition of Crime under Section 58

46. 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 exempt from DPP 3.

Proposal (36) : Expanding the Definition of "Relevant Person"

47. 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.

Proposal (37) : Extending the Time Limit for Laying Information for Prosecution

48. 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.

(B) Proposals NOT to be Taken Forward

Sensitive Personal Data

Proposal (38) : Sensitive Personal Data

49. Not to pursue the proposal to subject sensitive personal data (particularly biometric data) to more stringent regulation such as prohibiting the collection, holding, processing and use of such data except under specific circumstances.

50. Instead, we propose 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 in general, such as biometric data and health record; and

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

Statutory Powers and Functions of the PCPD

Proposal (39) : Granting Criminal Investigation and Prosecution Power to the PCPD

51. Not to pursue the proposal to confer the PCPD with the power to carry out criminal investigations and prosecutions. We consider it important to retain the existing arrangement, under which the Police conducts criminal investigation and Department of Justice undertakes prosecution, in order to maintain checks and balances.

Proposal (40) : Empowering the PCPD to Award Compensation to Aggrieved Data Subjects

52. Not to pursue the proposal to empower the PCPD to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user. We do not consider it desirable to vest in a single authority both enforcement and punitive functions. The data

subjects concerned can seek compensation through the court as provided for under section 66 of the PDPO.

Offences and Sanctions

Proposal (41) : Making Contravention of a Data Protection Principle an Offence

53. Not to pursue the proposal to make contravention of a DPP an offence.

Proposal (42) : Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

54. Not to pursue the proposal to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs. We consider that it would be more appropriate to make serious contravention a criminal offence.

Access to Personal Data

Proposal (43) : Parents' Right to Access Personal Data of Minors

55. Not to pursue the proposal 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 the minor) on behalf of a minor in order to protect the interests of minors.

Proposal (44) : Fee Charging for Handling Data Access Requests

56. Not to pursue the proposal that, for the purpose of imposition of a fee for complying with a data access request, a fee schedule should be provided in the PDPO and a data user should be required not to charge fees in excess of the prescribed maximum as set out in the said fee schedule.

Others

57. Not to pursue the proposals in Annex 2 to the consultation document on the Review of the Personal Data (Privacy) Ordinance ("the consultation document"), which we had indicated in the consultation document our intention not to pursue.

Chapter One: Introduction

1.1 The PDPO has been in force since 1996 (an overview of the PDPO is at Annex 1). Over the last decade or so, we have witnessed continuous developments in society, in particular, the rapid advancement in information technology, prevalence of the Internet and exponential growth of e-commerce. Increasing use of information and communications technology has helped enhance Hong Kong's competitiveness and efficiency, and brought more convenient and user-friendly services to the community. At the same time, the social development and technological advancement have brought new challenges to the protection of personal data privacy. The community's concern about personal data privacy protection has also been increasing.

1.2 Against this background, the Constitutional and Mainland Affairs Bureau ("CMAB"), with the support of the PCPD, has conducted a comprehensive review of the PDPO, to examine whether the existing provisions of the PDPO still afford adequate protection to personal data, in what aspects the regulation and protection of personal data should be tightened, and how to streamline the operation of the PDPO and address technical problems encountered in the implementation of the PDPO.

1.3 In conducting the review, we were guided by the following:

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

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

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

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

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

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

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

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

Public Consultation

1.4 After reviewing the PDPO, we formulated a series of proposals and issued the consultation document on 28 August 2009 to invite views from the public on the proposals. The consultation period ended on 30 November 2009.

1.5 This report sets out the views on the proposals submitted by the public and the Government's proposed way forward having regard to the public views. Chapter Two of this report gives a brief account of the public consultation exercise. Chapters Three and Four respectively outline the proposals that the Government, having considered the public views received, intends to take forward and those that the Government intends not to pursue. Chapter Five summarises various proposals and the proposed way forward.

Next Step

1.6 With a view to soliciting the views of members of the public extensively, the Government adopted an open mind and did not present a considered position for most of the proposals in the consultation document. In the light of the views received and other considerations, we have mapped out the proposals to be taken forward and those not to be taken forward.

1.7 Separately, the community has recently expressed concerns about the transfer of customer personal data by some enterprises for direct marketing purposes without explicitly and specifically informing the customers of the purpose of the transfer and the identity of the transferees. We have examined these concerns carefully and put forward in the consultation report some new

proposals to strengthen protection of personal data privacy in this regard.

1.8 We welcome public views on the specific arrangements and details of the proposals to be taken forward. In addition, we shall arrange to meet with relevant organisations or stakeholders for in-depth discussions on the details, including the content of the legislative amendments, of the proposals to be taken forward, so as to ensure smooth operation of the amended PDPO.

1.9 If you would like to comment on the specific arrangements or details of the proposals to be taken forward, or raise any other comments, please submit them by mail, facsimile or e-mail on or before 31 December 2010:

Address: Team 4
Constitutional and Mainland Affairs Bureau
Room 364, East Wing
Central Government Offices
Lower Albert Road
Hong Kong

Fax number: 2523 0565

E-mail address: pdpo_consultation@cmab.gov.hk

1.10 It is voluntary for members of the public to supply their personal data upon providing views. The submissions and personal data collected may be transferred to the relevant Government bureaux and departments or the Office of the PCPD for purposes directly related to this views collection exercise. The Government bureaux and departments, and the Office of the PCPD receiving the data may only use the data for such purposes.

1.11 The names and views of individuals and organisations who/which put forth submissions ("senders") may be published for public inspection or cited. We will respect the wish of senders to remain anonymous and/or keep their views confidential in part or in whole; but if no such wish is indicated, it will be assumed that the sender can be named and the views can be published in full.

1.12 Any sender providing personal data to the CMAB in the submission will have the right of access and correction with respect to such personal data. Any requests for data access or correction of personal data should be made in writing through the channels mentioned in paragraph 1.9 above.

Chapter Two: The Public Consultation Exercise

2.1 The CMAB issued the consultation document on 28 August 2009. Subsequently, we placed newspaper advertisements, arranged broadcast of Announcements in the Public Interest on the television and radio, and gave media interviews to publicise the consultation exercise.

2.2 Members of the public could obtain a copy of the consultation document from the Public Enquiry Service Centres of the District Offices under the Home Affairs Department, or download it from the CMAB website. Copies of the consultation document were also sent to sectors and major organisations interested in the review of the PDPO.

2.3 During the public consultation period, we consulted the community extensively through different channels to gauge feedback from the Legislative Council ("LegCo"), District Councils ("DCs"), organisations and individuals of different sectors, and the general public.

2.4 To encourage discussions in various sectors of the community, we consulted the Panel on Constitutional Affairs of LegCo on 11 September 2009. We also held two public forums at the Youth Square in Chai Wan and the Tsuen Wan Town Hall on 18 September and 30 October 2009 respectively for members of the public to participate and express their views. The summaries of views expressed by the participants at the two forums are at Annex 2.

2.5 In order to gauge the views of the local community, we organised two DC forums at the Leighton Hill Community Hall and the Sha Tin Town Hall on 8 October and 13 October 2009 respectively. All DC members were invited.

2.6 Over 200 people attended the four consultation sessions mentioned above. They included members and co-opted members of DCs; members of area committees, rural committees, mutual aid committees and the Public Affairs Forum; students; professionals and representatives of other organisations.

2.7 We also met with representatives of sectors and organisations interested in the review of the PDPO and took part in forums and seminars organised by them to listen to their views. The organisers of these consultation activities are listed at Annex 3.

2.8 During the consultation period, we encouraged the community to put forward their views, via mail, facsimile or e-mail, on the proposals set out in the consultation document, and a total of 161 written submissions were received. After the end of the consultation period, the CMAB further received 17 submissions. Save those kept confidential at the request of the submitting parties, the submissions are all reproduced at Annex 4. Annex 4 can be viewed at the Public Enquiry Service Centres of the District Offices under the Home Affairs Department or the CMAB website.

Chapter Three: Proposals to be Taken Forward

3.1.1 The views expressed by the public through various channels show that many of the proposals put forward in the consultation document are supported by the general public. We consider that these proposals should be taken forward. This chapter sets out in detail the analyses of views on these proposals and our proposed way forward.

Direct Marketing and Related Matters

(1) Collection and Use of Personal Data in Direct Marketing (Proposal No. 12 and Item A.1 in Annex 2 to the Consultation Document)

Proposals in the Consultation Document

3.2.1 The consultation document examined whether:

(a) the penalty for misuse of personal data in direct marketing under section 34(1)(b)(ii) of the PDPO should be raised (Proposal No. 12 in the consultation document);

(b) section 34 of the PDPO should be amended to the effect that, before a data user uses personal data obtained from any source for direct marketing purposes, the data user should obtain the explicit consent of the data subject to so use the personal data, i.e. the "opt-in" proposal (item A.1 in Annex 2 to the consultation document); and

(c) a territory-wide central do-not-call register against direct marketing activities should be set up (item A.1 in Annex 2 to the consultation document).

3.2.2 Section 34 of the PDPO stipulates that if a data user uses personal data obtained from any source for direct marketing purposes, he/she must, the first time he/she so uses the personal data, inform the data subject that the data user is required to cease to so use the data if the data subject so requests. Section 34(1)(b)(ii) provides that, if the data subject requests the data user not to use his/her personal data for direct marketing

purposes, the data user shall cease to so use the data. A data user who, without reasonable excuse, contravenes this requirement commits an offence and is liable on conviction to a fine at Level 3 ($10,000) under section 64(10).

Proposal (a)

3.2.3 The consultation document mentioned a case brought before the court concerning the making of direct marketing calls by a telecommunications company, where the Magistrate remarked that the penalties under the PDPO could hardly act as an effective deterrent for large companies. To curb misuse of personal data in direct marketing activities more effectively, the consultation document proposed that we consider raising the penalty level for contravention of section 34(1)(b)(ii) of the PDPO.

Proposals (b) and (c)

3.2.4 The consultation document pointed out that section 34 of the PDPO already regulated the use of personal data in direct marketing. To guard against misuse of personal data in direct marketing, we have put forth the proposal to raise the penalty level for contravention of the requirement under section 34(1)(b)(ii).

3.2.5 Besides, direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the UEMO. The Administration will consider the possibility of regulating person-to-person telemarketing calls if the problem grows in future.

3.2.6 In view of the above, the consultation document did not consider it appropriate to make further amendments to section 34 of the PDPO.

Views Received

Proposal (a)

3.2.7 Of the submissions received, close to 40% expressed views on proposal (a). More than half of them supported the implementation of the proposal while some raised objection.

Some did not make a clear indication of preference. During the consultation activities, some participants expressed their views on this proposal.

3.2.8 Respondents who support the implementation of this proposal agree that raising the penalty level can be an effective deterrent, curbing the misuse of personal data in direct marketing activities[1].

3.2.9 A respondent considers that the penalty should be raised to a level higher than the incentive to misuse personal data in direct marketing activities[2]. Some respondents propose to increase the fine from the current $10,000 to $50,000[3]. There are also respondents who consider that the penalty should be revised to an even higher level[4].

3.2.10 Respondents who oppose the raising of the penalty level mainly hold the following views:

- there have not been many such complaint cases in the past, and raising the penalty level should not be very effective in curbing such acts[5];

- although direct marketing may infringe the personal data privacy of the data subject, it causes him/her little material damage. It may not be proportional to impose heavy punishment on such acts[6]; and

---

1 Please refer to S0040, S0060, S0074, S0092, S0097, S0121, S0132, S0134, S0135, S0151, S0165, S0166, S0168 and S0173 of Annex 4.

2 Please refer to S0087 of Annex 4.

3 Please refer to S0067, S0083, S0122, S0145 and S0148 of Annex 4.

4 For example, the Law Society of Hong Kong (S0073) suggests a fine at Level 6 ($100,000) while the Hong Kong Medical Association (S0162) suggests that imprisonment terms should be considered. Please also refer to S0015, S0102 and S0140 of Annex 4.

5 Please refer to S0033, S0052 and S0072 of Annex 4. Moreover, Yahoo! Hong Kong Limited (S0123) considers that the current level of punishment already provides sufficient deterrent and does not see the necessity to raise the level of punishment.

6 Please refer to S0072, S0119 and S0152 of Annex 4.

- this proposal will increase the operation risk of legitimate direct marketing activities which will in turn increase the burden on commercial operations and undermine economic activities[7].

3.2.11 A respondent suggests that the Administration should step up publicity so that the general public are aware that the present legislation has already given them power to request the data users to stop using their personal data in direct marketing[8].

Proposals (b) and (c)

3.2.12 Of the submissions received, less than 10% expressed views on proposals (b) and (c). While some of them supported the Administration's stance of not pursuing the proposals, some considered that the Administration should implement them. In other public consultation activities, some participants pointed out that direct marketing activities caused nuisances to everyday life and opined that the Government should explore ways to strengthen regulation of these activities.

3.2.13 Among the views supporting the Administration's stance of not pursuing this proposal[9], some point out that proposal (b), i.e. the "opt-in" proposal, will add burden to the operations of enterprises carrying out direct marketing activities. Also, the implementation of the "opt-in" proposal will conflict with the "unsubscribe" regime[10] currently adopted under the UEMO to regulate direct marketing activities in the form of electronic communications and may lead to unnecessary confusion. As regards proposal (c), i.e. setting up a territory-wide do-not-call register, since the Office of the Telecommunications Authority has established do-not-call registers for the purposes of the UEMO, another do-not-call register under the PDPO will be difficult to administer and enforce, and may lead to confusion.

---

7 Please refer to S0123, S0124 and S0177 of Annex 4.

8 Please refer to S0157 of Annex 4.

9 Please refer to S0048, S0049, S0052, S0080, S0101 and S0124 of Annex 4.

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

Any introduction of further do-not-call registers should be considered in the context of the UEMO[11].

3.2.14 There are, on the other hand, views opining that the Administration should take forward the "opt-in" proposal in view of the nuisances caused by direct marketing activities[12]. In addition, the Office of the PCPD suggests that the advantage of the "opt-in" regime lies in the need for explicit consent from a data subject for the use of personal data and this requirement is in alignment with the "prescribed consent" under the use limitation principle expounded under DPP 3 [13]. Some participants of the public consultation activities opine that organisations should not take it as consent to use the personal data for direct marketing purposes when a data subject does not express objection. There are also respondents who opine that data subjects should be given the right to request the data user to disclose the source from which it has collected the personal data for carrying out direct marketing activities as a further step to enhance protection[14].

Proposed Way Forward

Proposal (a)

3.2.15 Of the submissions that expressed views on proposal (a), more than half support the implementation of this proposal. Direct marketing activities may be annoying and may intrude into the

---

11 Please refer to S0124 of Annex 4. Baker & Mckenzie (S0124) considers that any do-not-call register should be with respect to a specific means of communication, like those currently set up under the UEMO. Also, splitting the administration of do-not-call registers between regulatory authorities may lead to confusion for both data subjects and data users.

12 Please refer to S0058, S0117, S0126, S0157 and S0178 of Annex 4.

13 The rationale behind the PCPD's comment on the "opt-in" approach is that in many cases, data users obtained personal data from another source and they do not have pre-existing customer relationships with the data subjects. However, on the Office of the PCPD's suggestion, it should be noted that DPP 3 concerns change in the use of personal data, i.e. the data subject's prescribed consent is required only if his/her personal data are to be used for a purpose other than the purpose for which the data were to be used at the time of collection of the data or a directly related purpose. If direct marketing is among the original purposes or directly related purposes, there is no need for the data user to seek the data subject's prescribed consent. A data subject who wishes the data user to cease to so use his/her personal data may request the data user to act accordingly under section 34 of the PDPO.

14 Please refer to S0097, S0157 and S0178 of Annex 4.

privacy of individuals. The respondents generally agree that there is a need to raise the level of penalty to more effectively curb the misuse of personal data in direct marketing activities. Therefore, we intend to implement this proposal.

3.2.16 In deciding the appropriate level of penalty on the misuse of personal data in direct marketing activities, considerations include whether the penalty can act as an effective deterrent, whether direct marketing activities bring serious damage to data subjects and how the penalty level would impact on economic activities.

3.2.17 For reference, 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 request. A person who contravenes section 58(1) commits an offence and is liable on summary conviction to a fine at Level 6 ($100,000). A person who knowingly contravenes section 58(1) commits an offence and is liable upon conviction on indictment to a fine of $1,000,000 and imprisonment for five years.

3.2.18 Having regard to the public comments received and the relevant considerations, one possible option is to raise the penalty for contravention of section 34(1)(b)(ii) of the PDPO to a fine of $500,000 and imprisonment for three years.

Proposals (b) and (c)

3.2.19 There are different views on whether to pursue proposals (b) and (c). As pointed out by some respondents, proposal (b) (the "opt-in" proposal) will add burden to the operations of enterprises carrying out direct marketing activities. As regards proposal (c) (setting up a central do-not-call register), it should be noted that the purpose of the PDPO is to protect personal data privacy. Regulation of direct marketing activities goes beyond the protection of personal data privacy. Direct marketing activities in the form of electronic communications are currently regulated by the UEMO. As regards person-to-person telemarketing calls, according to two surveys conducted by the Office of the Telecommunications Authority in 2008 and 2009, around half of these calls did not involve the

recipients' personal data[15]. If measures are to be introduced to address the problem of inconvenience caused by person-to-person telemarketing calls, they should cover all such calls so as to avoid confusion and dispute over whether the use of personal data is involved. This goes beyond the protection of personal data privacy and the ambit of the PDPO. The Administration is monitoring person-to-person direct marketing activities. If the problem grows in the future, the Administration will consider the possibility of regulating such activities.

3.2.20 In the light of the above, we are inclined to maintain the stance in the consultation document that it is not appropriate to pursue the "opt-in" proposal or introduce a territory-wide do-not-call register against direct marketing activities. Instead, we propose to raise the penalty for contravention of the direct marketing provision in section 34(1)(b)(ii) of the PDPO (as set out in paragraph 3.2.18 above). We also propose to introduce additional requirements on data users in the collection and use of personal data for direct marketing purposes in order to enhance protection to data subjects. They are elaborated in paragraphs 3.2.21 to 3.2.35 below.

Collection and use of personal data for direct marketing purposes

3.2.21 We are fully aware of the community concerns about the collection and use of personal data for direct marketing purposes following the recent cases of transfer of massive customer personal data by 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 customers' consent.

3.2.22 Currently, under the PDPO, DPP 1(1) provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. Only personal data that are necessary for or directly related to the purpose should be collected, and the data collected should be adequate but not excessive for that purpose. DPP 1(2) provides that personal

---

[15] Please refer to the paper entitled "Person-to-Person Telemarketing Calls" (LC Paper No. CB(1)240/09-10(04)) for discussion at the meeting of LegCo Panel on Information Technology and Broadcasting on 9 November 2009.

data shall be collected by means which are lawful and fair in the circumstances of the case.

3.2.23 DPP 1(3) stipulates that a data user should take all practicable steps to ensure that the data subject is explicitly informed, on or before collecting the data, of the purpose (in general or specific terms) for which the data are to be used, and the classes of persons to whom the data may be transferred. DPP 3 stipulates that, without the prescribed consent of the data subject, personal data shall not be used for any purpose other than the purposes for which the data were to be used at the time of collection or a directly related purpose.

3.2.24 Contravention of a DPP by itself is not an offence under the PDPO. Instead, the PCPD is empowered to remedy the breach by issuing an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he/she commits an offence under section 64(7), and is liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

3.2.25 The PCPD has investigated some of the cases mentioned in paragraph 3.2.21. The PCPD's investigations, the public disclosures/statements made by some of the concerned enterprises and media reports on this subject have revealed some business practices on collection and transfer of personal data, over which different quarters of the community have called for strengthened regulation.

3.2.26 When subscribing for a service, an applicant (the data subject) is very often required to provide his/her personal data and sign a contract or subscription form containing provisions on, among other things, the purposes for which the personal data collected are to be used, including transfer[16] of the personal data by the service provider (the data user). In some cases, the purposes and the classes of persons to whom the data may be transferred are not stated in reasonably specific terms. A data subject's consent to such provisions may give the data user wide discretion in the use or transfer of the personal data, without the data subject being aware of the exact use or the identity of the

[16] Under the PDPO, the meaning of "use" in relation to personal data includes "transfer".

transferees.

3.2.27 A commonly cited reason for data subjects giving consent to such generally described purposes or classes of transferees is that the concerned provisions are in very small print. In such circumstances, the data subject may sign a contract or subscription form without noticing that the latter contains a statement seeking or deeming his/her consent to use his/her personal data for particular purposes or to transfer the data to certain classes of persons.

3.2.28 Another common business practice is that the contract or subscription form is designed in such a way to seek the applicant's bundled consent to the terms and conditions of the service, the purposes for which the personal data collected are to be used, and the classes of persons to whom the personal data may be transferred. In such cases, even if the applicant would have preferred not to give consent to some of the purposes for which his/her personal data are to be used or some of the classes of persons to whom his/her personal data may be transferred, he/she would have no choice but to give bundled consent in order to obtain the service.

3.2.29 As explained in paragraphs 3.2.22 to 3.2.24 above, the current PDPO already contains provisions regulating the collection and use of personal data through DPP 1 and 3. Section 34 of the PDPO also imposes requirements on the data user in direct marketing. The existing control regime applies to both data users who collect personal data from data subjects and transfer the personal data to others as well as data users who obtain personal data from other sources for direct marketing. However, the business practices mentioned above have given rise to concerns that the requirements in the existing legislation are too general and not specific enough to afford adequate protection to personal data privacy.

3.2.30 To address these concerns, the PCPD will shortly issue a new guidance note on the collection and use of personal data for direct marketing, replacing the existing Guidance Note on "Cross Marketing Activities" and Fact Sheet on "Guidelines on Cold-Calling". The new guidance note will provide practical guidelines to assist practitioners to comply with the provisions of the PDPO. It will also draw their attention to recommended

practices in personal data privacy protection.

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

3.2.32 DPP 1(3) already provides that a data user should, on or before collecting personal data, explicitly inform the data subject of the purpose (in general or specific terms) for which the personal data collected are to be used and the classes of persons to whom the data may be transferred. To enhance the protection for data subjects and facilitate their understanding of the relevant contractual provisions before giving consent, we propose to introduce in the PDPO the following additional specific requirements on data users who intend to use (including transfer) the personal data collected for direct marketing purposes :

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

(b) the presentation of the part of the data user's PICS on the intended direct marketing activities (whether by the data

user himself/herself or the transferee(s)), the classes of persons to whom the data may be transferred for direct marketing purposes and the kinds of data to be transferred for direct marketing purposes should be understandable and reasonably readable by the general public; and

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

3.2.33 We propose that non-compliance with any of the new requirements in paragraph 3.2.32 above will be subject to the issue of an enforcement notice by the PCPD. Failure to comply with the enforcement notice will be an offence, as currently provided for under the PDPO.

3.2.34 As mentioned in paragraph 3.2.30 above, the PCPD will shortly issue a new guidance note on the collection and use of personal data for direct marketing activities. We propose that, to tie in with the entry into force of the new requirements mentioned in paragraph 3.2.32 above, the PCPD should take into account the new requirements and revise the guidance note or replace it with a Code of Practice to provide practical guidance on the new requirements. The PCPD will consult the relevant stakeholders as appropriate in the preparation of the revised guidance note or Code of Practice. The PCPD will also launch a publicity and public education programme to promote understanding of the new requirements by both data users and data subjects, and assist data users in complying with the new requirements.

3.2.35 We also propose that, after the entry into force of the requirements in paragraph 3.2.32 above, a data user commits an offence and is liable on conviction to a fine of $500,000 and imprisonment for three years if he/she:

(a) does not comply with any of the requirements and subsequently uses (including transfers) the personal data

for direct marketing purposes; or

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

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

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

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

not covered in the PICS.

(2) Unauthorised Sale of Personal Data by Data User

Problem

3.3.1 Paragraph 3.2.21 above mentioned a series of incidents of transfer of customer personal data by enterprises for direct marketing purposes. Some of them involved monetary gains, arousing widespread concerns in the community. There have been calls for more stringent regulation in this regard and criminalising the sale of personal data by data users.

Current Regulatory Regime

3.3.2 At present, the use (which includes transfer) of personal data is regulated by DPP 3 which provides that, without the prescribed consent of the data subject, personal data shall not be used for any purpose other than the purposes for which the data were to be used at the time of collection or a directly related purpose.

3.3.3 The PDPO does not prohibit the sale of personal data *per se*. If a data user uses personal data for a purpose (e.g. sale) which is not the purpose for which the data were collected or a directly related purpose, he/she contravenes DPP 3 unless the relevant prescribed consent is obtained. Contravention of a DPP by itself is not an offence. Instead, the PCPD is empowered to

remedy the breach by issuing an enforcement notice to direct the data user to take specified remedial steps within a specified period. Failure to comply with the enforcement notice will be an offence and the penalty is a fine at Level 5 ($50,000) and imprisonment for two years.

Proposal

3.3.4 We note the concerns of the community over the sale of personal data by data users and the calls for criminalising such acts. There are, however, views that the resulting damage does not warrant outright criminalisation of such acts. We have also researched into the legislation of some overseas jurisdictions, such as the United Kingdom ("UK"), Australia and New Zealand. The personal data protection laws of these jurisdictions do not prohibit or criminalise the sale of personal data by data users. On the other hand, some consider that data users should be allowed to sell personal data if the data subjects consent to the sale for various reasons (such as there being something in return for them).

3.3.5 Having taken into account public views and the relevant considerations, one possible option is set out below:

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

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

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

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

3.3.6 On paragraph 3.3.5(c) above, the merit of the opt-in model is that the explicit consent of the data subject has to be sought, while the opt-out model is in line with that currently adopted under section 34 of the PDPO regarding the use of personal data in direct marketing and that under the proposal in paragraph 3.2.32 above. We welcome public views on which model to prescribe, or other approaches such as allowing flexibility for individual data users to adopt an appropriate model.

3.3.7 We propose that non-compliance with any of the requirements in paragraph 3.3.5(a) to (c) above will be subject to issue of an enforcement notice by the PCPD.

3.3.8 As regards the penalty for the offence in paragraph 3.3.5(d) above, we welcome public views. For reference, section 58(1) of the UEMO provides that a person to whom an unsubscribe request is sent shall not use any information obtained thereby other than for the purpose of complying with the relevant requirements (including the requirement to comply with the unsubscribe request). A person who contravenes section 58(1) commits an offence and is liable on summary conviction to a fine at Level 6 ($100,000). A person who knowingly contravenes section 58(1) commits an offence and is liable upon conviction on indictment to a fine of $1,000,000 and imprisonment for five years.

3.3.9 Hong Kong will be in the forefront if we are to criminalise the sale of personal data by data users without the consent of the data subjects. Before taking a view on the matter, we would welcome public views, including whether and if so, what exemptions and / or defences should be provided.

3.3.10 The above proposed requirements for data users, if implemented, should be applicable to all data users, including enterprises and individual persons, regardless of the amount of personal data held. Following the recent series of data transfer by enterprises, there are calls for higher standards for companies in possession of pan-community personal data. First, it is difficult to define what constitutes pan-community personal data. The amount of personal data held by a company may also change from time to time. Second, it would lead to confusion for both data users and the general public if we

categorize data users according to the amount of personal data they handle and set different standards of requirement for them. Therefore, we consider that any new requirements proposed should be applicable to all data users.

3.3.11 As for the buyers of the personal data, since they will hold the personal data, they will become data users and be bound by the current provisions of and any new requirements in the PDPO on the collection, holding, processing or use of the personal data and liable to the applicable sanctions if they contravene the requirements. In particular, if they subsequently sell the personal data to another person, they will also be subject to the same proposed requirements as set out in paragraph 3.3.5 above.

(3) Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent (Proposal No. 8 in the Consultation Document)

Proposal in the Consultation Document

3.4.1 The proposal examines whether we should make it an offence for a person (e.g. an employee of a data user) who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent[17]; and if so, whether there is a need for defence provisions and the appropriate level of penalty.

3.4.2 At present, use of personal data is regulated by DPP 3, which provides that unless the data subject gives prescribed consent, personal data should be used for the purposes for which they were collected or for a directly related purpose. Contravention of a DPP *per se* is not an offence. In view of the seriousness of the intrusion into personal data privacy and the gravity of harm that may be caused to the data subjects as a result of the acts mentioned in paragraph 3.4.1 above, the consultation document proposed that consideration should be given to whether such blatant acts should be subject to criminal sanction.

---

[17] Examples include (a) obtaining customers' personal data by an employee of a company without the consent of the company for sale to third parties; and (b) obtaining a patient's sensitive health records by hospital staff without the consent of the hospital for disclosure to third parties.

3.4.3 On defence provisions for the proposed offence, the consultation document referred to the UK Data Protection Act, which provides that : (a) a person must not knowingly or recklessly, without the consent of the data controller (i) obtain or disclose personal data or the information contained in personal data, or (ii) procure the disclosure to another person of the information contained in personal data; (b) a person who sells personal data is guilty of an offence if he has obtained the data in contravention of (a). The Act provides for various defences to such act of obtaining, disclosing or procuring disclosure if:

(a) it was necessary for preventing or detecting crime;

(b) it 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 such disclosure;

(e) in the particular circumstances the obtaining, disclosing or procuring such disclosure was justified as being in the public interest;

(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.

3.4.4 As for penalty for the proposed offence, it is proposed in the consultation document that for the purpose of achieving deterrent effect, consideration may be given to imposing on the offender a fine commensurate with the gravity of the misdeed. By way of reference, the highest level of penalty currently imposed under the PDPO is a fine at Level 5 ($50,000) and imprisonment for two years.

Views Received

3.4.5 Half of the submissions received commented on this proposal. Of them, the majority supported the proposal, a small proportion objected to the proposal, and the rest indicated that they had no comment. In the various consultation activities, some participants voiced opinions on this proposal.

3.4.6 Those who are supportive of this proposal agree with the rationale given in the consultation document[18], reckoning that the proposal could strengthen the deterrent and regulatory effects of the PDPO[19]. A respondent considers that the proposed restrictive regulation will not interfere with the normal and innocuous browsing activities of web-users[20].

3.4.7 Separately, on the scope of regulation, some respondents stress that the proposal should only target those acts which are for profits or malicious purposes[21]. Some respondents consider that the definition of "for malicious purposes" is too broad and vague, and suggest that the proposed offence should be amended to cover only those acts which are "for profits"[22]. On the other hand, some respondents consider that the scope of the proposed offence, which would only cover acts "for profits" or "for malicious purposes", may be too narrow, and suggest that reference should instead be made to the wording of the UK Data Protection Act[23].

---

18 Please refer to S0062, S0067, S0087, S0132, S0177 and S0180 of Annex 4.

19 Please refer to S0015, S0055, S0145 and S0154 of Annex 4.

20 The Office of the PCPD (S0097) disagrees with the view that the proposal may interfere with the normal and innocuous browsing activities of web-users. A person who downloads personal data from the Internet may have a defence if he had the reasonable belief that he has the lawful right to obtain the personal data or that the data user would have consented to the obtaining. Only those who act "knowingly or recklessly" will be affected by the offence.

21 Please refer to S0068 and S0131 of Annex 4.

22 Please refer to S0048, S0049, S0101, S0126 and S0157 of Annex 4.

23 For example, Baker & McKenzie (S0124) proposes that the wording of the offence should be more closely based on the UK offence, in particular that it should be an offence to knowingly or recklessly disclose. The Office of the PCPD (S0097) states that in a court case that concerns a Taxation Officer who recorded the particulars (names, identity card numbers, business registration numbers, addresses and telephone numbers) of 13,400 taxpayers for his future personal use, there was no evidence to prove that the collection of the personal data had brought the Taxation Officer any financial gain. The Office of the PCPD opines that such act, though serious in nature, will not be caught by the proposed new offence which is restricted to obtaining the data for "profits" or "malicious purpose".

3.4.8 As regards defences, there are views that the defences under the UK legislation, as set out in paragraph 3.4.3 above, are suitable for reference by Hong Kong[24]. Some respondents express the view that the defence provisions should exempt all acts which are not in violation of the spirit of personal data protection as enshrined in the PDPO[25]. Some suggest that the exemptions mentioned in (e) and (f) of paragraph 3.4.3 above, which involve public interest, should be considered carefully to see whether they should similarly be applicable in the Hong Kong context[26].

3.4.9 Only a few respondents express their views regarding penalty. One suggests that the proposed fine should be double, or even triple that of the maximum fine currently under the PDPO so as to achieve deterrent effect[27]. Some propose that the penalty should not be lower than that for contravention of enforcement notice, i.e. a fine of $50,000 and imprisonment for two years[28]. Another suggests that reference could be made to the penalties provided in similar legislation overseas[29].

3.4.10 Those objecting to this proposal mainly hold the view that the existing regulation is adequate, noting that the present situation of wilful leakage of personal data is not so serious as to warrant the introduction of a new criminal offence[30]. Some respondents consider it more appropriate to deal with the act of disclosing personal data for profits under other laws than under

---

24 Please refer to S0048, S0049, S0132, S0145, S0155, S0157 and S0162 of Annex 4.

25 Please refer to S0056 of Annex 4. In addition, the Hong Kong Association of Banks (S0068) and Hong Kong General Chamber of Commerce (S0119) propose that a defence should be available to those data users who had taken reasonable steps to prevent their employees from committing the offence.

26 Please refer to S0021 and S0113 of Annex 4.

27 Please refer to S0148 of Annex 4.

28 Please refer to S0162 of Annex 4. In addition, Baker & McKenzie supports the proposal of imposing on the offender a fine commensurate with the gravity of the misdeed, and suggests that the penalty should be left to the discretion of the magistrate, having regard to all relevant factors. Please refer to S0124 of Annex 4 for details.

29 Please refer to S0137 of Annex 4.

30 Please refer to S0080, S0126, S0152 and S0156 of Annex 4.

the privacy legislation[31], while some express worries that the proposal may impose burdens on ordinary Internet users.

3.4.11 A respondent queries why the Administration does not consider imposing civil liabilities, instead of criminal liabilities. The consideration is that civil remedies, including the issue of an injunction order, could help prevent further dissemination of personal data. In addition, through civil proceedings, a data subject could claim damages or even request the party who has gained profits from disclosing the information to hand in the profit[32].

3.4.12 Respondents, whether they support or object to this proposal, consider that terms such as "malicious purposes" should be clearly defined so that members of the public would not commit the offence inadvertently[33], if the proposal is to be put into force.

Proposed Way Forward

3.4.13 The public generally agree that it is necessary to tighten the regulation of the irresponsible act of disclosing personal data

---

31 For example, both the Federation of Hong Kong Industries (S0122) and the Internet Professional Association (S0148) suggest that unlawful disclosure or sale of personal data should be treated as a commercial crime and be dealt with by the Police. In addition, the Hong Kong Information Technology Federation (S0138) reckons that such acts should be dealt with under the laws concerning computer crimes.

32 Please refer to the following extract of the minutes of special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009: "Mr Ronny TONG was of the view that PDPO should be reviewed and overhauled given its deficiencies as reflected in a series of personal data leakage cases in the past few years. He, however, queried the effectiveness of Proposal No. 8 and enquired why the Administration had not considered imposing civil liabilities, instead of criminal liabilities, on persons leaking personal data. He said that civil remedies included, among others, the issue of an injunction order which would help prevent further dissemination of personal data. Through civil proceedings, a data subject could claim damages or even obtain an account of profit from the data user who had disclosed personal data for profits purposes."

33 The Hong Kong Association of Banks (S0068) considers that the legislation should clearly define the acts which would constitute a criminal offence and inadvertent acts should be excluded. Given the ambiguity of the term, the Democratic Party (S0178) suggests that the Administration should carefully study the implementation of relevant legislation in overseas jurisdictions before deciding whether to adopt the concept of "malicious purpose". Please also refer to S0056, S0092, S0122, S0148 and S0157 of Annex 4, and the following extract of the minutes of special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009: "Mr IP Kwok-him enquired about the definition of "malicious" purposes and expressed concern that members of the public may be trapped to commit the offence inadvertently if the definition was not clear. He said that the proposal should strike a balance between personal data protection and the right to access information as well as freedom of expression."

obtained without the consent of the data user for profits or malicious purposes. In view of the seriousness of the intrusion into personal data privacy and the gravity of harm that may be caused to the data subjects by these acts, we recommend that this proposal should be implemented and the PDPO be amended accordingly.

3.4.14 On the scope of regulation, we understand the concern of the public about the definition of "for malicious purposes". We have made reference to the provisions in relevant legislation. One possible formulation is to define it as "with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another"[34].

3.4.15 Regarding defences, most respondents agree that those provided under the UK Data Protection Act should be taken as a reference. As for the exemptions involving public interest, section 61 of the PDPO already provides for the exemption involving news activities. In drafting the defence provisions for the proposed offence, we will consider the relevant provisions in the existing legislation and make reference to the UK legislation, while heeding the difference between the offence under the UK legislation and the proposed offence.

3.4.16 On penalty, some suggest that it should be set at a higher level so as to achieve deterrent effect. As this offence concerns, among other things, also the sale of personal data, one option is to set the penalty at the same level as that for the offence proposed in paragraph 3.3.5(d) above.

3.4.17 As regards the suggestion that the relevant situations should be dealt with by civil remedies instead of criminal sanctions, in view of the seriousness of the intrusion into personal data privacy and the gravity of harm that may be caused to the data subjects as a result of these intentional or wilful acts, we consider that imposing criminal sanctions would be more appropriate.

---

[34] Under section 161 of the Crimes Ordinance, a person commits an offence if he obtains access to a computer "with a view to dishonest gain for himself or another; or with a dishonest intent to cause loss to another". Under section 66 of the PDPO, the damage that may be sought by a data subject for contravention of a requirement under the PDPO by a data user may include injury to feelings.

(4) Excluding Social Services from the Definition of "Direct Marketing" (Proposal No. 38 in the Consultation Document)

Proposal in the Consultation Document

3.5.1 The proposal examines whether to amend section 34 of the PDPO to exclude from the definition of "direct marketing" the offering of social services and facilities by social workers to individuals in need of such services and facilities.

3.5.2 The offering of social services by a social worker could be regarded as direct marketing as defined in section 34(2) of the PDPO. As a result, if an individual contacted by a social worker requests the social worker to cease to use his/her personal data for offering social services or facilities, the social worker has to cease to so use the data. This would seriously frustrate the delivery of services by social workers who, in the proper interests of the client and of the society at large, should continue to "knock at the door" of the client, sometimes even against his or her wish. It is necessary to amend the PDPO to exclude the provision of essential social welfare services from the definition of "direct marketing" under section 34 for the benefit of the target recipients.

Views Received

3.5.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while a minority raised objection. Some other indicated that they had no comment. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.5.4 Respondents who support this proposal agree with the analysis in the consultation document[35]. A respondent suggests that the exemption should apply by reference to the nature of the services provided rather than the persons who offer the services (i.e. social workers)[36].

---

[35] Please refer to S0073, S0080, S0097, S0151, S0156 and S0157 of Annex 4.

[36] Please refer to S0066 of Annex 4. PCCW (S0066) suggests that the exemption should not be confined to social services offered by social workers, but should extend to social services offered or to be offered by any person or organisation.

3.5.5 A respondent who objects to this proposal points out that since more and more social services organisations are taking part in direct marketing activities of a commercial nature, the relevant proposal should not be implemented in order to ensure a level playing field for those in the market[37].

Proposed Way Forward

3.5.6 Views received support the proposal in general. We intend to implement the proposal to amend section 34 of the PDPO. In drafting the relevant amendments, we will carefully examine to which social services providers (individuals or organisations) the proposed exemption should apply so as to ensure that the exemption can serve the intended purpose, i.e. to safeguard the interests of the clients by providing them with the necessary social services.

Data Security

(5) Regulation of Data Processors and Sub-contracting Activities (Proposal No. 2 in the Consultation Document)

Proposal in the Consultation Document

3.6.1 The proposal examines whether the regulation of data processors and sub-contracting activities should be strengthened and the regulatory regimes that can be considered.

3.6.2 Under section 2(12) of the PDPO, a person (data processor) is not taken to be a data user if he holds, processes 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 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).

3.6.3 The consultation document mentioned that sub-contracting or entrusting third parties to handle personal data was gaining

[37] Please refer to S0079 of Annex 4.

prevalence. Leakage of mass personal data on the Internet may result if the data processor contravenes the security regulations. We need to consider how to strengthen the regulation of data processors and sub-contracting activities. Regulatory options include imposing specific obligations on data users (i.e. regulating data processors indirectly through data users), directly regulating data processors, or a combination of the two.

Imposing Specific Obligations on Data Users (Indirect Regulation)

3.6.4 The consultation document proposed for consideration requiring the data user to use contractual or other means to ensure that its data processors and any sub-contractors, whether within Hong Kong or offshore, comply with the requirements under the PDPO in respect of activities related to personal data sub-contracted to them, without imposing explicit obligations on the data processors under the PDPO. This approach imposes specific obligations on data users. Contravention of the requirement will render the data user liable to enforcement action by the PCPD, including the serving of an enforcement notice.

3.6.5 However, if this approach is adopted, the PCPD will not be able to intervene directly with defaults committed by a data processor, thus denying an aggrieved data subject and a data user of a possible redress avenue under the PDPO against the data processor. However, the data subject will have redress against the data user, while the data user will have redress against the data processor, under contractual law.

Regulating Data Processors (Direct Regulation)

3.6.6 As mentioned in the consultation document, in the light of the rising trend of data users sub-contracting or entrusting data processing work to third parties, data subjects may have an expectation that their personal data will have the same protection as that provided by data users, and that data processors should be subject to specific regulation in law. In addition, with the prevalence of sub-contracting arrangements, personal data may be transferred by a data processor to other sub-contractor(s) who may in turn further sub-contract the data processing activities to other agents with whom the data user

has no direct contractual relationship. Without direct regulation of data processors, a data user may be held fully liable under section 65(2) of the PDPO for the wrongdoings of data processors and also sub-contractors with whom he has no direct contractual relationship.

3.6.7 Therefore, the consultation document suggested another option, namely, direct regulation of data processors, for consideration. Data processors will be required:

(a) to ensure that the personal data will be used only for the purpose for which such data were so entrusted or for directly-related purpose;

(b) to take all reasonably practicable steps to ensure the security and safeguarding of the personal data under its custody; and

(c) to take all reasonably practicable steps to erase personal data no longer required for fulfillment of the purpose for which the personal data were entrusted.

Failure to comply with any of the requirements in (a) to (c) above will render a data processor liable to enforcement action by the PCPD, including the serving of an enforcement notice.

3.6.8 The consultation document also pointed out that given that the definition of "data processor" covered business operators of different nature and scale, various practical problems might arise when these operators tried to comply with the above requirements.

3.6.9 First of all, many Internet-related businesses process the same data on behalf of several data users. They may be unaware of the nature of the data, and the purpose for which they were originally collected and whether the information contains personal data. This may make it difficult to specify detailed obligations for data processors in generally applicable legislation without a risk of causing unintended consequences for current or future Internet-related businesses.

3.6.10 In addition, if data processors are imposed with extensive obligations and required to ascertain whether the information

they are storing, indexing, transmitting, serving, etc. is personal data and whether such information is being used for the purpose specified when it is entrusted by a data user for processing, the free flow of information on the Internet and the development of the information technology sector may be impeded.

3.6.11 Indeed, in wake of the fast-evolving Internet environment, many Internet-related businesses have flexibly adopted privacy policies of their own which are appropriate for their business and acceptable to their customers. To ensure flexibility in the development of Internet-related businesses, the consultation document proposed for consideration to make it clear that if a data processor has adopted a privacy policy, which sets out its policy regarding the use, security and retention of personal data, then the obligations in paragraph 3.6.7 should be construed as a requirement to comply with the relevant terms of such privacy policy. Failure to comply with the requirements in its own privacy policy will render a data processor liable to enforcement action by the PCPD, including the serving of an enforcement notice. A data user would also be in breach of his obligations under the PDPO if he chose a data processor whose privacy policy was too lax.

3.6.12 The consultation document sought the views of the public on the following issues:

- whether a data user should be required to use contractual or other measures to secure compliance with the relevant PDPO obligations by its data processor (i.e. indirect regulation);

- whether the activities of a data processor should be directly regulated under the PDPO; and

- if direct regulation of data processors is to be adopted, what obligations should be imposed on data processors, and whether it is appropriate and practical to subject different categories of data processors to different obligations.

Views Received

3.6.13 Of the submissions received, 45% expressed views on this area. Most of them were in support of the general direction of strengthening the regulation of data processors and sub-contracting activities. A small proportion objected to any form of additional regulation and some made no clear indication of their stance. In the consultation activities, almost all participants who commented on this area expressed concern over the strengthening of regulation of data processors and sub-contracting activities.

3.6.14 Respondents who support strengthening the regulation of data processors and sub-contracting activities agree that any leakage of data would cause distress to the data subject concerned. As such, tighter regulation of data processing activities should be adopted and appropriate penalty imposed on the individual concerned in case of contravention [38]. Among these respondents, views supporting direct regulation and indirect regulation are evenly split. A small proportion supports a combination of both. A few others have expressed opinions on the regulatory arrangements.

3.6.15 Respondents who support direct regulation generally consider the effect of indirect regulation limited, and direct regulation is preferable. Their views are set out as follows:

- direct regulation of data processors is more practical and effective. This is because it would be difficult to only rely on a data user to ensure that its data processor has taken reasonable and practicable steps to safeguard the personal data if a data processor is not subject to any legal obligations[39];

---

38 Please refer to S0015, S0060, S0074, S0097, S0129, S0130 and S0154 of Annex 4.

39 For example, the Urban Renewal Authority (S0146) points out that direct regulation on the activities of data processors are more appropriate as enforcement action taken by the PCPD against data processors who are in breach of the PDPO is much more effective than legal action on breach of contract initiated by data users against data processors. The Hong Kong General Chamber of Commerce (S0119) points out that as further sub-contracting activities are not uncommon, it will be an onerous requirement for primary data users to proactively and continuously monitor the operations of their sub-contractors to ensure that their activities are in compliance with the requirements under the PDPO. The Office of the PCPD (S0097) states that some of the data leakage incidents show that very often the cause of the incidents was the lack of sufficient security safeguards on the part of the data processors. Therefore, direct regulation on data processors is essential. Please also refer to S0089, S0137, S0156, S0160 and S0176 of Annex 4.

- appropriate obligations should be placed on data processors. For example, data processors should be required to take appropriate steps to ensure that the personal data processed by them are kept properly. The PCPD should also retain the power to interfere and conduct investigation against a data processor[40];

- given that a data user is already held liable for any act done by its data processor under section 65(2) of the PDPO, the existing legislation already imposes sufficient obligations upon a data user[41]. Indirect regulation, if implemented, will mean additional supervisory obligations for the data user and liabilities for all wrongdoings of its data processors and the sub-contractors with whom it has no direct contractual relationship[42]. This is unfair to the data user. After all, the onus of supervision should be with the Office of the PCPD instead of the data user. The Office of the PCPD should regulate data processors directly, not indirectly through data users[43]; and

- a data subject will expect the same degree of protection for his/her personal data, whether the personal data concerned are handled by a data user or a data processor entrusted by the data user. As such, data processors should be subject to the same degree of regulation under the law[44].

3.6.16 Respondents who support indirect regulation agree to require data users to use contractual or other means to ensure that their data processors comply with the requirements under the PDPO, and generally consider that direct regulation is plagued with loopholes and impracticable. Their views are set out below:

- a data processer may not have the same capability as that of a data user in ensuring the security and lawful use of personal data. It is, therefore, impracticable to request a

---

40 Please refer to S0055 of Annex 4.

41 Please refer to S0123 and S0124 of Annex 4.

42 Please refer to S0072 of Annex 4.

43 Please refer to S0124 of Annex 4.

44 Please refer to S0056 and S0119 of Annex 4.

data processor to ascertain the nature and the authorised use of the data[45]. It is inappropriate to impose direct regulation on data processors at this stage to avoid a sudden increase in pressure on and operating costs of the industry[46];

- some respondents point out that with the prevalence of cross-border sub-contracting activities, if data users entrust the data processing work to overseas contractors who are beyond the jurisdiction of local legislation, the direct regulatory regime will be reduced to mere form[47]. This will, in a way, encourage data users to get around the regulation by entrusting the work to overseas contractors, thus indirectly undermining the business of local sub-contractors and compromising the competitiveness of Hong Kong[48];

- some respondents consider it difficult to define the generic obligations of data processors. To formulate a set of laws applicable to data processors of each and every category will be even more difficult[49]; and

- some respondents consider that indirect regulation allows greater flexibility. By means of contracts, data users and data processors can make flexible arrangements according to circumstances to ensure that the data processing activities are in compliance with the requirements under the PDPO[50]. It is also proposed that the Office of the

---

45 For example, the Hong Kong Computer Society (S0150) points out that, with the continual and speedy development of information technology, the term "data processor" is difficult to be comprehensively defined. Besides, many Internet-related businesses are unaware of the nature of the data they are processing including the purpose for which the data were originally collected. Please also refer to S0073, S0087, S0116 and S0138 of Annex 4.

46 Please refer to S0116, S0121, S0134, S0138 and S0148 of Annex 4.

47 Please refer to S0087, S0116, S0122 and S0138 of Annex 4.

48 Please refer to S0148 of Annex 4.

49 Please refer to S0122 of Annex 4.

50 Please refer to S0116 of Annex 4. Besides, Freshfields Bruckhaus Deringer (S0087) points out that the compliance position in relation to personal data may change, for example, where new privacy policy terms are agreed or where a data subject has requested their removal from a marketing list. These changes are far more likely to be administered by the data user than the data processor and it will often be impracticable for data processors to remain current with this information.

PCPD should formulate guidelines on contract drafting and selection of sub-contracting agents for reference of the data users[51].

3.6.17 Besides, a small proportion of respondents agree to requiring data users to use contractual or other means to ensure that their data processors would comply with the requirements under the PDPO, and also agree to regulating the activities of data processors directly under the PDPO[52]. There are views that in addition to implementing direct regulation of data processors, obligations should also be imposed on data users requiring them to use contractual or other means to require their data processors to provide similar degree of protection. It should also be stipulated clearly that it is the obligation of a data user to ensure the security of personal data when transferring such data to a data processor so as to protect personal data privacy at all levels. As a formal contract will normally be signed between an organisation and the contractor it engaged to carry out the data processing work, adding these specific terms in the contract should not pose any extra burden on the organisation[53].

3.6.18 A small proportion of respondents expressed views on the regulatory arrangements:

- in respect of the details of the regulatory arrangements, some respondents agree to the proposed regulatory arrangements mentioned in items (a) to (c) of paragraph

---

51 Please refer to S0122 of Annex 4.

52 For example, the Estate Agents Authority (S0072), the Office of the PCPD (S0097) and the Democratic Party (S0178) consider that adopting both regulatory models could further enhance the protection of data subjects. Hong Kong Human Rights Monitor (S0157) opines that personal data could be protected from all aspects. In addition, the Hong Kong Association of Banks (S0068) considers that any requirements imposed on data users should be reasonable and practicable. Data users should not be required to secure data processors' compliance with the PDPO by proactively and continuously overseeing or monitoring the operations of data processors, so as not to create an unduly burdensome administrative and operational obligation on data users, which would defeat the objective of the sub-contracting arrangement. The Association also considers that directly regulating data processors' activities would help enhance and maintain the quality and standard of data processors. Please also refer to S0166 of Annex 4.

53 The Office of the PCPD (S0097) expects that data users would select contractors of reasonable standard and quality that can provide adequate security of the personal data in order to comply with the proposed specific obligation.

3.6.7 above[54]. Some suggest that data processors should be divided into different categories and subject to different degrees of regulation[55]. Yet, there are some opposite views that data processors of different categories should not be subject to different obligations[56]; and

- in order to ensure flexibility in the development of Internet-related businesses, Internet-related businesses should be required to exercise self-regulation by adopting privacy policy of their own which sets out the policy regarding the use, security and retention of personal data[57]. Nevertheless, some respondents consider otherwise and opine that there are not enough justifications to support a more relaxed regulatory regime for data processing activities carried out by Internet-related businesses[58]. The Office of the PCPD emphasises that it has the statutory obligation to monitor and supervise compliance with the PDPO and it should not solely rely on individual Internet-related businesses to exercise self-regulation by adopting privacy policies formulated by themselves to ensure the protection of personal data. It also points out

---

54 The Office of the PCPD (S0097) emphasises that as a data processor, an Internet-related business will only be required to ascertain the purpose for which they collected the data for the users of their Internet-related services. It will not be required to ascertain the original purpose for which the data were collected by the users of the services. This issue can be addressed by DPP 3. It also points out that the proposal is not meant to require Internet service providers and web-based service providers to examine each piece of information they process so as to find out whether it contains personal data and what kind of personal data it is, or to provide tailor-made security measures for each set of personal data. Rather, they only need to treat every piece of information as "personal data" and provide proper protection. Yahoo! Hong Kong Limited (S0123) proposes a minor amendment to DPP 4 to clarify that personal data is deemed held by the data user himself if held by his agents or contractors. Baker & Mckenzie (S0124) proposes certain amendments to the regulatory arrangement stated in item (a) of the proposal. Please also refer to S0132 and S0151 of Annex 4.

55 Please refer to S0052 of Annex 4. In addition, the Hong Kong Bar Association (S0067) considers that the proposal should only be applicable to certain types of data processors. Some data processors (e.g. operators of webmail services or social networking websites) have no knowledge of the nature of data processed by them, nor can they exercise full control over the processing of the data. Therefore, they should not be subject to the regulation. On the other hand, data processors who are entrusted to carry out data processing with respect to data which they know are personal data (such as customer record) and who have full control over the processing of such data should be subject to direct regulation.

56 Please refer to S0124 and S0126 of Annex 4.

57 Please refer to S0119, S0123, S0151 and S0162 of Annex 4.

58 Please refer to S0116 and S0124 of Annex 4.

that it does not see convincing justifications for more relaxed requirements specifically for data processing by Internet-related businesses[59].

3.6.19 There are also views that data processors and other sub-contractors could be brought directly under the definition of data user under the PDPO and subject to the same degree of regulation[60] and it is not necessary to formulate additional requirement.

3.6.20 Respondents opposing any form of additional regulation mainly hold the following views:

- some opine that the existing regulatory model is sufficient[61];

- some comment that both direct and indirect regulatory models have shortcomings. Regarding direct regulation, some opine that it may not be practicable to achieve effective regulation as many data processors and their sub-contracting agents are now operating outside Hong Kong[62]; some consider that the proposed regulatory model will, in a way, encourage more data processors to shift the work procedures to places outside Hong Kong to get around the regulation, thus seriously undermining the competitiveness of Hong Kong[63]. As to indirect regulation, some are of the view that such an approach is unfair to data users as the data user (a private operator) should not be relied on to ensure that its data processor (another private operator) is in compliance with the requirements under the law. In addition, regulation by

---

59 Please refer to S0097 of Annex 4.

60 Please refer to S0033 and S0080 of Annex 4.

61 Please refer to S0003, S0109 and S0152 of Annex 4. Clifford Chance (S0113) points out that there is no need to impose further statutory obligations upon data users as the existing legislation already holds data users accountable for the act of its entrusted agents. Hong Kong Jewelry Manufacturers' Association (S0071) is also opposed to the implementation of the proposal. It considers that a stringent regulatory model will not be compatible with the daily operations of the jewellery manufacturing industry.

62 Please refer to S0109 and S0177 of Annex 4.

63 Please refer to S0048, S0049 and S0101 of Annex 4.

means of contract may not be effective[64];

- in the consultation activities, many information technology operators expressed concerns on the proposal to strengthen regulation of data processors and sub-contracting activities. In general, they consider that the proposal will have far-reaching implications on the industry, especially Internet service providers. Some participants opine that Internet service providers are merely responsible for data transmission and should not be defined as data processors. Besides, it is technically impracticable to require Internet services providers to ensure that the data will not be misused[65]; and

- some participants of consultation activities point out that data processing activities in the information technology sector are very complicated. Apart from data processors, parties storing the data in the course of data processing may also be involved. Given that data processing involves a number of parties, some participants consider that the proposed requirement should not be incorporated in the legislation. Instead, they propose to handle it by way of a code of practice.

Proposed Way Forward

3.6.21 The above analysis shows that views received generally support the direction of strengthening the regulation of data processors and sub-contracting activities. However, there are mixed views as to the regulatory model. There are both supporting and opposing views on the direct or indirect regulatory model mentioned in the consultation document. No consensus could be reached.

---

64 Please refer to S0048, S0049 and S0101 of Annex 4. The Hong Kong Institute of Chartered Secretaries (S0062) holds the same views and points out that regulating data processors indirectly through data users will increase the compliance costs of the data users.

65 In addition, PCCW (S0066) also points out that some data processors (especially those in Internet-related businesses) are often unaware of the nature and the content of the data processed by them. They should therefore not be subject to regulation. However, the Office of the PCPD points out that the purpose for which any personal data were entrusted to the Internet service providers and web-based service providers should be transmission of emails. As such, the Internet service providers and web-based service providers should have no practical difficulties in ascertaining the purpose for which the personal data are entrusted to them. To comply with the proposed obligations, they should not use the personal data for any purpose other than for the purpose of transmission of the data.

3.6.22 There are views suggesting that direct regulation of data processors is more practical and effective and they oppose indirect regulation. However, the information technology sector generally objects to direct regulation of data processors. They point out that given that data processors, in particular those engaging in Internet-related businesses, do not have any knowledge of the nature or the use of the data and the procedures involved in data processing are complicated, the adoption of direct regulation may impede the free flow of information on the Internet. Furthermore, the proposal of direct regulation would, in a way, encourage more data processors to get around the regulation by shifting the work procedures to places outside Hong Kong, thus seriously undermining the competitiveness of Hong Kong.

3.6.23 As regards the option to impose obligations on data users, some consider that the obligation imposed on data users under the existing PDPO is already sufficient. They should not be subject to further monitoring obligation. Yet in general, opposition to or concerns about this option are relatively lesser.

3.6.24 Respondents who oppose any form of additional regulation opine that there are shortcomings in both the direct and indirect regulatory models. In addition, the existing PDPO already holds a data user liable for any act done by its data processor. The law has already provided enough protection. They also propose to enhance the protection of personal data privacy by way of a code of practice instead of legislation.

3.6.25 Considering that the public in general agree to the general direction of strengthening the regulation of data processors and sub-contracting activities and data users are already held liable under section 65(2) of the PDPO for any act done by the data processors entrusted by them, we propose 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 render the data user liable to enforcement action by the PCPD, including the serving of an enforcement notice.

3.6.26 We also propose 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.

(6) Personal Data Security Breach Notification (Proposal No. 3 in the Consultation Document)

Proposal in the Consultation Document

3.7.1 The proposal examines whether a personal data security breach notification ("privacy breach notification") system should be instituted to require organisations to 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.

3.7.2 At present, 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. Some jurisdictions such as Canada are moving towards a mandatory notification approach.

3.7.3 The consultation document proposed to start with a voluntary privacy breach notification system so that we could 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. For this purpose, the Office of the PCPD may issue guidance notes on voluntary privacy breach notification for the public and private organisations to duly notify the affected individuals and the PCPD in the event of a privacy breach.

3.7.4 To facilitate the discussion, paragraphs 4.37 to 4.42 of the consultation document set out a possible option which describes the circumstances that trigger the privacy breach notification system, the content, method and time limit of the notification as

well as the consequences of failing to give notification etc.

3.7.5 The consultation document invited comments on the need to institute a voluntary privacy breach notification system and its details including the circumstances under which data users should issue the notice, the content to be covered in the notice, to whom the notice of breach should be sent and by what means should the notice be sent.

Views Received

3.7.6 Nearly half of the submissions received expressed views on this proposal. Most of these submissions agreed to setting up a privacy breach notification system. The majority of them opined that a voluntary privacy breach notification system should be instituted[66] while some supported a mandatory privacy breach notification system. In addition, a few submissions proposed to institute a mixed privacy breach notification system under which for breach incidents involving certain types of data or data users, mandatory notification would be required while for other breach incidents, voluntary notification would be allowed. A minority of the submissions indicated that the existing arrangement was adequate and there was no need to set up a privacy breach notification system. During the various consultation activities, the information technology sector was particularly concerned about this proposal.

3.7.7 Only some respondents commented on the particulars of the privacy breach notification system, including the content, target and time limit of the notification. On the whole, except for the method and content of notification, there was a wide divergence in the views received as to the particulars of the privacy breach notification system. There were views that further consultation should be arranged for discussing the particulars of the notification and relevant guidance notes[67].

---

66 The Hong Kong Research Association conducted a survey to study whether the public agreed to setting up a voluntary privacy breach notification system. The findings showed that 64% of the respondents agreed whilst 16% disagreed. Please refer to S0127 of Annex 4 for details. The Office of the PCPD (S0097) points out that the frequent incidents of electronic data losses reported locally, particular associated with the widespread use of portable electronic devices calls for a tighter control.

67 Please refer to S0068 of Annex 4.

Views Supporting a Privacy Breach Notification System

3.7.8 Respondents who agree to the institution of privacy breach notification system consider that the system can help mitigate the damage to the affected individuals and enhance the transparency and accountability of the organisations. They have also presented the following comments:

- agree that the privacy breach notification system can let the affected individuals take remedial measures as early as possible to mitigate the damage[68];
- consider that with the implementation of the privacy breach notification system, the cost of data users in handling data leakage incidents will increase and this will encourage data users to strengthen the safeguard of data security[69];
- propose that the Office of the PCPD should draw up clear guidelines on the circumstances that will trigger the privacy breach notification system[70]; and
- regarding the data covered by the privacy breach notification system, some people from the information technology sector indicate that the privacy breach notification system should only be limited to those data without password security protection.

---

68 Please refer to S0073, S0099, S0102, S0157 and S0178 of Annex 4. In addition, the Office of the PCPD (S0097) points out that the privacy breach notification system can minimize the exposure of the data subjects to possible damage. This is particularly so when a significant number of data subjects are affected by the breach and where sensitive personal data are lost or stolen. The Independent Police Complaints Council data leakage incident is a good example where sensitive personal data were leaked on the Internet and the affected individuals had to be notified in order that they might take steps to prevent any misuse of their personal data. Furthermore, the Internet Professional Association (S0148) indicates that the privacy breach notification system can set out the procedures for data users to follow in case of data leakage incidents.

69 Please refer to S0150 of Annex 4. In addition, Microsoft (Hong Kong) (S0116) indicates that the introduction of the relevant privacy breach notification system can also promote public confidence in the data custody practices of data users.

70 Please refer to S0052, S0068, S0071, S0073, S0083, S0099, S0116, S0124, S0138, S0148 and S0176 of Annex 4.

Views Supporting a Voluntary Privacy Breach Notification System

3.7.9 Those supporting a voluntary privacy breach notification system are of the view that:

- the proposed privacy breach notification system is still at the initial stage of development and there is no clear and objective standard for notification. If the privacy breach notification system is made mandatory at this stage, it will impose undue burden on data users. Therefore, it will be more appropriate to institute a voluntary privacy breach notification system first[71];

- there are worries that a mandatory privacy breach notification system may result in over-notification. It may be difficult for the public to evaluate the seriousness of the incidents and they may become indifferent to the notification, causing "notification fatigue"[72]; and

- there is neither a mandatory privacy breach notification system nor a universal practice regarding the particulars of the privacy breach notification system internationally. If Hong Kong is to institute a mandatory privacy breach notification system before other places, the differences in arrangements may make it difficult for multinational companies to comply with[73].

Views Supporting a Mandatory Privacy Breach Notification System

3.7.10 Those supporting a mandatory privacy breach notification system are of the view that a voluntary privacy breach notification system is unable to provide the necessary incentive

---

71 For example, although the Law Society of Hong Kong (S0073) indicates agreement to the setting up of a mandatory privacy breach notification system, it holds that a balance should be struck between the need for notification and the costs that will be involved for businesses. It is of the view that a system of notification should be introduced initially by voluntary guidelines issued by the PCPD. Microsoft (Hong Kong) (S0116) points out that a voluntary notification regime will provide crucial data which can then guide subsequent changes to the PDPO. Please refer to S0052, S0066, S0071, S0083, S0087, S0102, S0113, S0122, S0124, S0138 and S0148 of Annex 4.

72 Please refer to S0083, S0123 and S0124 of Annex 4.

73 Please refer to S0138 of Annex 4.

for institutions to make the notification. There is a great possibility that institutions may opt not to make notification so as to avoid their images being blemished, and thus making the system unable to provide sufficient protection to data subjects[74].

3.7.11 Some respondents suggest that a mandatory privacy breach notification should be required only under certain exceptional circumstances, such as when the leakage incident involves sensitive personal data or a certain category of institutions, or when comparatively many people are affected. Otherwise, data users should be allowed to decide on whether privacy breach notification should be made[75].

3.7.12 On the suggestion of making the notification mandatory for a certain category of institutions, the Office of the PCPD points out that although many overseas jurisdictions have not made privacy breach notification system a mandatory requirement, it is the trend for future law reform of other jurisdictions. Government departments and public sector organisations collect vast amount of personal data from members of the public. As those departments and organisations have already implemented a voluntary privacy breach notification system, imposing mandatory privacy breach notification requirement on them as a start will not excessively add to their burden. The Office of

---

74 There are views that if a voluntary privacy breach notification system is implemented, only responsible organisations will make the notification and bear the relevant costs. The system will make responsible companies less competitive but be more beneficial to irresponsible companies (S0155). Please also refer to S0055, S0092, S0118, S0126, S0132, S0160, S0166 and S0168 of Annex 4.

75 For example, Hong Kong IT Alliance (S0109) indicates that if data leakage incident involves government departments, financial institutions or hospitals (guidelines are already drawn up for these sectors), they should be required to make the privacy breach notification as soon as possible while other trades or institutions may opt to make the privacy breach notification. Economy Synergy (S0134) suggests that mandatory notification should be made to the PCPD only for cases involving sensitive personal data leakage, so as to avoid "notification fatigue". However, the submission has not suggested a definition for sensitive personal data. Hong Kong Computer Society (S0150) supports the adoption of a voluntary system under general circumstances. However, when financial or medical data are involved with potential considerable loss, data users should be required to make the notification. Hong Kong Human Rights Monitor (S0157) is of the view that a mandatory privacy breach notification system should be instituted for public sector organisations first while private sector organisations may opt to make the privacy breach notification. After regularly reviewing and fine-tuning the system and if the Administration finds it operating smoothly, it may then set up a comprehensive mandatory privacy breach notification system covering both public and private sector organisations. The Democratic Party (S0178) holds the view that those industries handling high risk personal data, such as banking and finance, may first implement the mandatory notification system, and then extend the coverage to the relatively low risk industries in phases.

the PCPD also recommends that the PCPD should be given the power to specify by notice in the Gazette the class of data users to which the notification requirement applies[76].

Circumstances Triggering the Privacy Breach Notification

3.7.13 Most respondents who comment on this part consider that privacy breach notification is not necessary for all data security breaches. Some point out that the privacy breach notification system should only be triggered when the privacy breach may probably lead to misuse of a subject's unencrypted financial or identity data that will result in identity theft or financial loss[77].

Recipients of the Privacy Breach Notification

3.7.14 The submissions contain different views on the requirements of privacy breach notification. The majority agree that notification should be sent to the affected individuals and most of them consider that both the PCPD and the affected individuals should be notified so that the affected individuals can get prepared early and minimise the damages[78]. There are individual views that it should be mandatory for the data users to notify the PCPD and the Office of the PCPD would then assess the risks and suggest whether privacy breach notifications should be issued to the affected individuals[79]. There are also individual respondents who hold opposite view

---

76 Please refer to S0097 of Annex 4. The Office of the PCPD suggests that, in exercising this power, the PCPD may consider a number of factors including the amount of personal data held by the specific class of data user, the degree of sensitivity of the data as well as the risk of harm to the data subjects as a result of a security breach. The proposed mechanism ensures a gradual process and a selective approach that will balance different interests within the community.

77 For example, the Hospital Authority (S0080) points out that privacy breach notification should be limited to serious cases of personal data leakage or loss. However, it has not given a definition for serious incidents. Please also refer to S0116, S0122, S0138 and S0148 of Annex 4.

78 Please refer to S0083, S0092, S0097, S0102, S0122 and S0148 of Annex 4. Moreover, the Society for Community Organisation (S0132) proposes that in addition to the Office of the PCPD and the affected individuals, the general public should also be informed of the data leakage.

79 For example, the Democratic Alliance for Betterment of Hong Kong ("DAB") (S0145) considers that privacy breach notification to the PCPD by all data users should be made mandatory. As regards whether privacy breach notification should be sent to the affected individuals afterwards, the PCPD, who has better professional assessment ability, would make an assessment and decide whether the institution involved should be required to give privacy breach notification.

and consider that it is not necessary to notify the PCPD[80].

Notification Method

3.7.15 Almost the majority of the submissions consider that the method to make the privacy breach notification should not be limited to one single way but should be decided by the data users[81].

Content to be Covered in the Notice

3.7.16 The majority of the submissions that have commented on the content to be covered in the notice agree with the details outlined in the consultation document[82].

Time Limit on Issuing Privacy Breach Notification

3.7.17 The opinions are divided on the time limit on issuing privacy breach notification. Some respondents agree that privacy breach notification should be sent right after the risk assessment[83], while some consider that the organisations need to collect and analyse the information about the incident and assess the impact prior to issuing the privacy breach notification and the time limit of five business days as suggested in the consultation document will be too short[84]. However, some

---

80 For example, PCCW (S0066) points out that the incidents may involve complicated technologies and notifying PCPD would not necessarily contribute to the damage control. Therefore, the introduction of another bureaucratic step would only serve to consume resources more appropriately directed at containing data leakage.

81 The Law Society of Hong Kong (S0073) suggests that written notification should be sent and if many people are involved in an incident, advertisements should be placed in newspapers. The majority of the remaining submissions indicate that data users should be allowed to decide on the notification method having regard to factors such as cost, number of affected individuals and the normal practice of the data users etc. Please also refer to S0116, S0122, S0124, S0138 and S0148 of Annex 4.

82 Please refer to S0062, S0073, S0113, S0124, S0126, S0132 and S0151 of Annex 4. The AIDS Concern (S0089) suggests that the follow-up measures taken or to be taken by the data user and the Office of the PCPD should also be included in the notice.

83 Please refer to S0122 and S0148 of Annex 4.

84 Please refer to S0066, S0080 and S0156 of Annex 4. Among them, PCCW (S0066) states that as overseas offices may be involved in an incident, more time may be needed to make an assessment as to whether a notification should be sent.

respondents hold opposite view and consider that the time limit of five business days is too long[85].

Views Opposing a Privacy Breach Notification System

3.7.18 Respondents who object to the institution of a privacy breach notification system mainly hold that there is already a voluntary privacy breach notification system in the Government and the banking sector and there is no evidence showing that there are problems of serious delay or inadequacy in privacy breach notifications. It is therefore not necessary to institute another extensive privacy breach notification system[86].

3.7.19 There are views that it is better for the Office of the PCPD to prepare some codes of practice setting out the best practices for handling personal data leakage incidents for organisations to follow rather than requiring organisations to notify the Office of the PCPD of each and every incident.

Proposed Way Forward

3.7.20 The above analysis reveals that the public generally agree to the general direction of introducing a personal data security breach notification system so as to require data users to notify affected individuals and/or the PCPD in the event of personal data security breach.

3.7.21 Relatively more members of the public are of the view that a voluntary privacy breach notification system should be instituted, having regard to the fact that the privacy breach notification system is not yet mature.

3.7.22 Those respondents who support the institution of a privacy breach notification system generally consider that guidance notes on the circumstances under which the system would be

---

85 Please refer to S0157 of Annex 4.

86 Please refer to S0048 and S0101 of Annex 4. Moreover, the Hong Kong General Chamber of Commerce (S0119) stresses that even if the future privacy breach notification system is voluntary, enterprises will in practice be obliged to join the system to avoid the adverse reputational effects of not signing up. In practice, many companies would promptly take pre-emptive action in case of major security breach by notifying data subjects in order to protect their reputation. Hence, there is no urgent need for further guidelines or mandatory requirements.

triggered and other details of the system should be issued.

3.7.23 Any system, be it voluntary or mandatory, should apply to all including Government departments as well as public and private sector organisations so that affected individuals can take appropriate measures to mitigate their loss. However, the impact of a mandatory system cannot be underestimated, as the mandatory requirements may impose onerous burden on data users.

3.7.24 Having taken into account the submissions received and the overseas practices, we consider that we should start with a voluntary privacy breach notification system, with guidance notes issued by the Office of the PCPD. This allows us to adjust the detailed arrangements of the notification, if necessary, having regard to actual operational experience and assessment on the impact of leakage notification, so as to make the privacy breach notification system reasonable and practicable.

3.7.25 In this regard, on 21 June 2010, the PCPD promulgated a guidance note entitled "Data Breach Handling and the Giving of Breach Notifications" to assist data users in handling data breaches and to facilitate them in giving data breach notifications. We will work with the PCPD on the promotional and educational initiatives that can be taken by the PCPD to raise awareness of the guidance note, promote the adoption of a privacy breach notification system by data users voluntarily 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.

Statutory Powers and Functions of the PCPD

(7) Legal Assistance to Data Subjects under Section 66 (Proposal No. 5 in the Consultation Document)

Proposal in the Consultation Document

3.8.1 The proposal examines whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under section 66 of the PDPO, along

the lines of the model of the Equal Opportunities Commission ("EOC")[87].

Views Received

3.8.2 Of the submissions received, over 40% expressed views on this proposal. The majority supported that the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject who intended to seek compensation, a small proportion objected to the proposal, and the rest did not clearly indicate their stand. During the consultation activities, participants from different sectors expressed their views on this proposal.

3.8.3 Most of the respondents who are supportive of this proposal agree with the justifications given in the consultation document. Their views are summarised as follows:

- if the PCPD is empowered to provide legal assistance to an aggrieved data subject, the aggrieved party, when seeking redress under the PDPO, will be in a better position to assess the chance of success of his civil claim and will not be inhibited from filing a lawsuit due to cost considerations. This proposal, if pursued, can achieve greater deterrent effect on acts or practices which intrude into personal data privacy, and enhance the overall effectiveness of sanctions under the PDPO[88];

- as the PCPD possesses first-hand information and is familiar with the PDPO, he is the appropriate authority to provide legal assistance to the public[89];

- as the EOC currently provides legal assistance to the public, the PCPD should follow its practice; and

---

87 The EOC is empowered to assist individuals who wish to pursue compensation through legal proceedings by :
(a) giving advice;
(b) arranging for the giving of advice and assistance by a solicitor or counsel;
(c) arranging for the representation by a solicitor or counsel; and
(d) providing any form of assistance which the EOC considers appropriate.

88 Please refer to S0011, S0073, S0089, S0097, S0102, S0165, S0166, S0171, S0173, and S0178 of Annex 4.

89 Please refer to S0121 and S0134 of Annex 4.

- some respondents supporting the proposal consider that sufficient financial resources should be provided to the PCPD to exercise the new power[90].

3.8.4 Those who object to the proposal have expressed the following views:

- there are not sufficient justifications to subsidise civil claims under the PDPO by taxpayers' money[91];

- as the aggrieved party can apply for legal assistance through the existing channel (i.e. the Legal Aid Department), the PCPD should retain his current independent role[92]; and

- the proposal may confer excessive powers on the PCPD and the PCPD may become partial to the aggrieved party.

3.8.5 To ensure the proper use of public funds, the respondents, whether supporting or objecting to the proposal, generally agree that reference should be made to the factors considered by the EOC in deciding whether to provide legal assistance. These factors include whether the case raises a question of principle, or whether it will be 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[93]. There are also views suggesting that the PCPD should assess the chance of success of a claim to avoid wasting public funds[94].

3.8.6 At a meeting with the information technology sector, some participants commented that if this proposal was to be implemented, measures should be taken to prevent abuse of the mechanism. For example, a means test system can be

---

90 Please refer to S0120, S0145 and S0157 of Annex 4.

91 Please refer to S0048, S0049 and S0101 of Annex 4.

92 Please refer to S0052 and S0066, S0177 and S0180 of Annex 4.

93 Please refer to S0102, S0124 and S0168 of Annex 4.

94 Please refer to S0055 of Annex 4. S0135 also expresses similar views.

introduced similar to the one adopted by the Legal Aid Department so that the information technology sector will not have a heavy burden in responding to legal actions.

Proposed Way Forward

3.8.7 The above analysis shows that the views received generally agree to the direction that the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject, while emphasising the importance of taking proper measures to prevent abuse.

3.8.8 Therefore, we recommend that:

(a) the PDPO should be amended by adding new provisions to empower the PCPD to provide legal assistance to an aggrieved data subject;

(b) as regards details of the provision of legal assistance, making reference to the EOC model, we propose to provide the following assistance to a person who intends to institute legal proceedings to seek compensation: giving legal advice on the sufficiency of evidence, arranging for a lawyer from the Office of the PCPD to act as the legal representative of the applicant, arranging for either a lawyer from the Office of the PCPD or an outside lawyer to represent the applicant in legal proceedings, and providing any form of assistance which the Office of the PCPD considers appropriate; and

(c) to ensure proper use of public funds, the legislation should require the Office of the PCPD to consider a request for legal assistance on the basis of the following factors: 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.

3.8.9 If the Office of the PCPD cannot provide legal assistance on the application of the aggrieved party, the latter can still apply to the Legal Aid Department for legal aid or bring a lawsuit by himself.

(8) Circumstances for Issue of an Enforcement Notice (Proposal No. 20 in the Consultation Document)

Proposal in the Consultation Document

3.9.1 Section 50 of the PDPO provides that the PCPD, following the completion of an investigation, where he is of the opinion that a data user: (a) is contravening a requirement under the PDPO; or (b) has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated, may issue an enforcement notice to direct the data user to take such steps as are specified in the notice to remedy the contravention or the matters occasioning it. In deciding whether to serve an enforcement notice, the PCPD must also consider whether the contravention has caused or is likely to cause damage or distress to the data subject.

3.9.2 Under section 50 of the PDPO, the PCPD cannot serve an enforcement notice on a data user if the contravening act has ceased and the PCPD considers that there is no evidence showing that the contravention will likely be repeated, even if the act has caused harm or damage to the data subject.

3.9.3 To enhance the effectiveness of the PDPO in the protection of personal data privacy, the consultation document sought the views of the public on whether, in addition to the circumstances set out in items (a) and (b) in paragraph 3.9.1 above, to add another item (c), that is to empower the PCPD to serve an enforcement notice where the contravention has caused or is likely to cause damage or distress to the data subject.

Views Received

3.9.4 Of the submissions received, over 10% expressed views on this proposal. Of these, some 40% opposed the implementation of the proposal, over 30% indicated their support while the rest did not give a clear standpoint. Comments on the proposal were also received during various consultation activities.

3.9.5 Those who oppose the implementation of this proposal mainly consider it unnecessary to serve an enforcement notice on a data user if the contravening act has ceased and there is no likelihood

of repetition[95]. Also, quite a lot of comments consider the existing mechanism effective and should therefore be maintained. They consider the introduction of a new provision unnecessary as this will impose additional administrative burden on data users[96].

3.9.6 Those who express support to the implementation of this proposal point out that currently the PCPD is constrained by the PDPO in issuing enforcement notices, and the proposed amendment will allow PCPD more flexibility in serving enforcement notices, thereby improving the protection in relation to personal data privacy[97]. The Office of the PCPD also proposes that besides item (c) as mentioned in paragraph 3.9.3, an additional item "such matters as the Commissioner may think fit to consider" be added so as to give the PCPD more flexibility in serving enforcement notices and to provide greater protection to privacy[98]. However, a respondent is of the view that granting such power to PCPD will create uncertainty as to the application of the section and may easily lead to dispute[99].

Proposed Way Forward

3.9.7 According to section 50 of the PDPO, currently the PCPD cannot serve an enforcement notice on a data user if the contravening act has ceased, unless there is sufficient evidence for him to form the opinion that the contravention will likely be repeated (i.e. item (b) of paragraph 3.9.1).

3.9.8 That said, in some cases, although the contravening act has ceased, and it is unlikely that the contravention will be repeated,

---

95 Please refer to S0062, S0066 and S0068 of Annex 4. PCCW (S0066) suggests that, to enhance the protection of personal data privacy, the PCPD may consider providing professional recommendations and technical assistance to data users upon request.

96 Please refer to S0068, S0080, S0123 and S0156 of Annex 4.

97 Please refer to S0052, S0073, S0097, S0132, S0151, S0162, S0165 and S0166 of Annex 4. Also, Baker & McKenzie (S0124) considers that if the intention is that the PCPD would be permitted in the enforcement notice to require the data user not to repeat the same activity, then this proposal shall be pursued, provided that the prohibited activity is clearly defined.

98 Please refer to S0097 of Annex 4. Also, Hong Kong Human Rights Monitor (S0157) indicates preliminary agreement with the PCPD's proposal and considers that further consultation should be conducted by the Administration on the proposal.

99 Please refer to S0124 of Annex 4.

damage or distress to the data subject may have already been resulted and may be continuing. Under these circumstances, the PCPD may need to issue an enforcement notice to direct the data user to take such steps as are specified in the notice to avoid further damage or distress to the data subject.

3.9.9 The UK Data Protection Act provides that if the Information Commissioner of the UK is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioner may serve on him an enforcement notice. The Act does not require the Commissioner to consider whether the contravention will likely continue or be repeated.

3.9.10 To enhance the effectiveness of the PDPO in the protection of personal data privacy, we propose to model on the provisions of the UK Data Protection Act and empower the PCPD to, following the completion of an investigation, where he is of the opinion that a data user: (a) is contravening a requirement under the PDPO; or (b) has contravened such a requirement, issue an enforcement notice to direct the data user to take such steps as are specified in the notice to remedy the contravention or the matters occasioning it. In deciding whether to serve an enforcement notice, the PCPD still has to follow the existing requirement under the PDPO to consider whether the contravention has caused or is likely to cause damage or distress to the data subject.

(9) Clarifying Power to Direct Remedial Steps in an Enforcement Notice
(Proposal No. 21 in the Consultation Document)

Proposal in the Consultation Document

3.10.1 The proposal examines whether it should be specified 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.

3.10.2 The existing section 50(1) of the PDPO requires the PCPD to specify in an enforcement notice a period within which remedial steps are required to be taken by the data user. However, if the

remedial steps directed by the PCPD in an enforcement notice to be taken by the data user within the specified period include desisting from doing a certain act or engaging in a certain practice, it may be misconstrued as requiring the data user to desist from doing the act or engaging in the practice only within the specified period, but not thereafter.

3.10.3 To remove this grey area, the consultation document proposed to specify in section 50(1) that the PCPD has the power to direct in an enforcement notice a data user to desist from doing a certain act or engaging in a certain practice within the specified period and also thereafter.

Views Received

3.10.4 Of the submissions received, more than 10% expressed views on this proposal. The majority supported the implementation of the proposal while some had no comment. A minority raised objection. During the consultation activities, no participant expressed clear standpoint on this proposal.

3.10.5 Those in support of this proposal all agree that there is a need to amend the existing provision to clarify the power of the PCPD to give directive on remedial steps in an enforcement notice[100]. Those opposing this proposal opine that it is not necessary to amend the relevant provision as the provision is only slightly unclear and will not affect the power of the PCPD[101].

Proposed Way Forward

3.10.6 Views received generally support this proposal. To clarify the relevant provision, we intend to implement this proposal and make corresponding amendments to the PDPO.

---

[100] Please refer to S0062, S0073, S0097, S0124, S0151, S0157, S0162, S0165 and S0166 of Annex 4.

[101] Please refer to S0080 and S0156 of Annex 4. Besides, the Society for Community Organisation (S0132) opines that it is just a matter of wording. Even no amendment is made, the PCPD can still direct the data user in an enforcement notice to desist from doing a certain act or engaging in a certain practice.

(10) Removing the Time Limit to Discontinue an Investigation (Proposal No. 22 in the Consultation Document)

Proposal in the Consultation Document

3.11.1 The proposal examines whether the provision on the time limit with regard to a decision to discontinue an investigation by the PCPD should be amended to remove the time limit.

3.11.2 At present, section 39(3) of the PDPO stipulates that, if the PCPD refuses to continue an investigation initiated by a complaint, he has to notify the complainant of the refusal within 45 days after receiving the complaint. If the PCPD has not taken a decision to discontinue an investigation within the 45-day time frame, the PCPD may have to continue with the investigation even if he subsequently finds that further investigation is not warranted or is unnecessary. The continuation of such an investigation is not fair to the complainee. Neither is it conducive to the optimal use of the PCPD's resources.

3.11.3 Therefore, the consultation document proposed to remove the requirement under section 39(3) of the PDPO to inform the complainant of a decision to discontinue an investigation within 45 days after receipt of the complaint. However, the existing requirement that the PCPD should notify a complainant in writing of his decision not to continue with the investigation and the reasons for the decision will be retained, so that the complainant may appeal under section 39(4) against the PCPD's decision to discontinue an investigation.

Views Received

3.11.4 Of the submissions received, more than 10% expressed views on this proposal. The majority supported the implementation of this proposal while some had no comment. A minority raised objection. During the consultation activities, no participant expressed clear standpoint on this proposal.

3.11.5 Respondents supporting this proposal all agree that the implementation of the proposed amendment will help improve the cost effectiveness of the operation of the Office of the PCPD

and accord fairer treatment to the complainee[102]. A few respondents who raise objection point out that the existing rule is clear and precise and should be retained[103].

Proposed Way Forward

3.11.6 Since the submissions received generally support this proposal, and the implementation will help improve the cost effectiveness of the operation of the Office of the PCPD and to provide fair treatment to the complainee, we intend to implement this proposal and make corresponding amendments to the PDPO.

(11) Additional Grounds for Refusing to Investigate (Proposal No. 23 in the Consultation Document)

Proposal in the Consultation Document

3.12.1 The proposal examines whether the relevant provision should be amended to include additional grounds for the PCPD to refuse to carry out or continue an investigation.

3.12.2 At present, under section 38 of the PDPO, upon receipt of a complaint, the PCPD shall, subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in a complaint is a contravention of a requirement under the PDPO. Section 39(2) empowers the PCPD to refuse to carry out or continue an investigation if he is of the opinion that having regard to all the circumstances of the case:

(a) the complaint, or a complaint of a substantially similar nature, has previously led to an investigation, as a result of which the PCPD was of the opinion that there had been no contravention of a requirement under the PDPO;

(b) the act or practice specified in the complaint is trivial;

---

[102] Please refer to S0011, S0062, S0073, S0080, S0097, S0124, S0152, S0156, S0157, S0162 and S0165 of Annex 4.

[103] The Society for Community Organisation (S0132) opines that the existing provision should be retained as the complainant knows that he will be informed of the PCPD's decision within a certain period of time. The Hong Kong Doctors Union (S0151) also objects to the implementation of the proposal and proposes to extend the time limit from 45 days to 60 days.

(c) the complaint is frivolous or vexatious or is not made in good faith; or

(d) any investigation or further investigation is for any other reason unnecessary.

3.12.3 The PCPD has a wide discretion to refuse to carry out or continue an investigation on the ground under section 39(2)(d), i.e. "any investigation or further investigation is for any other reason unnecessary". In the light of regulatory experience, some common situations where the PCPD has exercised his discretion to refuse to carry out an investigation are:

(a) where the primary cause of the complaint is not related to personal data privacy;

(b) where the complaint relates to an action for which the complainant has a remedy in any court or tribunal, or which is currently or soon to be under investigation by another regulatory body; or

(c) where the act or practice specified in a complaint relates to personal data or documents containing personal data which have been or will likely be used at any stage in legal proceedings or inquiry.

3.12.4 To make the provision clearer, the consultation document proposed a possible option, i.e. to include the scenarios cited in paragraph 3.12.3 above as specific grounds for refusing to investigate under section 39(2). This would enable potential complainants to have a better idea of the situations where the PCPD may refuse to carry out or continue investigations on their complaints. This would help minimise potential contention about the exercise of discretion by the PCPD under section 39(2)(d) and hence reduce the chances of complainants taking the cases to the AAB.

3.12.5 However, the consultation document raised the following concerns with regard to the abovementioned arrangement. Firstly, the consultation document indicated reservation on including as a ground of refusal "where a complaint relates to an action for which the complainant has a remedy in any court or tribunal" (i.e. paragraph 3.12.3(b) above). The purpose of

setting up the PCPD is to provide relief for privacy violations in addition to any civil remedies that may be available. To refuse to investigate a complaint on the aforesaid ground would deprive an aggrieved party of an alternative for redress.

3.12.6 Moreover, the inclusion of these additional specific grounds for refusal to investigate could be perceived as taking away the right of a data subject to have his complaint, which relates to personal data privacy, from being investigated. Although the complainant may seek redress by lodging an appeal with the AAB against the PCPD's decision not to investigate, the scope of such review would be limited. Given the PCPD's role in the protection of personal data privacy, it may not be appropriate to make it clear in the PDPO these additional specific grounds for the PCPD to refuse investigation.

3.12.7 After taking the above analysis into consideration, views are invited on whether it is appropriate to include the following additional specific grounds for the PCPD to refuse to carry out or continue an investigation under section 39(2):

(a) the primary cause of the complaint is not related to personal data privacy;

(b) the complaint relates to any action which is currently or soon to be under investigation by another regulatory body; or

(c) the act or practice specified in the complaint relates to personal data or documents containing personal data which have been or will likely be or are intended to be used at any stage in any legal proceedings or inquiry before any magistrate or in any court, tribunal, board or regulatory or LEAs.

Views Received

3.12.8 Of the submissions received, more than 10% expressed views on this proposal. The majority supported the implementation of the general direction of the proposal while some of them made suggestions on the details of implementation. No submissions objected to the general direction of this proposal. During the consultation activities, no participants expressed

clear standpoint on this proposal.

3.12.9 Respondents supporting this proposal all agree that the proposal would make the existing provision clearer and enable complainants to have a better understanding of the circumstances in which the PCPD would refuse to carry out or continue an investigation[104]. However, some respondents who agree to the general direction of the proposal express the following concerns on the proposed specific grounds mentioned in paragraph 3.12.7:

- some object to the introduction of item (b) as they consider that even if a case is being investigated by another regulatory body, the focus may not be related to personal data privacy. Hence, this should not constitute a ground for the PCPD to refuse to carry out an investigation[105]; and

- there are also individual submissions objecting to the introduction of item (c). They opine that even if the personal data concerned have been or would likely be used at any stage in any legal proceedings or inquiry, the PCPD can carry out an investigation on any act or practice of unreasonable or improper handling of personal data before such use of the data[106].

Proposed Way Forward

3.12.10 Views received generally support the general direction of this proposal to clarify the relevant provision. However, as some express concerns that the proposed specific grounds mentioned in items (b) and (c) in paragraph 3.12.7 may deprive an aggrieved party of the right to seek redress under the PDPO, we

---

104 Please refer to S0011, S0062, S0073, S0080, S0097, S0151, S0152, S0156, S0157 and S0165 of Annex 4. Moreover, the Office of the PCPD (S0097) points out that in some cases it may not be an appropriate forum for the aggrieved individual to seek redress, when compared with the sanction imposed under other laws or ordinances. In order to address the concern, it had proposed for a saving clause when it is not reasonable to expect the complainant to resort or to have resorted to the right or remedy in court or tribunal. In addition, the Ombudsman Ordinance also contain similar ground of refusal under section 10(1)(e)(ii).

105 Please refer to S0132, S0151 and S0157 of Annex 4. On the other hand, Baker & McKenzie (S0124) opines that the complainant should not be required to prove that the complaint is genuinely based on data privacy concerns. Complainants should not be precluded from seeking the PCPD's assistance in investigating and restraining the activity prohibited by the PDPO.

106 Please refer to S0151 and S0157 of Annex 4.

propose that, at this stage, only item (a) of paragraph 3.12.7 (i.e. "the primary cause of the complaint is not related to personal data privacy") should be included in section 39(2) as a ground for the PCPD to refuse to carry out or continue an investigation. As regards the other scenarios, the PCPD could consider whether an investigation would be carried out in accordance with section 39(2)(d) taking into account the justifications of individual cases.

(12) Relieving the PCPD's Obligation to Notify the Complainant who has Withdrawn his Complaint of Investigation Result (Proposal No. 28 in the Consultation Document)

Proposal in the Consultation Document

3.13.1 The proposal examines whether 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) where the complainant has withdrawn his complaint.

3.13.2 Section 40 of the PDPO empowers the PCPD to carry out or continue an investigation initiated by a complaint notwithstanding the fact that the complainant has withdrawn the complaint if the PCPD considers that it is in the public interest to do so. Section 40 further stipulates that in any such case, the provisions of the PDPO shall apply to the complaint and the complainant as if the complaint had not been withdrawn.

3.13.3 Under section 47(3), the PCPD is obliged to notify the complainant of the result of the investigation, any recommendations made to the relevant data user, any report arising from the investigation that he proposes to publish under section 48, any comments made by or on behalf of the relevant data user on any such recommendations or reports, whether or not he has served or proposes to serve an enforcement notice on the relevant data user in consequence of the investigation and other comments arising from the investigation. However, if the complainant has withdrawn his complaint, it should not be obligatory for the PCPD to inform the complainant of the PCPD's investigation result and the related matters. The proposal is meant to remove the required notification under such circumstances.

Views Received

3.13.4 Of the submissions received, less than 10% expressed views on this proposal. The majority indicated that they had no comment. The rest supported the implementation of the proposal, while an individual submission expressed objection. During the consultation activities, no participants expressed clear standpoint on this proposal.

3.13.5 Respondents supporting this proposal all agree with the analysis of the consultation document and consider it necessary to implement the proposed amendment[107]. The respondent who raises objection opines that the existing requirement should be retained and the PCPD should inform the complainant of the investigation result once the investigation is completed[108].

Proposed Way Forward

3.13.6 Of the submissions received, more are in support of this proposal. We would make corresponding amendments to the PDPO 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) where the complainant has withdrawn his complaint.

(13) PCPD to Serve an Enforcement Notice together with the Result of Investigation (Proposal No. 42 in the Consultation Document)

Proposal in the Consultation Document

3.14.1 The proposal examines whether to amend section 47 of the PDPO to allow the PCPD to serve an enforcement notice on the relevant data user at the time of notifying the relevant parties of the result of investigation.

3.14.2 Sections 47(2)(d) and 47(3)(e) require the PCPD to notify the relevant data user and the complainant respectively upon completion of investigation whether or not he "proposes to serve an enforcement notice" on the relevant data user in

[107] Please refer to S0073, S0097 and S0151 of Annex 4.

[108] Please refer to S0157 of Annex 4.

consequence of the investigation. The PCPD may subsequently serve the enforcement notice on the data user. To enable the PCPD to serve an enforcement notice to direct the relevant data user to take remedial actions as soon as possible, the consultation document proposed to amend sections 47(2)(d) and 47(3)(e) to allow the PCPD to serve an enforcement notice on the relevant data user at the time of notifying the complainant and the relevant data user of the result of investigation.

Views Received

3.14.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal[109] while some indicated that they had no comment. No respondents raised objection. During the consultation activities, no participants had a clear standpoint on this proposal.

Proposed Way Forward

3.14.4 Views received support this proposal in general. We intend to implement this proposal by amending section 47 of the PDPO to allow the PCPD to serve an enforcement notice on the relevant data user at the time of notifying the relevant parties of the investigation result.

(14) PCPD to Disclose Information in the Performance of Functions (Proposal No. 29 in the Consultation Document)

Proposal in the Consultation Document

3.15.1 The proposal examines whether section 46 of the PDPO should be amended 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.

3.15.2 Section 46 of the PDPO prohibits the PCPD and his staff from disclosing matters that come to their knowledge in the performance of functions and exercise of powers except in

[109] Please refer to S0011, S0048, S0049, S0062, S0073, S0097, S0101, S0151 and S0157 of Annex 4.

limited specified circumstances[110].

3.15.3 This proposal would enable the PCPD and his staff to disclose information reasonably necessary for the proper performance of the functions and powers of the PCPD, such as disclosure of information to statutory bodies like the AAB which handles appeals against certain decisions of the PCPD as stipulated in the PDPO and to overseas data protection authorities to facilitate cross-border privacy cooperation in the enforcement of personal data privacy rights. Some statutory bodies such as the Securities and Futures Commission and the EOC are permitted under their respective legislation to disclose information for the proper discharge of the functions and the exercise of powers.

Views Received

3.15.4 Of the submissions received, less than 10% expressed views on this proposal. The majority supported the implementation of the proposal while an individual submission raised objection. The rest indicated that they had no comment. During the consultation activities, no participants expressed clear standpoint on this proposal.

3.15.5 Respondents supporting this proposal all agree with the analysis in the consultation document and consider that there is a need to implement the proposal[111].

3.15.6 The respondent who raises objection points out that a general provision allowing the PCPD and his prescribed officers to disclose information should not be made as it is too vague and broad. Any exceptions from the secrecy obligation should be specified, limited and concrete[112]. A respondent who supports the implementation of the proposal also considers it necessary

---

[110] These include: (a) court proceedings for an offence under the PDPO; (b) reporting evidence of any crime; or (c) disclosing to a person any matter which in the PCPD's opinion may be ground for a complaint by that person.

[111] Please refer to S0011, S0048, S0049, S0062, S0097, S0101, S0151 and S0157 of Annex 4.

[112] Please refer to S0068 of Annex 4. The Hong Kong Association of Banks (S0068) points out also that information disclosed to overseas data protection authorities should be restricted to non-confidential data.

to enumerate situations under which disclosure may be made[113].

Proposed Way Forward

3.15.7 Views received support this proposal in general. We intend to implement this proposal and make corresponding amendments to the PDPO 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. When drafting the legislation, we would make reference to the provisions under other relevant legislation.

(15) Immunity for the PCPD and his Prescribed Officers from being Personally Liable to Lawsuit (Proposal No. 30 in the Consultation Document)

Proposal in the Consultation Document

3.16.1 The proposal examines whether the PDPO should be amended to protect the PCPD and his prescribed officers from being 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.

3.16.2 At present, the PCPD and his prescribed officers are not immune from legal liability as a result of exercise of powers and functions under the PDPO. Similar immunity provisions are stipulated in the legislation governing other statutory bodies (e.g. the Airport Authority, EOC, Mandatory Provident Fund Schemes Authority and The Ombudsman.)

Views Received

3.16.3 Of the submissions received, less than 10% expressed views on this proposal. The majority supported the implementation of the proposal while a respondent raised objection. The rest indicated that they had no comment. During the consultation activities, no participants expressed clear standpoint on this proposal.

---

[113] Please refer to S0073 of Annex 4. The Law Society of Hong Kong (S0073) opines that unless the act under investigation will constitute violation of the DPPs or an offence under the PDPO if committed in Hong Kong, there should not be any disclosure to overseas data protection authorities.

3.16.4 Respondents supporting this proposal all agree with the analysis in the consultation document and consider it necessary to implement the proposed amendment[114]. The respondent who objects to this proposal opines that this proposal will lead to abuse and the immunity protection should be considered on a case by case basis[115].

Proposed Way Forward

3.16.5 Views received generally support this proposal. We intend to implement this proposal by adding a new provision in the PDPO to stipulate 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.

3.16.6 In response to possible abuse by public officers mentioned by a respondent, we would make reference to similar exemption clauses provided to statutory bodies in other legislation when we draft the amendments, to ensure that the protection would be appropriate and fair.

(16) Power to Impose Charges for Educational and Promotional Activities (Proposal No. 31 in the Consultation Document)

Proposal in the Consultation Document

3.17.1 The proposal examines whether an express provision should be made to empower the PCPD to impose reasonable charges for undertaking educational or promotional activities or services.

3.17.2 At present, there is no express provision under the PDPO to empower the PCPD to charge fees for educational and promotional services he renders. Some of the statutory bodies are currently provided with the power to charge fees. For example, the EOC is empowered to impose reasonable charges for educational or research projects undertaken by it under

[114] Please refer to S0048, S0049, S0073, S0097, S0101, S0151 and S0157 of Annex 4.

[115] Please refer to S0011 of Annex 4.

section 65 of the Sex Discrimination Ordinance (Cap. 480). Section 9A of The Ombudsman Ordinance (Cap. 397) provides that the Ombudsman may charge such reasonable fee in respect of service approved by the Director of Administration.

Views Received

3.17.3 Of the submissions received, less than 10% expressed views on this proposal. The majority supported the implementation of the proposal while some of them raised objection. The rest indicated that they had no comment. During the consultation activities, no participants expressed a clear standpoint on this proposal.

3.17.4 Respondents supporting this proposal all agree with the analysis in the consultation document and consider that it is reasonable for the PCPD to impose charges for undertaking educational or promotional activities or services. This is because the charges imposed are to cover the expenses involved in providing educational or promotional activities or services and not for making profit[116].

3.17.5 Individual respondents objecting to this proposal opine that one of the major duties of the Office of the PCPD is to undertake educational and promotional activities. Hence, it should not impose any charges for these services[117].

Proposed Way Forward

3.17.6 Views received generally support this proposal. We intend to implement this proposal and make corresponding amendments to the PDPO to expressly provide the PCPD with power to impose reasonable charges for undertaking educational or promotional activities or services. When drafting the

---

[116] Please refer to S0048, S0049, S0073, S0097, S0101, S0157 and S0166 of Annex 4. Moreover, Hong Kong Human Rights Monitor (S0157) opines that the PCPD should also have the discretion to waive the charges.

[117] Please refer to S0124 of Annex 4. Baker & McKenzie (S0124) opines that if the Office of the PCPD imposes charges for providing educational and promotional services, some smaller or less well-resourced organisations are placed at a disadvantage. Please refer to S0011 and S0151 for other comments objecting to this proposal.

amendments, we would make reference to similar provisions on charging in other legislation.

(17) Power to Obtain Information to Verify a Data User Return (Proposal No. 32 in the Consultation Document)

Proposal in the Consultation Document

3.18.1 The proposal examines whether to confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return filed under section 14 of the PDPO.

3.18.2 A data user is required under section 14 of the PDPO to submit to the PCPD a return containing prescribed information[118]. The data user return is open for public inspection. The proposal is to empower the PCPD to obtain information from the data user to verify the information stated in a data user return to ensure that the information provided is accurate.

Views Received

3.18.3 Of the submissions received, less than 10% expressed views on this proposal. Over 60% of them supported the implementation of the proposal while some 15% raised objection. The rest indicated that they had no comment. During the consultation activities, no participants expressed a clear standpoint on this proposal.

3.18.4 Those who support this proposal agree with the analysis in the consultation document[119]. Of those who raise objection, some opine that at present, as section 64(1) stipulates that a data user who knowingly or recklessly supplies any information which is

---

[118] The information includes the name and address of the data user, the kind of personal data collected, the purposes of collection, classes of transferees, and places outside Hong Kong to which the personal data are transferred.

[119] Please refer to S0011, S0048, S0062, S0101, S0151 and S0157 of Annex 4. Also, the Law Society of Hong Kong (S0073) suggests that it should be clearly indicated in the legislation that for the purpose of verifying the information in a data user return, the PCPD is exercising a general inspection power comparable to inspection powers under section 36, rather than investigation powers under section 38 of PDPO. Separately, the Office of the PCPD suggests empowering the PCPD to specify from time to time, by notice in the Gazette, the "prescribed information" to be submitted.

false or misleading commits an offence, the proposal need not be implemented[120]. Separately, an opposing view points out that at present, the PCPD may under section 14 require a data user to submit a data user return but he has never exercised this power. It is not proper to grant an additional power to the PCPD on top of one that he has never invoked.

Proposed Way Forward

3.18.5 In fact, section 14 is already in force (although the PCPD has not yet implemented the data user return arrangements). When considering whether the proposal should be implemented, whether or not the PCPD has actually invoked this statutory power should not be a consideration. Most of the views received also recognise the need to confer upon the PCPD the power to obtain information from any person in order to verify the information in a data user return, so as to ensure its accuracy. Therefore, we intend to implement this proposal.

Offences and Sanctions

(18) Repeated Contravention of a Data Protection Principle on Same Facts
(Proposal No. 9 in the Consultation Document)

Proposal in the Consultation Document

3.19.1 The proposal examines whether it should be made an offence for a data user who, having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice.

3.19.2 At present, if a data user breaches a DPP, the PCPD may issue an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he commits an offence[121]. However, under the existing provisions, if a data user resumes

---

[120] Please refer to S0068 of Annex 4.

[121] Liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

the same contravening act or practice shortly after compliance with an enforcement notice issued against him, the PCPD can only issue another enforcement notice.

3.19.3 To forestall circumvention of the regulatory regime as described above, the consultation document proposed that consideration be given to making it an offence for repeated contravention of a DPP intentionally on same facts. However, the consultation document also pointed out that this would be moving away from the original intent of adopting the DPPs in the PDPO and that since the enactment of the PDPO, the PCPD has not come across any such case of circumvention as described above.

3.19.4 The consultation document consulted the public on whether repeated contravention of a DPP intentionally should be made an offence and on the penalty level for the offence.

Views Received

3.19.5 Nearly 40% of the submissions received commented on this proposal. Among these submissions, there were mixed views of supporting and opposing the proposal. Only a few participants commented on the proposal during various consultation activities.

3.19.6 Some respondents who are in support of the broad direction of this proposal agree to the proposed arrangements set out in the consultation document[122] and opine that the proposal can help increase the deterrent effect and forestall possible circumvention of the regulatory regime[123]. The Office of the PCPD comments that it is not uncommon for different complainants to complain against the same data user at different times on the same or similar facts and the series of data loss incidents are real examples of repeated contraventions. The Office of the PCPD believes that a proactive and forward-looking attitude should be adopted in order to enhance data privacy protection at this electronic age[124]. A respondent

---

122 Please refer to S0060, S0073, S0074, S0083, S0089, S0107, S0129, S0151, S0179 and S0180 of Annex 4.

123 Please also refer to S0014, S0083 and S0157 of Annex 4.

124 Please refer to S0097 of Annex 4.

suggests that as the enforcement notice is couched in more specific terms than DPPs, resuming the same contravening act or practice shortly after compliance with an enforcement notice should be made an offence. This, in the respondent's view, would not be moving away from the original intent of adopting the DPPs[125].

3.19.7 However, many of those who agree with the broad direction of the proposal have also made the following suggestions regarding the detailed implementation:

- although the enforcement notice is couched in more specific terms than DPPs in general, there may be some cases in which the enforcement notices are not clear enough so that data users repeat the same contravening acts unconsciously. The proposal should only address instances of malicious and intentional acts to circumvent the regulatory regime in order to avoid incriminating the innocents. As such, it is suggested that exemption clauses should be made to exempt unintentional acts or cases with reasonable defences[126]; and

- the meaning of "resuming the same contravening act or practice shortly" should be clearly defined, and it is suggested that the time limit should be one to two years[127].

3.19.8 There are only a few respondents who comment on the penalty level. Some suggest that the penalty should be the same as that for breaching an enforcement notice[128], i.e. liable to a fine at Level 5 ($50,000) and imprisonment for two years upon conviction, while some argue that it should carry a heavier

---

125 Please refer to S0067 of Annex 4.

126 PCCW (S0066) considers that the validity of the enforcement notice has to be proved beyond reasonable doubts before laying charges. The Society of Operations Engineers (Hong Kong Region) (S0131) opines that the Administration should consider an exception or flexibility for non-profit making bodies when imposing heavier penalty for the repeated non-compliance with an enforcement notice as they may lack of comprehensive data control. Please also refer to S0011, S0121 and S0134 of Annex 4.

127 For example, the Society for Community Organisation (S0132) suggests setting a time limit, say, one or two years, so that data users who have violated DPPs in the past would not be held criminally liable for contraventions of the relevant DPPs on same facts several years or decades later. Please also refer to S0102 of Annex 4.

128 Please refer to S0155 of Annex 4.

penalty than that for an ordinary breach of enforcement notice[129]. Some consider that a lighter penalty should be imposed[130]. Opinions vary.

3.19.9 The views raised by those opposing this proposal are:

(a) the current regulatory regime is considered to be effective, and since the enactment of the PDPO, the PCPD has not come across similar cases of circumvention of the regulatory regime. So, it is not necessary to make the act an offence[131];

(b) DPPs are couched in generic terms and can be subject to a wide range of interpretations. If the contravention (whether repeated or not) of a DPP is made an offence, it will seriously affect general commercial operations[132]. As the actual circumstances of each case are different, it is very hard to define clearly "the same contravening act or practice" in the legislation. Moreover, for the purpose of exempting certain unintentional contraventions, it is necessary to determine objectively whether the data user intentionally does the same act or engages in the same practice, and the word "intentionally" should be narrowly defined. Therefore, the proposal is considered not feasible[133]; and

(c) the enactment of a new criminal offence should be in compliance with basic legal principles, i.e. the offence should be stated clearly and specifically, and the enactment

---

129 Please refer to S0097 and S0162 of Annex 4.

130 The Hong Kong Bar Association (S0067) considers that the penalty for repeated contraventions of DPPs should be less than for a breach of enforcement notice because there would be no element of directly flouting a requirement imposed by the PCPD. Therefore, it proposes a penalty of a fine at Level 5.

131 Please refer to S0048, S0049, S0052, S0056, S0068, S0080, S0087, S0101, S0113, S0122, S0126, S0135, S0148, S0152 and S0156 of Annex 4.

132 Please refer to S0123, S0166 and S0168 of Annex 4. Moreover, the Hong Kong Information Technology Federation (S0138) remarks that the proposal would create significant uncertainty, as businesses will not necessarily know when particular behavior becomes criminal. It is particularly concerned about the adverse effect that criminalisation would have on IT industry, where businesses are often engaged in new or innovative activities.

133 Please refer to S0124 of Annex 4.

should be fully justified. It is opined that the Government should consider strengthening the enforcement of the PDPO to increase its overall deterrent effect rather than enacting a new criminal offence[134].

3.19.10 A respondent who has no comments on the proposal also expresses the concern mentioned in point (b) above[135].

Proposed Way Forward

3.19.11 Although the PCPD has not come across any cases of circumvention as described above, as seen from the series of data leakage incidents, cases of repeated contravention of DPPs are possible. As the enforcement notice is couched in more specific terms than DPPs, it would not be moving away from the original intent of adopting the DPPs to make resuming the same contravening act or practice intentionally after compliance with an enforcement notice an offence. Therefore, we intend to implement this proposal.

3.19.12 On penalty, although repeated contraventions of DPPs are not as serious as a breach of enforcement notice because there would be no element of directly flouting a requirement imposed by the PCPD to a certain extent, it can be regarded as making use of the loopholes in the existing provisions to avoid regulation if the data user intentionally resumes the same act or practice that contravenes the DPPs after compliance with an enforcement notice. To deter those acts effectively, we propose that the penalty should be the same as that for breaching an enforcement notice, i.e. liable to a fine at Level 5 ($50,000) and imprisonment for two years upon conviction.

---

134 Please refer to the following extract of the minutes of special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009: "Dr Margaret NG said that in creating a new offence, one must abide by the basic legal principle of making specific the offence clear and with full justification in order to prevent injustice. While the enforcement of PDPO might not be satisfactory, measures to step up enforcement actions, instead of imposing more penalties, creating criminal offences and conferring more power on the Commissioner, could be an answer to the problem."

135 The Hong Kong Chamber of Small and Medium Business Ltd. (S0136) is of the opinion that "repeated contravening acts" should be clearly defined and provide strong support to small and medium enterprises.

(19) Repeated Non-compliance with Enforcement Notice (Proposal No. 11 in the Consultation Document)

Proposal in the Consultation Document

3.20.1 The proposal examines whether heavier penalty should be imposed on data users for repeated non-compliance with enforcement notice.

3.20.2 At present, according to the PDPO, if the PCPD, following the completion of an investigation, is of the opinion that a data user is contravening a requirement under the PDPO (including the DPPs), or has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated, the PCPD may, having considered the damage or distress to the data subject caused by the contravention, serve on the relevant data user an enforcement notice to direct him to take such steps as are specified in the notice to remedy the contravention. It is an offence under section 64(7) of the PDPO for a data user to contravene an enforcement notice issued by the PCPD. On conviction, the data user is liable to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000. However, the PDPO does not provide for heavier sanction for repeated offenders.

3.20.3 As pointed out in the consultation document, various pieces of local legislation also impose heavier penalty for repeated offenders. It is also pointed out that since the enactment of the PDPO, the problem with repeated offenders has not been serious and no data user has been prosecuted more than once for contravention of an enforcement notice.

3.20.4 The consultation document invited comments from the public on whether heavier penalty should be imposed for repeated offenders, and on the appropriate penalty level.

Views Received

3.20.5 Nearly 40% of the submissions received commented on this proposal. Over half supported the proposal, some objected to it, and the rest did not clearly indicate their stand. In the various consultation activities, only a small number of

participants commented on this proposal.

3.20.6 Those who are supportive of this proposal consider that it could strengthen the deterrent and regulatory effects of the PDPO[136]. In addition, some respondents put forth other reasons for supporting the proposal, including:

- unlike DPPs, an enforcement notice states clearly and specifically the contravening act or practice and also the remedial steps to be taken. A data user who has repeatedly contravened enforcement notice should be subject to heavier penalty[137]; and

- as various pieces of local legislation also impose heavier penalty for repeated offenders, this proposal would not set a precedent. Given the prevalence of direct marketing activities and that repeated offenders demonstrate their lack of remorsefulness, the Office of the PCPD also finds it justifiable to impose heavier penalty[138].

3.20.7 However, some respondents who are supportive of the broad direction of the proposal suggest that the proposal should only target intentional and malicious circumvention of the regulatory regime[139].

---

136 Please refer to S0005, S0060, S0073, S0074, S0089, S0121, S0134, S0151, S0157, S0162 and S0165 of Annex 4.

137 For example, Freshfields Bruckhaus Deringer (S0087) expresses the view that an enforcement notice will give specificity to the unlawful conduct at issue and give advance written notice of an intention to prosecute the conduct should the remedial steps not be taken within the time specified in the notice. An offence crafted on this basis would therefore provide a fair and justifiable basis for bringing a prosecution.

138 Please refer to S0097 and S0135 of Annex 4.

139 The Society of Operations Engineers (Hong Kong Region) (S0131) suggests that the Government should consider offering an exception or flexibility to the non-profit-making society when imposing heavier penalty for the repeated non-compliance with an enforcement notice as they may lack of comprehensive data control tools or resources. However, in the public consultation activities, some participants expressed the opposite view, saying that many non-commercial organisations (such as owners' incorporations and district organisations) were also in possession of a large amount of personal particulars of members of the public, and the harm done to the data subjects by misuse of such data by such organisations would be no less serious than the nuisance caused by commercial promotion activities. As such, they suggested that non-commercial organisations should also be covered by the regulation.

3.20.8 On the penalty level, only a few respondents express their views. Some suggest that the fine should be doubled (i.e. $100,000 on conviction and in the case of a continuing offence, a daily fine of $2,000), while the term of imprisonment should remain to be two years[140]. A respondent proposes a fine of $500,000[141], while another proposes raising the daily fine to $5,000[142]. There is also a view that the appropriate level of penalty should be decided by the court[143].

3.20.9 Those who object to this proposal mainly hold the view that since the enactment of the PDPO, the problem with repeated offenders has not been serious and thus it is not necessary to introduce an additional offence[144]. Separately, a respondent expresses the view that with technological advances, the enforcement notice issued by the PCPD might not be able to fully remedy a contravening act or practice. Therefore, the respondent considers that not all cases of repeated non-compliance with enforcement notice should be made an offence, and each case should instead be dealt with on an individual basis[145].

Proposed Way Forward

3.20.10 Over half of the submissions support the implementation of this proposal. The comments received generally agree that the wording of an enforcement notice is specific and concrete enough to specify clearly the contravening act or practice concerned. They also agree that if a data user has repeatedly committed an offence, it is fair and proper to impose on him heavier penalty, which is in line with the practice of many other

---

140 Please refer to S0122 and S0148 of Annex 4.

141 Please refer to S0124 of Annex 4. In addition, Baker & McKenzie (S0124) proposes that a defence provision should be provided to data users who can prove that he has exercised all due diligence to comply with the enforcement notice.

142 Please refer to S0102 of Annex 4.

143 The Society for Community Organisation (S0132) suggests that the court could consider the following factors when considering the sentence: the duration of contravening an enforcement notice, subsequent steps taken by the data user after the issuance of an enforcement notice, and the seriousness of the impact on the data owner as a result of the contravention.

144 Please refer to S0048, S0049, S0052, S0056, S0067, S0068, S0080, S0101, S0113, S0123, S0126, S0152 and S0156 of Annex 4.

145 Please refer to S0011 of Annex 4.

pieces of local legislation (such as the UEMO and the Control of Obscene and Indecent Articles Ordinance ("COIAO") (Cap. 390)).

3.20.11 Therefore, we intend to implement this proposal, and amend the PDPO by adding a new provision to impose heavier penalty for repeated contravention of section 64(7) of the PDPO.

3.20.12 As to the penalty level, some other local legislation such as the COIAO imposes doubled fine on repeated offenders with the same term of imprisonment (i.e. 12 months). Under the PDPO, the existing penalty for a data user who has contravened an enforcement notice issued by the PCPD is, on conviction, a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000. We recommend for consideration that for repeated non-compliance, a heavier fine could be imposed with the same term of imprisonment, i.e. a fine at Level 6 ($100,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $2,000.

Rights of Data Subjects

(20) Third Party to Give Prescribed Consent to Change of Use of Personal Data
(Proposal No. 13 in the Consultation Document)

Proposal in the Consultation Document

3.21.1 The proposal examines whether there is a need to devise a system which empowers a specified third party to give consent to the change of use of personal data of certain classes of data subjects (such as mentally incapacitated persons or minors) when it is in their best interests to do so.

3.21.2 There is no provision in the PDPO to permit a person to give consent on behalf of a data subject to the change of use of the latter's personal data. To safeguard the vital interests of vulnerable classes of data subjects, particularly in connection with the provision of essential services such as healthcare, education and social services, it was proposed in the consultation document that consideration might be given to devising a mechanism which would allow a third party to give

prescribed consent[146] on behalf of a data subject to change the use of the personal data of the data subject concerned on condition that :

(a) the data subject is incapable of giving prescribed consent as he does not have a sufficient understanding or does not have the intelligence which enables him to fully understand what is being proposed to him; and

(b) the proposed use of the personal data involves a clear benefit to the data subject.

3.21.3 To guard against abuse, a data user is required to make necessary enquiries to form a reasonable belief that both conditions are fulfilled. Otherwise, the data user may have contravened the requirements of the PDPO.

3.21.4 As regards the definition of "third party", it was proposed in the consultation document that reference might be made to the definition of "relevant person" under the existing PDPO[147]. Nevertheless, the consultation document also pointed out the drawback of allowing only the relevant person to give consent to the change of use of personal data on behalf of a data subject. For example, in a situation where the data subject is entrusted to the care of other persons because the relevant person is untraceable, allowing only the relevant person to give prescribed consent under the legislation may pose difficulties for the data subject concerned to access essential services. Therefore, the meaning of the "third party" may need to cover the above entrusted parties.

---

146 According to section 2(3) of the PDPO, prescribed consent :
(a) means the express consent of the person given voluntarily;
(b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).

147 According to section 18(1) of the PDPO, a relevant personal on behalf of an individual may make a data access request to a data user. The term "relevant person" in relation to an individual is defined under section 2(1) of the PDPO to mean: (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. If Proposal (36) of this report is taken forward, the definition will be expanded to include the guardians of data subjects with mental incapacity, who are appointed under sections 44A, 59O, 59Q of the Mental Health Ordinance (Cap. 136).

3.21.5 The consultation document invited views on the mechanism of empowering a "third party" to give consent to the change of use of personal data of such classes of data subjects and the definition of "third party".

Views Received

3.21.6 More than 25% of the submissions received commented on this proposal. The majority were supportive of the need for the proposed empowering system, a small proportion expressed objection, and the rest made no clear indication of their preference. In other public consultation activities, no specific views were given by participants on this proposal.

3.21.7 While the majority of views support this proposal, quite a number of them suggest that additional conditions should be attached to give adequate protection to the data subject, such as ensuring, as far as reasonably practicable, that the change of use is in accordance with the wish and in the interest of the data subject[148].

3.21.8 On the definition of "third party", the majority of views support building it on the definition of "relevant person" under the PDPO[149]. While some agree that allowing only the relevant person to give consent to the change of use of personal data on behalf of a data subject would have the drawback mentioned in

---

148 For example, the Society for Community Organisation (S0132) proposes that a system should be devised to require the third party to inform the data subject of and as far as practicable consult the data subject on his decision to change the use of the latter's personal data and notify the Office of the PCPD of the same. Hong Kong Human Rights Monitor (S0157) suggests that a data user should be required to properly assess the capability of and consult the data subject before carrying out the instruction of the third party so as to ensure that it is in accordance with the data subject's wish; and that the third party could lodge an appeal with the Office of the PCPD if his request is refused by the data user. DAB (S0145) suggests that a data user should be required to ascertain that the change of use would not impose any criminal or civil liabilities on the data subject before carrying out the instruction of the third party. Please also refer to S0102 and S0126 of Annex 4.

149 Please refer to S0066, S0122, S0148 and S0162 of Annex 4. Besides, the Society for Community Organisation (S0132) reckons that regular review should be conducted on the person appointed as the third party to ensure his representativeness. It also proposes that an appeal system should be set up for the data subject if he is dissatisfied with the third party arrangement.

the consultation document[150], there are also concerns that over-expansion of the coverage would increase the risk of data leakage and make it difficult for data users to ascertain the identity of the "third party"[151].

3.21.9 On the proposal to require data users to make enquiries and ensure that the instruction of the "third party" meets the specified conditions, many respondents opine that it would impose additional burden on data users. As such, they suggest that in implementing the proposal, data users should be provided with adequate assistance and guidance[152] to minimise the impact on the daily operation of organisations.

3.21.10 Those opposing this proposal are concerned that the proposal requires a data user to determine whether a data subject is really incapable of giving prescribed consent and the proposed use of the personal data involved a clear benefit to the data subject when deciding whether to comply with the instruction of the third party. It is considered that this would put an onerous burden on data users. They also point out that it may not be appropriate for a general data user to determine whether the proposed use of the personal data will bring about a clear benefit to a data subject[153].

Proposed Way Forward

3.21.11 This proposal is generally supported by the respondents. We plan to implement this proposal and amend the PDPO

---

150 For example, in addition to the definition of "relevant person" in the PDPO, the Liberal Party (S0135) suggests that the definition of "third party" could be expanded to include other adult immediate family members of the data subject. The Official Solicitor's Office (S0161) suggests that consideration could be given to allowing other persons, such as the primary carer of the data subject, to give prescribed consent, having regard to the actual circumstances. The Hong Kong Family Welfare Society (S0099) suggests that suspected child abusers should be expressly excluded from the definition. Please also refer to S0079 and S0126 of Annex 4.

151 Please refer to S0119 and S0157 of Annex 4.

152 For example, the Law Society of Hong Kong (S0073) suggests that the PCPD should consider issuing a code of practice or guidelines to guide data users on the necessary enquiries required to be made before the data user could form a reasonable belief that the instruction of the third party met the specified conditions.

153 For example, the Hong Kong Association of Banks (S0068) expresses the view that protection of vital interest of the vulnerable individuals is not a privacy-related issue, and points out that, as they are already safeguarded under other existing laws, it is not appropriate to create a separate framework under the PDPO. Please also refer to S0080 of Annex 4.

accordingly.

3.21.12 As regards the coverage of the term "third party", in the light of the views received, we recommend that it should cover the definition of "relevant person" in the PDPO, that is :

(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.

In addition, if Proposal (36) of this report (on expanding the definition of "relevant person") is implemented, the definition of "relevant person" will be expanded to include the guardians of data subjects with mental incapacity appointed under sections 44A, 59O and 59Q of the Mental Health Ordinance.

3.21.13 As regards whether the definition of the "third party" should be further expanded to cover other people entrusted to take care of the data subjects concerned, to avoid increasing the chance of leakage of personal data, we do not plan to expand the coverage at this stage.

3.21.14 Taking into account the concerns expressed by some respondents, apart from amending the PDPO to implement this proposal, we will consider discussing with the Office of the PCPD the preparation of a code of practice or guidelines for data users on how to make enquiries to determine whether the instruction of the third party fulfills the specified conditions, with a view to alleviating the burden that the proposed system may impose on data users as far as possible.

(21) Access to Personal Data in Dispute (Proposal No. 15 in the Consultation Document)

Proposal in the Consultation Document

3.22.1 The proposal examines whether a provision should be added to the PDPO that, where the lawfulness of a refusal to comply with a data access request is in dispute before the AAB, a court or a magistrate, the relevant personal data should not be disclosed to

the data requestor and other parties bound by the decision of AAB, the court or magistrate, whether by discovery or otherwise, pending a determination in favour of the requestor.

3.22.2 Under the PDPO, a data subject might lodge a complaint with the PCPD against a data user who failed to comply with the data subject's request to access his own personal data. In the course of enquiry or investigation, the PCPD may request production of the requested data and may keep a copy of the requested data for record. After the PCPD has made a decision, the aggrieved party may lodge an appeal with the AAB or apply for a judicial review.

3.22.3 Under the AAB Ordinance (Cap. 442), save for documents for which a claim to privilege against disclosure is made, the PCPD as the respondent is obliged to give description of every document that is in his possession or under his control which relates to the appeal (including the document which contains the requested data) to the AAB Secretary, the appellant and the person(s) bound by the decision appealed against.

3.22.4 The standing instruction made by the AAB would normally require the PCPD to serve on the AAB, the appellant and the person(s) bound by the decision appealed against a copy of every document in the possession or under the control of the PCPD which includes a copy of the requested data. Where the aggrieved party applies for a judicial review, the parties to the proceedings would have a right to discovery of such documents. There is, however, no provision in the PDPO prohibiting the production of the requested data in the appeal or judicial review proceedings.

3.22.5 The disclosure mentioned above enables the complainant to obtain the requested data before the case is heard by the AAB or the court. This would mean that the complainant will already have had access to the requested data, even if the AAB or the court ultimately rules that the data user's refusal to comply with the data access request is lawful.

3.22.6 The UK Data Protection Act contains a provision prohibiting the court to require disclosure of the document containing the personal data in dispute to the applicant by way of discovery or otherwise, pending determination of the dispute in the

applicant's favour.

Views Received

3.22.7 Of the submissions received, more than 10% expressed views on this proposal. The majority of them supported the implementation of the proposal while a minority indicated that they had no comment. During the consultation activities, no participants expressed clear standpoint on this proposal.

3.22.8 Respondents supporting this proposal agree to the proposed arrangement set out in the consultation document[154] and opine that the proposal could plug the procedural loophole whereby people could obtain the requested data by appealing to the AAB or applying for judicial review[155].

3.22.9 On the other hand, a respondent considers that certain flexibility should be kept when implementing the proposed amendment. Disclosure of information should not be prohibited across the board[156].

Proposed Way Forward

3.22.10 Views received in general support the implementation of this proposal. We propose to suitably amend the PDPO, to prohibit the disclosure of document containing the data in dispute to the data requestor and other parties bound by the decision of AAB, the court or magistrate by way of disclosure or otherwise before the AAB, the court or magistrate determines in favour of the applicant.

---

154 Please refer to S0048, S0049, S0062, S0073, S0097, S0101, S0124, S0151 and S0162 of Annex 4. The Society for Community Organisation (S0132) supports following the UK Data Protection Act in prohibiting the disclosure of document containing the data in dispute to the applicant by way of disclosure or otherwise before the court rules in the applicant's favour.

155 For example, PCCW (S0066) and the Hong Kong Association of Banks (S0068) opine that implementation of this proposal could prevent the abuse of the appeal mechanism. Moreover, the Internet Professional Association (S0148) points out that this proposal can effectively prevent the data requestor from accessing the requested data through the appeal procedure even if it is ultimately ruled that the data user's refusal to comply with the data access request is lawful.

156 Hong Kong Human Rights Monitor (S0157) points out that disclosure based on other reasonable grounds should be allowed.

Rights and Obligations of Data Users

(22) Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation (Proposal No. 16 in the Consultation Document)

Proposal in the Consultation Document

3.23.1 The proposal examines whether a provision should be added where 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.

3.23.2 At present, under section 19 of the PDPO, a data user is required to comply with a data access request after receiving that request. However, a data user may refuse to comply with a data access request subject to various grounds for refusal specified in sections 20 and 28(5).

3.23.3 However, these grounds for refusal do not cover the situation where a data user is bound by a statutory secrecy requirement or entitled to a statutory right to non-disclosure. A data user bound by a statutory duty to maintain secrecy ("secrecy requirement") will face a dilemma of either breaching the data access provision of the PDPO or the relevant secrecy provision in another ordinance. On the other hand, the PCPD's decision may be challenged if he accepts a data user's compliance with a statutory secrecy requirement or a statutory right to non-disclosure as a ground for refusing a data access request.

3.23.4 A number of local ordinances impose a statutory duty of "secrecy" or a duty not to disclose information[157]. To solve the abovementioned problem, the consultation document suggested considering the provision of a new ground for a data user to refuse to comply with a data access request under section 20(3) where the data user was obliged or entitled under any other ordinances not to disclose the personal data.

3.23.5 The personal data privacy legislation of Australia, New Zealand and the UK has similar exemption clauses.

---

[157] For example, section 74 of the Sexual Discrimination Ordinance (Cap. 480) and section 15 of The Ombudsman Ordinance (Cap. 397).

Views Received

3.23.6 Of the submissions received, nearly 15% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while an individual submission expressed objection. During the various consultation activities, no participants expressed any clear standpoint on this proposal.

3.23.7 Respondents supporting this proposal all agree with the proposed arrangement put forward in the consultation document[158] and they consider that this proposal can save the data user from the dilemma of either contravening the provisions in the PDPO on data access or the relevant secrecy provision in another ordinance[159]. There are also views suggesting that when the proposal is implemented, care should be taken to ensure that the relevant legislative amendments will not contradict the provisions in other ordinances[160].

3.23.8 A respondent who opposes this proposal points out that if disclosure is already prohibited under other ordinances, non-disclosure should be maintained (including disclosure to the PCPD). Therefore, there will not be any dilemma. It is hence not necessary to implement the proposal[161].

Proposed Way Forward

3.23.9 Views received support the implementation of this proposal in general. We will make reference to relevant local legislation and overseas personal data privacy laws and make relevant amendments to the PDPO, so that data users would not need to

---

158 Please refer to S0048, S0049, S0062, S0073, S0080, S0097, S0101, S0113, S0123, S0124, S0151, S0156, S0162 and S0178 of Annex 4. The Society for Community Organisation (S0132) supports following overseas personal data privacy laws to include exemption clauses and specifying that any dispute should be brought to the court for ruling. PCCW (S0066) supports the implementation of the proposal and proposes that the exemption should not only be restricted to obligations under PDPO, but should be extended to rules and regulations imposed by regulators in different industries.

159 Please refer to S0148 and S0157 of Annex 4.

160 Please refer to S0068 of Annex 4. On the other hand, Hong Kong Human Rights Monitor (S0157) proposes that the Administration should consider the need to amend the secrecy provisions in existing legislations to set out grounds for defence allowing reasonable disclosure of personal data apart from setting out exemption clauses under the PDPO.

161 Please refer to S0011 of Annex 4.

comply with the data access requirement when there are other statutory requirements on non-disclosure.

(23) Response to Data Access Requests in Writing and within 40 Days (Proposal No. 19 in the Consultation Document)

Proposal in the Consultation Document

3.24.1 The proposal examines (a) whether a data user should be required to inform a requestor in writing if he does not hold the requested personal data, save for a request related to criminal conviction record data which the Police does not hold, in which case the Police can make the response orally; and (b) whether a data user should be required to inform a requestor within 40 days if he does not hold the personal data for which a copy of the personal data is requested, irrespective of whether the response is in written or verbal form.

3.24.2 At present, a data subject or a relevant person (see footnote 147) may make a data access request to a data user under section 18(1) of the PDPO. Section 19(1) requires a data user to comply with a data access request within 40 days after receiving the request. However, if the data user does not hold the data, there is no explicit provision in the PDPO requiring the data user to inform the requestor in writing of this.

3.24.3 Separately, at present, in handling personal data access requests in respect of criminal conviction records, the Police will only orally advise the requestor if he has a clear record. This practice is underpinned by rehabilitation considerations for ex-offenders as well as concerns about possible forgery of / unauthorised alterations to documents issued by the Police to confirm a clear record. If the requirement for a written response also applies to such requests, citizens who cannot produce clear criminal conviction records may be labelled as "underclass" citizens. This will deal a serious blow to the rehabilitation of ex-offenders. In view of this, the consultation document put forward one option for consideration, i.e. to exempt the Police from the requirement of giving a written response on clear record in respect of a request for access to criminal conviction record data, and a verbal response could be given instead.

Views Received

3.24.4 Of the submissions received, more than 10% expressed views on this proposal. The majority supported the implementation of the proposal while some of them raised objection. Some individual respondents did not express any clear standpoint. During the consultation activities, some individual participants expressed their views on this proposal.

3.24.5 Respondents supporting this proposal all agree that this proposal could strengthen communication between the data user and the data subject[162]. Most of them also support exempting a written response by the Police in respect of a request related to criminal conviction record data which the Police does not hold[163]. Some are of this view because otherwise, every employer may require every job applicant to provide a copy of a clear record and the Police will perform the screening function for the employers. This will unnecessarily increase the day-to-day workload of the Police and affect the livelihood of existing employees.

3.24.6 However, a respondent supporting this proposal opines that prevention of forgery should not be a ground to provide exemption to the Police. Forgery of document is an offence to be dealt with separately. Requests that should be replied in written form should not be dealt with orally simply to prevent forgery[164]. Some respondents object to implementing this proposal because they do not think an exemption should be granted to the Police[165].

Proposed Way Forward

3.24.7 Views received in general support the proposal mentioned in paragraph 3.24.1 above. We intend to implement this proposal and make corresponding amendments to the PDPO, i.e. a data

---

[162] Please refer to S0068, S0073, S0080, S0097, S0104, S0124, S0151, S0156, S0157 and S0162 of Annex 4. However, there is an individual comment that the limit of 40 days is too long. It should be changed to 4 days or even 48 hours. For details, please refer to S0011 of Annex 4.

[163] Please refer to S0068, S0073, S0080, S0104, S0124, S0151, S0156 and S0157 of Annex 4.

[164] Please refer to S0132 of Annex 4.

[165] Please refer to S0048, S0049 and S0101 of Annex 4.

user should be required 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 exempt from complying with the requirement of replying in writing, though it will still be required to make a verbal response within 40 days.

(24) Contact Information about the Individual who Receives Data Access or Correction Requests (Proposal No. 43 in the Consultation Document)

Proposal in the Consultation Document

3.25.1 The proposal examines whether 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.

3.25.2 DPP 1(3) requires a data user to provide the name of the person to whom a person may lodge a data access or correction request. As there may be personnel changes over time, it may be more practicable to provide an alternative way of compliance by allowing the data user to give the post title of the responsible person instead.

Views Received

3.25.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal[166] while some indicated that they had no comment. No respondents raised objection. During the consultation activities, no participants had a clear standpoint on this proposal.

Proposed Way Forward

3.25.4 Views received support this proposal in general. We intend to implement the proposal 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.

---

166 Please refer to S0011, S0048, S0049, S0062, S0068, S0073, S0080, S0097, S0101, S0151, S0156 and S0157 of Annex 4.

(25) Erasure of Personal Data (Proposal No. 17 in the Consultation Document)

Proposal in the Consultation Document

3.26.1 The proposal examines whether section 26 of and DPP 2(2) in Schedule 1 to the PDPO, which impose an absolute duty on a data user to erase obsolete personal data[167], should be amended to the effect that the requirement concerned would be regarded as having been complied with, if a data user can prove that he has taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use.

3.26.2 It was mentioned in the consultation document that whilst timely erasure of obsolete personal data was important, any PDPO requirements should not pose an excessive burden on businesses. In a number of overseas jurisdictions (including Australia, Canada, New Zealand and the UK), data users are generally regarded to have fulfilled similar requirements by taking reasonably practicable steps to erase obsolete personal data.

Views Received

3.26.3 Of the submissions received, more than 15% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while the rest did not have a clear standpoint. During the consultation activities, only individual participants expressed their views on this proposal.

[167] Under section 26 of PDPO, a data user shall erase personal data held by it where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless such erasure is prohibited under any law or it is in the public interest (including historical interest) for the data not to be erased. DPP 2(2) also requires that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3.26.4 Respondents supporting this proposal consider that this proposal can alleviate the burden of the data users and has social and economic benefits[168].

3.26.5 A few respondents express other views on the erasure of personal data. Some opine that data users should not keep personal data indefinitely. A respondent suggests a time limit of 5 to 7 years[169]. However, there is also opinion that this should be handled by the data users according to different circumstances and a rigid time limit should not be set[170].

Proposed Way Forward

3.26.6 Views received support this proposal in general. We propose to implement this proposal and make corresponding amendments to 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.

(26) Duty to Prevent Loss of Personal Data (Proposal No. 41 in the Consultation Document)

Proposal in the Consultation Document

3.27.1 The proposal examines whether 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.

3.27.2 DPP 4 (security of personal data principle) states that a data user should take all reasonably practicable steps to ensure that personal data held by him are protected against unauthorised or

---

168 Please refer to S0048, S0049, S0052, S0062, S0073, S0080, S0097, S0101, S0113, S0124, S0132 and S0162 of Annex 4. Also, the Hong Kong Investment Funds Association (S0056) suggests that the provision should further stipulate that, in respect of personal data the erasure of which is not reasonably practicable, the relevant requirement would be regarded as fulfilled if the data user can prove that he has taken all reasonably practicable steps to put the data in question in safe storage. The Working Group on Legal, Privacy and Security Issues of the Steering Committee on Electronic Health Record Sharing ("eHR Working Group") (S0156) also agrees to the proposal and proposes to amend section 26(1)(b) of the PDPO to explicitly exempt those related to public medical care.

169 Please refer to S0100 of Annex 4.

170 Please refer to S0151 of Annex 4.

accidental access, processing, erasure or other use. Although the legislative intent is to require data users to take similar security measures to prevent loss of personal data, this requirement has not been made explicit in the current provisions. This proposal aims to clarify the relevant provisions to reflect the legislative intent more clearly.

Views Received

3.27.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while a minority raised objection. Some others indicated that they had no comment. During the consultation activities, no participants expressed a clear standpoint on this proposal.

3.27.4 Respondents who support this proposal agree with the analysis in the consultation document and consider it necessary to amend DPP 4 to reflect more clearly the legislative intent[171]. A respondent comments that the meaning of "loss" is not clear in the proposal and considers it not necessary to change the existing mechanism[172].

Proposed Way Forward

3.27.5 Views received in general support this proposal. We intend to implement the proposal and 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.

Introducing New Exemptions

(27) Transfer of Personal Data in Business Mergers or Acquisition (Proposal No. 24 in the Consultation Document)

Proposal in the Consultation Document

3.28.1 The proposal examines whether an exemption from DPP 3 should be provided for the transfer or disclosure of personal

---

171 Please refer to S0011, S0048, S0049, S0073, S0097, S0101, S0151, S0157 and S0175 of Annex 4.

172 Please refer to S0068 of Annex 4.

data in intended merger, acquisition or transfer of businesses subject to certain conditions.

3.28.2 During the due diligence stage of merger, amalgamation, transfer or sale of businesses, business information which may contain personal data held by one party may have to be disclosed or transferred to another party for examination and evaluation. Where such use of personal data does not fall within the original or directly related purpose of collection, the transfer of personal data in the absence of prescribed consent of the data subjects would be inconsistent with DPP 3 (use of personal data principle). However, obtaining prescribed consent prior to the transfer will pose a hurdle to merger or acquisition activities which are very often time sensitive. Moreover, there may be a genuine need to keep the transaction confidential at the due diligence stage.

3.28.3 The personal data privacy laws of Australia and New Zealand contain specific provisions permitting transfer of personal data to cater for sale, merger or amalgamation of business.

3.28.4 Any proposals regulating the transfer of personal data in business merger or acquisition must have regard to both the protection of personal data privacy interests of the data subjects concerned and the business interests in general. The consultation document put forward a possible option, which is to exempt personal data used in the process of a merger, acquisition or transfer of business from DPP 3 on condition that:

(a) the service to be provided to the data subjects by the resultant organisation or the business transferee will essentially be the same as or similar to that provided by the original data user who holds the data;

(b) it is not practicable to obtain the data subjects' prescribed consent for such a use;

(c) personal data thus disclosed is necessary but not excessive for the due diligence purpose;

(d) the transferee shall only use and process the personal data within the confines of the restricted purpose of due diligence unless the prescribed consent of the data subject(s)

is obtained or the use of the personal data is otherwise permitted or exempt under the PDPO;

(e) personal data so transferred must be properly destroyed or returned to the transferor if the transaction is not proceeded with or not completed; and

(f) the exemption will not apply to business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of personal data.

3.28.5 To prevent abuse, the consultation document suggested that consideration might be given to imposing a fine for contravention of the requirements on the retention and restriction on the use of personal data mentioned in (d) and (e) above.

3.28.6 The consultation document invited public comments on the option set out in paragraphs 3.28.4 to 3.28.5 above.

Views Received

3.28.7 Of the submissions received, more than 10% expressed views on this proposal. All of them supported the implementation of the proposal. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.28.8 Respondents supporting this proposal agree that the proposal would be beneficial to business operations and development. It would also be in the economic interest of the community[173]. For the conditions set out in paragraph 3.28.4, they are generally considered reasonable and agreeable[174]. Some respondents comment on individual items[175]. For example,

---

[173] Please refer to S0073, S0080, S0087, S0097 and S0152 of Annex 4.

[174] Please refer to S0062, S0073, S0132, S0151 and S0162 of Annex 4.

[175] For example, the Hong Kong Association of Banks (S0068) considers that condition (a) is sufficient. Moreover, regarding condition (a), Hong Kong Human Rights Monitor (S0157) proposes to specify that the level of service provided should not be lower than the original one. The Consumer Council (S0126) proposes to add one condition that the personal data should be transferred on an anonymous basis. Baker & McKenzie (S0124) considers that the proposed conditions are too restrictive and conditions (b) and (c) introduce a subjective element to the exemption. Please also refer to S0113 of Annex 4.

there is a comment that it would be sufficient to make item (a) the only condition.

Proposed Way Forward

3.28.9 The views received generally support this proposal. We intend to implement this proposal and make corresponding amendments to the PDPO. An exemption from DPP 3 will be granted for the transfer or disclosure of personal data in merger, acquisition or transfer of businesses if the conditions (a) to (f) set out in paragraph 3.28.4 are met. In addition, as merger and acquisition activities in general involve massive personal data of different people, to prevent abuse of the exemption and possible harm to data subjects, we propose to impose a fine at Level 5 (a maximum of $50,000) and imprisonment for two years for contravention of the requirements on the retention and restriction on the use of personal data mentioned in (d) and (e) of paragraph 3.28.4 above.

(28) Provision of Identity and Location Data on Health Grounds (Proposal No. 25 in the Consultation Document)

Proposal in the Consultation Document

3.29.1 This proposal involves the scope of application of the exemption under section 59 of the PDPO. Under section 59, data in relation to the physical or mental health of a data subject are exempt from the use of personal data principle (DPP 3) and access to personal data principle (DPP 6) if the application of these provisions to the data would likely cause serious harm to the physical or mental health of the data subject or any other individual. However, the exemption would not apply to the supply of personal data relating to location and identity of the data subject.

3.29.2 The provision of personal data relating to the identity and the location of the data subject can facilitate immediate access and rescue actions. The personal data protection laws of the UK, Australia, New Zealand and Canada permit disclosure of any personal data where disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual.

3.29.3 The consultation document invited the public to comment on the proposal to amend section 59 of the PDPO to broaden the scope of application of exemption to cover personal data relating to the identity and location of the data subject.

Views Received

3.29.4 Of the submissions received, more than 10% expressed views on this proposal. The majority of them supported the implementation of the proposal while the rest of them did not have any comment. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.29.5 Respondents supporting this proposal all agree with the analysis in the consultation document and consider that there is a need to implement the proposed amendment to allow the disclosure of personal data relating to the identity and the location of the data subject when necessary to provide immediate access to the data subject and conduct rescue actions, so as to prevent or lessen a serious threat to the life or health of an individual [176]. Moreover, a respondent supporting the implementation of this proposal suggests limiting such exemption to extreme emergency to prevent abuse of the exemption mechanism[177].

Proposed Way Forward

3.29.6 Views received support this proposal in general. We intend to implement this proposal and make corresponding amendments to the PDPO to broaden the scope of application of exemption under section 59 to cover personal data relating to the identity and location of the data subject.

3.29.7 Regarding the proposal of limiting such exemption to extreme emergency raised by a respondent, we do not intend to follow up on this as section 59 of the PDPO has already clearly specified that the exemption is only limited to cases where

---

[176] Please refer to S0011, S0048, S0049, S0080, S0097, S0101, S0132, S0151, S0156, S0157, S0162, S0166, S0175 and S0178 of Annex 4. Moreover, the Law Society of Hong Kong (S0073) supports implementing this proposal because the benefits brought about by the disclosure outweighed the impact on the personal data privacy of the data subject.

[177] The Hong Kong Family Welfare Society (S0099) proposes that the exemption should be restricted to extreme circumstances where public bodies (such as the Police) become involved to deal with emergencies or crisis.

serious harm would likely be caused to the physical or mental health of the data subject or any other individual.

(29) Handling Personal Data in Emergency Situations (Proposal No. 26 in the Consultation Document)

Proposal in the Consultation Document

3.30.1 The proposal examines whether it should be specified that in the handling of emergency or catastrophic situations, exemption from DPP 1(3)[178] and DPP 3[179] will be granted to LEAs, rescue and relief agencies, and organisations and individuals holding relevant personal data of individuals involved or maybe involved in the situations.

3.30.2 The existing exemption provisions under the PDPO cannot fully cover the handling of personal data in emergency or catastrophic situations where victims or missing persons require immediate assistance and rescue. Unless specific exemptions under section 58 (crime, etc.) and section 59 (health) apply, LEAs as well as rescue and relief agencies can only share personal data the use of which for accident or emergency rescue was envisaged at the time of their collection. The same applies to the provision of personal data by third parties to these agencies.

3.30.3 At an initial stage of an emergency rescue operation, LEAs/rescue agencies need to ascertain who are involved in the accident, locate missing persons and verify unconfirmed identities of persons who are in distress. These agencies may need to collect personal data from the involved individuals, or approach organisations or individuals holding relevant personal data to assist in rescue related work. Exemption from DPP 1(3) and DPP 3 would facilitate these operations and be in the interest of the victims.

---

[178] DPP 1(3) states that where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that he is informed of the purpose for which the data are to be used and the classes of persons to whom the data may be transferred.

[179] DPP 3 states that personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than (a) the purpose for which the data were to be used at the time of the collection of the data; or (b) a purpose directly related to the purpose referred to in paragraph (a).

3.30.4 For the sake of protecting personal data privacy, in granting such exemption, the permitted purposes of use, the duration and restrictions imposed regarding the use of personal data under emergency or catastrophic situation have to be specified clearly to contain the risk of improper or unauthorised handling of personal data.

3.30.5 The consultation document proposed that in any case related to rescue and relief work by LEAs and rescue and relief agencies, consideration could be given to exempting these agencies and organisations and individuals holding relevant personal data from the DPP 1(3) and DPP 3 to:

(a) identify individuals who are or may reasonably be suspected to be involved in an accident or other life-threatening situations;

(b) inform family members of the individuals under (a) of the latter's involvement in the accident, etc; and

(c) generally to facilitate the provision of rescue or relief services to the individuals under (a).

Views Received

3.30.6 Of the submissions received, more than 15% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while the rest indicated that they had no comment. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.30.7 Respondents supporting this proposal all agree to the analysis of the consultation document and consider that it is necessary to implement the proposal to facilitate the carrying out of rescue and relief missions[180]. Moreover, some respondents agreeing to the implementation of the proposal suggest that such exemption should be limited to emergency or catastrophic situation and the relevant amendment should specify the permitted purposes of use, the duration and restrictions imposed regarding the use of personal data under the emergency or

[180] Please refer to S0001, S0011, S0048, S0049, S0074, S0079, S0080, S0097, S0101, S0120, S0131, S0132, S0149, S0151, S0154, S0156, S0157, S0162, S0166, S0173, S0175 and S0178 of Annex 4.

catastrophic situation to prevent abuse of the exemption mechanism[181].

Proposed Way Forward

3.30.8 Views received generally support this proposal. We plan to implement this proposal and make corresponding amendments to the PDPO specifying that in the handling of rescue and relief work mentioned in paragraph 3.30.5 above by LEAs and rescue and relief agencies, specific exemption from DPP 1(3) and DPP 3 will be granted to these agencies and organisations and individuals holding relevant personal data. In drafting the legislative amendments, we will consider the suggestion regarding the prevention of abuse of the mechanism.

(30) Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship (Proposal No. 27 in the Consultation Document)

Proposal in the Consultation Document

3.31.1 The proposal examines whether an exemption under the PDPO should be provided to allow data users to transfer personal data of a minor that are relevant to parental care and guardianship to the parents or guardians of the minor.

3.31.2 The consultation document pointed out that, under section 18(1) of the PDPO, parents or guardians may access the personal data of their minor children held by data users. However, the PDPO does not allow data users to transfer or disclose, of their own accord, the personal data of minors to their parents or guardians, even if this is to the benefit of the minors concerned[182].

3.31.3 Currently, if the Police are satisfied that a minor will likely commit a crime, or will become a repeated offender, and that

---

[181] Please refer to S0073 of Annex 4. Also, the Liberal Party (S0135) points out that as a lot of the personal data involved in relief missions, such as personal medical records, are sensitive, the scope of application of the exemption should be limited. For example, it could be limited to situations such as accidents or life-threatening circumstances to prevent abuse.

[182] DPP 3 of the PDPO provides that, without the prescribed consent of the data subject, personal data shall not be used for any purpose other than the purposes for which they were collected or for a directly related purpose. Under the PDPO, the meaning of "use" in relation to personal data includes "disclose" and "transfer".

the knowledge of the parents or guardians of the matter will help prevent the committing of the offence, the Police can invoke the exemption under section 58 of the PDPO in relation to crime prevention, and transfer or disclose the relevant data to the parents or guardians of the minor. However, the exemption cannot be invoked in some cases[183], and this makes the transfer or disclosure of the relevant data not possible without the consent of the minor.

3.31.4 To help parents better fulfill their responsibility to exercise proper care and guardianship of their minor children, the consultation document proposed to give consideration to whether an exemption under the PDPO should be provided to allow data users to transfer personal data of minors to their parents or guardians; and if so, what specific conditions should be attached to restrict the transfer to cases which are absolutely necessary, such as :

(a) restricting the disclosure to minor "at risk" cases; and

(b) on condition that the transfer is in the best interests of the minor.

3.31.5 The consultation document invited public views on whether an exemption should be provided, and if so, what specific conditions should be attached.

Views Received

3.31.6 Of the submissions received, over 20% expressed views on this proposal. The majority agreed to the intent of this proposal to help parents to exercise care and guardianship of their minor children. However, a number of them had concerns about the detailed arrangements of the proposal. Those who opposed the proposal expressed worries about various details of the proposal. In various public consultation activities, respondents who commented on this proposal were mainly representatives of human rights concern groups and community service groups.

3.31.7 Some respondents who agree to the intent of this proposal have no comment on the arrangements raised for consideration in the

[183] See the example in paragraph 3.31.12 below.

consultation document[184]. However, some respondents have different views on the implementation details and put forward various observations and suggestions for revising the implementation arrangements. For example :

- the Office of the PCPD appreciates the rationale behind the proposal but opines that due account should be given to the type of exempted personal data, the degree of disclosure and the relevant circumstances at the material time so as to make the transfer of relevant data justifiable[185];

- some respondents agree to the intent of the proposal but consider that data users should consult the minors prior to data transfer under all practicable circumstances[186];

- to ensure adequate protection of personal data privacy of minors, the existing practice of transferring such data to parents by invoking the exemption under section 58 of the PDPO by the Police should remain unchanged. However, the threshold could be lowered slightly. If the Police have reasonable doubt that a minor might commit a crime, the exemption could be invoked[187];

- some respondents agree to restricting the exemption to minors in "at risk" cases, but some consider that the exemption should be applicable to all minors. Also, some suggest that the exemption should only be invoked under certain exceptional circumstances[188];

---

184 Please refer to S0003, S0040, S0092, S0105, S0161 and S0162 of Annex 4.

185 Please refer to S0097 of Annex 4. The Office of the PCPD also opines that a mechanism must be built in to guard against misuse and that it may be more appropriate to tackle the situation by way of other child protection laws. According to the Office of the PCPD's enquiry, there is no equivalent or similar exemption under overseas privacy legislation.

186 Please refer to S0011 and S0099 of Annex 4.

187 Please refer to S0073 of Annex 4.

188 For example, DAB (S0145) considers that the scope of exemption should include youths involved in drug abuse or serious crimes. On the other hand, the Society for Community Organisation (S0132) and the Liberal Party (S0135) suggest that personal data privacy of all minors should have the same level of protection and that minors should not be categorised as so-called minors "at risk" to prevent stigmatization. The Hong Kong Doctors Union (S0151) considers that the proposal should only be applicable to exceptional circumstances involving health or even life of the minor.

- regarding the requirement that the transfer of personal data must be in the best interests of the minors, some respondents support the proposal whilst some hold opposite views, opining that the wording "best interests" is ambiguous and should not be included as one of the considerations for data transfer to avoid unnecessary disputes[189]; and

- some respondents consider that if new provisions are introduced, some considerations should be included to enable data users to assess whether the data should be transferred to the parents[190].

3.31.8 Respondents who oppose this proposal raise the following points:

(i) they disagree with the proposal that even without consent of the minors, the data users may transfer the personal data to the parents on reliance of their unilateral judgments on the benefit of the minors. They opine that the wish of minors should be respected as far as possible. Unless there are strong justifications, the relevant proposal should not be implemented lightly as the relevant arrangements would seriously intrude into the personal data privacy of the minors[191];

(ii) there are already provisions under the existing PDPO which allow parents to access the personal data of the

---

189 For example, the Hong Kong Family Welfare Society (S0099) opines that the best interests of the minors should be one of the considerations for transfer of data. The Law Society of Hong Kong (S0073) opines that the interpretation of the wording would inevitably be subjective and would undermine the objective certainty of the provisions.

190 Please refer to S0132 of Annex 4.

191 Please refer to S0124 of Annex 4. Moreover, the Boys' and Girls' Club Association of Hong Kong (S0143) opines that the principle of respecting the wish of the children should be adhered to. If social workers (data users) consider that disclosure of personal data of minors to the parents would be to the benefit of the children, they would generally exercise their professional judgments and practices to encourage or motivate the children to notify their parents instead of transferring the personal data to the parents of their own accord without the consent of the children. The Hong Kong Human Rights Monitor (S0157) suggests that if the proposal is adopted, consideration should be given to require data users to submit application to the PCPD and empower the PCPD to decide whether to disclose the relevant data after seeking the agreement of the minors. The Democratic Party (S0178) suggests that the data user should first obtain the minor's consent if it is considered necessary to transfer his/her personal data to the parents or guardians.

minors held by data users. There is hence no need to provide exemption clauses[192];

(iii) there are views that the parents, to fulfill their responsibility to exercise proper care and guardianship of their children, should start with the establishment of long-term close and good parent-child relationship with their children rather than relying on the transfer of data in individual cases. The most fundamental and appropriate method is to establish mutual trust between parents and children so that parents are those whom children will want to talk to[193];

(iv) according to the proposal, data users need to judge whether the relevant data transfer is in the best interests of the minors. This would put onerous burden on data users[194]. The proposal also requires data users to provide, of their own accord, the personal data of minors to their parents. This would probably make the data users (e.g. medical healthcare practitioners) commit a breach of their relevant professional codes of confidentiality[195]; and

(v) there is criticism that the proposal in the consultation document to restrict the disclosure of the personal data of minors to minor "at risk" cases only would adversely label this group of youths as problem minors.

Proposed Way Forward

3.31.9 Most of the views received agree to the intent of this proposal to help parents to exercise care and guardianship of their minor children, though there are different views on the details of the proposal.

3.31.10 There are views that confining the exemption to only minors "at

---

192 Please refer to S0124 of Annex 4.

193 Please refer to S0079 and S0143 of Annex 4.

194 Baker & McKenzie (S0124) indicates that the data users may not be able to make an accurate assessment in respect of every case, and this could lead to errors and inconsistent treatment.

195 The eHR Working Group (S0156) indicates that the data users are concerned about whether the transfer of data would be exempt from relevant code of confidentiality, and if the minors expressly dissent to the relevant transfer of data, how the data users should handle the case.

risk" may lead to stigmatization and that the exemption should be applicable to all minors. There are also views that the scope of the exemption should be limited so as not to compromise the personal data privacy of minors as far as possible. There are also concerns that general data users may not have the ability to judge what constitute the best interests of minors.

3.31.11 Since most of the respondents agree to the intent of the proposal and the main difference in the views received is over the scope of the exemption, we intend to take forward the proposal but will confine the exemption to specific data users under special circumstances so as to strike a balance between the protection of the well-being and the personal data privacy of minors.

3.31.12 As set out in paragraph 3.31.3 above, there is a current exemption from the provisions of DPP 3 on the restricted grounds of preventing and detecting crimes that LEAs may make use of. There is scope for LEAs to further facilitate parents and guardians to exercise proper care and guardianship over their minor children who are obviously at risk but have not been caught committing crimes. For example, a 13-year old girl is found by the Police in a secluded area in problematic entertainment premises with drugs discarded onto the floor. While no drugs are found on the girl herself, all the circumstances may suggest that she may be involved in or vulnerable to becoming embroiled in drug taking or even trafficking.

3.31.13 In cases as such, notifying the parents/guardians may facilitate early identification of a hidden problem and enable necessary intervention to prevent the problem from further deteriorating. The boosting of such preventive efforts is especially important given the prevalence and hidden nature of drug abuse nowadays[196]. One particular feature of youth drug abuse is that in many cases, the abuser is well aware of the harm of drugs but continues to abuse drugs and evade parental attention. The balance is clearly in favour of protecting the minor's

[196] As the consumption methods and harmful effects of psychotropic substances (e.g. ketamine), which are prevalent among youths, are very hidden as opposed to those of heroin, it could be difficult for the parents or guardians to find out that the juvenile has drug abuse problem until he/she is caught for a drug-related offence or physical symptoms have gradually surfaced but by which time some damage may have become permanent.

physical and mental health and preventing self-destruction in his or her best interest.

3.31.14 Taking into account the views received, we propose to grant an exemption from the provisions of DPP 3 for personal data of minors under the following conditions :

(a) the transfer or disclosure of the data to the parents or guardians of the minor is to facilitate the latter to better discharge their responsibility to exercise proper care and guardianship, and is in the best interests of the minor; and

(b) the data are held by LEAs and are to be transferred or disclosed by LEAs to the parents or guardians of the minor.

(31) Use of Personal Data Required or Authorised by Law or Related to Legal Proceedings (Proposal No. 33 in the Consultation Document)

Proposal in the Consultation Document

3.32.1 The proposal examines whether an exemption from DPP 3 should be created for use of personal data required or authorised by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.

3.32.2 A data user may be required or authorised by or under law, or by the court to disclose information which may contain personal data. However, under DPP 3, personal data shall not be used for any purpose other than the original purpose of collection or its directly related purposes unless prescribed consent of the data subject is obtained. It is, therefore, necessary to create an exemption from DPP 3 for such use of personal data so that a data user would not run the risk of contravening DPP 3 in such circumstances.

Views Received

3.32.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the

implementation of the proposal[197] while some did not have any comment. No respondents expressed objection. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.32.4 A respondent supporting this proposal opines that the Administration should take into consideration that a data user may not have sufficient information to ascertain that the data concerned is required by legal proceedings[198].

Proposed Way Forward

3.32.5 Views received generally support this proposal. We intend to implement this proposal and make corresponding amendments to the PDPO to create an exemption from DPP 3 for use of personal data required or authorised by or under law, by court orders, or related to any legal proceedings in Hong Kong or is otherwise for establishing, exercising or defending legal rights.

3.32.6 In response to the opinion that a data user may not have sufficient information to ascertain that the information concerned is required by legal proceedings, we may help data users understand the requirements of the amended legislation through the public educational activities conducted by the Office of the PCPD.

(32) Transfer of Records for Archival Purpose (Proposal No. 34 in the Consultation Document)

Proposal in the Consultation Document

3.33.1 The proposal examines whether to create an exemption from DPP 3 for the transfer of records containing personal data of historical, research, educational or cultural interests to the GRS for archival purpose.

---

197 Please refer to S0062, S0067, S0073, S0097, S0151, S0156, S0157, S0161 and S0176 of Annex 4.

198 PCCW (S0066) suggests that, to address the issue, the Administration may consider relieving the data user from any liability if the data requestor is a member of the judiciary or a legal practitioner from a recognised jurisdiction.

3.33.2 To preserve Hong Kong's documentary heritage, it is necessary for Government bureaux and departments to transfer records of historical value, including those containing personal data, to the GRS for archival purpose. Transfer of such records has to comply with the requirements of DPP 3. Given the volume and variety of personal data in the records, it is not practicable to obtain the prescribed consent of each and every data subject before transferring the records to the GRS and some of the data subjects may not be traceable due to lapse of time.

3.33.3 This proposal aims to provide the necessary exemption from DPP 3 for the transfer of records containing personal data to GRS for archival purpose. Subsequent handling of the archival records containing personal data by GRS (including access to and use of records by members of public) will continue to be subject to the provisions of the PDPO.

Views Received

3.33.4 Of the submissions received, less than 10% expressed views on this proposal. The majority of them supported the implementation of the proposal while an individual submission raised objection. Some said that they had no comment. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.33.5 Respondents who support this proposal agree with the analysis in the consultation document and support creating an exemption from DPP 3 in the PDPO to allow for the transfer of records containing personal data of historical, research, educational or cultural interests to the GRS for archival purpose[199]. A respondent suggests that "for archival purpose" should be specifically defined[200]. Another respondent emphasises that the exemption should be limited to the transfer of records for archival purpose and that subsequent handling of the archival records containing personal data by the GRS will continue to be subject to the provisions of the PDPO[201].

---

199 Please refer to S0048, S0049, S0097, S0101 and S0151 of Annex 4. Also, Hong Kong Human Rights Monitor (S0157) suggests adding "recreational" as an exemption category.

200 Please refer to S0064 of Annex 4.

201 Please refer to S0011 of Annex 4.

3.33.6 The respondent who objects to this proposal considers that the exemption should only apply to personal data already made public. Records containing personal data that have not yet been made public should not be transferred to the GRS[202].

Proposed Way Forward

3.33.7 Views received in general support this proposal. We propose to implement this proposal to create an exemption from DPP 3 for the transfer of records containing personal data of historical, research, educational or cultural interests to the GRS for archival purpose. In drafting the exemption provision, we will clearly define the coverage and state that subsequent handling of the archival records containing personal data by the GRS (including access to and use of records by members of the public) will continue to be subject to the provisions of the PDPO.

(33) Refusal to Comply with a Data Access Request on Ground of Self-Incrimination (Proposal No. 35 in the Consultation Document)

Proposal in the Consultation Document

3.34.1 The proposal examines whether to create a new exemption for data users from complying with a data access request on the ground of self-incrimination.

3.34.2 Under common law, an individual has the fundamental right and privilege against disclosure of any information that may incriminate himself / herself. The PDPO, however, does not allow a data user to refuse to comply with a data access request on the ground that compliance with that request will incriminate himself / herself. The proposal serves to uphold the common law principle of privilege against self-incrimination.

---

202 Please refer to S0073 of Annex 4. The Law Society of Hong Kong (S0073) considers that the exemption is contrary to the spirit of the PDPO. Also, almost all records kept in the GRS archive are accessible to the public and so the data concerned would likely be disclosed using "public interest" as a reason.

Views Received

3.34.3 Of the submissions received, less than 10% expressed views on this proposal. The majority of them supported the implementation of the proposal while some said that they had no comment. Nobody raised objection. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.34.4 Respondents who support this proposal agree with the analysis in the consultation document[203] but there are views that the coverage of the exemption should be limited such that LEAs can conduct its investigation and seize evidence[204].

Proposed Way Forward

3.34.5 Views received in general support this proposal. We propose to implement this proposal to create a new exemption for data users from complying with a data access request on the ground of self-incrimination.

(34) Exemption for Personal Data Held by the Court or Judicial Officer (Proposal No. 39 in the Consultation Document)

Proposal in the Consultation Document

3.35.1 The proposal examines whether to add a new provision 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.

3.35.2 Personal data may be handled by the courts and judicial officers in the course of the exercise of judicial functions. However, the PDPO does not contain an express provision exempting such personal data from the application of the Ordinance.

---

[203] Please refer to S0048, S0049, S0062, S0068, S0097, S0101, S0151 and S0157 of Annex 4.

[204] Please refer to S0011 of Annex 4. Besides, the Law Society of Hong Kong (S0073) considers that the exemption should only apply to general access of data and should not be applicable where the request is made by a data subject accessing his/her own personal data. Baker & McKenzie (S0124) considers that it should be stated clearly whether the exemption is also applicable to body corporate.

Views Received

3.35.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority indicated that they had no comment, some supported the implementation of the proposal while one raised objection. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.35.4 Respondents who support this proposal agree with the analysis in the consultation document and consider that there is a need to implement the proposal 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[205].

3.35.5 A respondent who objects to this proposal sees no justifications to give blanket exemption to the court or judicial officer in the course of the exercise of judicial functions[206].

Proposed Way Forward

3.35.6 Article 85 of the Basic Law states that the courts of the Hong Kong Special Administrative Region shall exercise judicial power independently, free from any interference. Members of the judiciary shall be immune from legal action in the performance of their judicial functions.

3.35.7 There are similar exemptions in overseas privacy laws. For example, section 10 of the Information Privacy Act of Victoria, Australia gives exemption to a court, a tribunal or a registration authority and its staff members in the performance of judicial or quasi judicial duties in possession, control and use of personal information.

3.35.8 Views received generally accept this proposal. We intend to implement this proposal to add a new provision 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.

---

[205] Please refer to S0048, S0049, S0097, S0101, S0151 and S0157 of Annex 4.

[206] Please refer to S0073 of Annex 4. The Law Society of Hong Kong (S0073) considers the current exemptions in the PDPO specific and limited in scope. Without sufficient justifications for the proposal, it objects to granting full scale exemption to personal data held by the court or judicial officer in the course of the exercise of judicial functions.

Miscellaneous Proposed Amendments

(35) Definition of Crime under Section 58 (Proposal No. 36 in the Consultation Document)

Proposal in the Consultation Document

3.36.1 The proposal examines whether the word "crime" in section 58 of the PDPO should be defined to mean the following to clarify the scope of application of the exemption provision:

(a) a crime under the laws of Hong Kong, or

(b) a crime or offence under the law of a place outside Hong Kong, which has a legal or law enforcement cooperation arrangement with Hong Kong.

3.36.2 Under section 58(2) of the PDPO, personal data held for the purposes of the prevention or detection of crime, the apprehension, prosecution or detention of offenders are exempt from DPP 3 (use of personal data principle). It has not been clearly stipulated whether "crime" and "offenders" in section 58 have extraterritorial application. With the proposed amendment, LEAs under multilateral and bilateral cooperative agreements or arrangements may provide personal data to their overseas counterparts for criminal investigations or detection of crimes overseas. It would also enable assistance to be provided to foreign jurisdictions in verifying personal data in connection with requests for legal assistance.

Views Received

3.36.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal while a minority raised objection. Some indicated that they had no comment. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.36.4 Respondents who support this proposal agree with the analysis in the consultation document[207]. There are also views on the

[207] Please refer to S0073 and S0151 of Annex 4. Also, Yahoo! Hong Kong Limited (S0123) suggests that the term "LEAs" should be clarified as meaning "LEAs in Hong Kong" only.

proposed definition of "crime" in paragraph 3.36.1. In respect of item (a), there is a suggestion to change it to "an act or omission that is punishable as an offence under the laws of Hong Kong"[208] and in respect of item (b), to change it to "an act or omission for which legal assistance under the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525) has been sought and obtained". The Office of the PCPD points out that this Ordinance regulates the provision and obtaining of assistance in criminal matters between Hong Kong and places outside Hong Kong. Section 5(1)(g) of the Ordinance stipulates that "a request by a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence". The Office of the PCPD considers that the wording of paragraph 3.36.1(b) should be amended to strike a balance between the protection of privacy and crime investigation[209]. On the other hand, there are views supporting the proposed definition in paragraph 3.36.1(b) as it is considered that the coverage is wider[210].

3.36.5 A respondent objects to expanding the definition of "crime" to include a crime or offence under the law of a place outside Hong Kong on the ground the data user may not have the liability or knowledge to assess whether a situation amounts to a crime or offence overseas[211].

Proposed Way Forward

3.36.6 Views received generally support this proposal. We intend to implement this proposal to clarify the scope of the application of section 58 of the PDPO by adding a definition of "crime". In drafting the law, we will carefully examine the wording to

---

208 Please refer to S0097, S0124 and S0157 of Annex 4. Baker & McKenzie (S0124) points out that the amended wording provides that, even if the crime is committed outside Hong Kong, if it would constitute an offence if committed in Hong Kong, then it would come within the definition of crime.

209 Please refer to S0097 of Annex 4. This is supported by Hong Kong Human Rights Monitor (S0157).

210 Please refer to S0124 of Annex 4. Also, Baker & McKenzie (S0124) suggests to clarify the meaning of "legal or law enforcement cooperation".

211 Please refer to S0080 of Annex 4.

ensure that LEAs under multilateral and bilateral cooperative agreements or arrangements may provide personal data to their overseas counterparts for criminal investigations or detection of crimes overseas, and that assistance can be provided to foreign jurisdictions in verifying personal data in connection with requests for legal assistance.

(36) Expanding the Definition of "Relevant Person" (Proposal No. 37 in the Consultation Document)

Proposal in the Consultation Document

3.37.1 The proposal examines whether 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.

3.37.2 At present, the PDPO permits the lodging of complaint to the PCPD and the making of data access and data correction requests by a relevant person on behalf of the data subject concerned. The term "relevant person" is defined under section 2 of the PDPO to mean:

(a) a person who has parental responsibility for the minor;

(b) a person who is appointed by a court to manage the affairs of the individual who is incapable of managing his own affairs;

(c) a person authorised in writing by the individual to make a data access request, a data correction request, or both such requests, on behalf of the individual.

3.37.3 Under the existing definition, a lawful guardian appointed under the relevant provisions of the Mental Health Ordinance is not regarded as a "relevant person" under the PDPO. This proposal aims to expand the definition in order to accord sufficient protection to data subjects with mental incapacity with regard to their rights to complain and make data access and data correction requests.

Views Received

3.37.4 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority supported the implementation of the proposal[212] while some indicated that they had no comment. No submissions raised objection. During the consultation activities, no participants expressed any clear standpoint on this proposal.

Proposed Way Forward

3.37.5 Views received support this proposal in general. We intend to implement this proposal 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.

(37) Extending the Time Limit for Laying Information for Prosecution (Proposal No. 40 in the Consultation Document)

Proposal in the Consultation Document

3.38.1 The proposal examines whether 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.

3.38.2 The statutory time limit for laying information to prosecute an offence under the PDPO is prescribed under section 26 of the Magistrates Ordinance. The provision requires information to be laid before a magistrate within six months of commission of the offence. This timeframe is too tight since the PCPD needs to analyse the case, the Police to carry out investigation into a suspected offence and the Department of Justice to consider and initiate prosecution proceedings. The proposal aims to provide sufficient time for the PCPD, the Police and the Department of Justice to complete the necessary procedures for institution of prosecution.

[212] Please refer to S0073, S0080, S0097, S0151, S0156, S0157 and S0161 of Annex 4.

Views Received

3.38.3 Of the submissions received, less than 10% expressed views on this proposal. Of these, the majority indicated that they had no comment while some supported the implementation of the proposal and a minority of them raised objection. During the consultation activities, no participants expressed any clear standpoint on this proposal.

3.38.4 Respondents who support this proposal appreciate the fact that the current six-month time limit is too short and agree to extend it to two years. Moreover, they point out that this time frame is consistent with the spirit of section 39(1)(a) of the PDPO which states that the PCPD may refuse to carry out an investigation initiated by a complaint if the complainant has had actual knowledge of the act or the practice specified in the complaint for more than two years immediately preceding the date that he lodges the complaint[213]. Some individual respondents consider the 2-year time limit too long and suggest shortening it to one year[214].

3.38.5 Individual views who object to this proposal consider that the existing 6-month time limit safeguards data users[215] against the possibility of prejudice from excessive delays.

Proposed Way Forward

3.38.6 Views received support this proposal in general. We intend to implement this proposal 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.

---

213 Please refer to S0097 and S0157 of Annex 4.

214 Please refer to S0073 and S0151 of Annex 4.

215 Please refer to S0124 of Annex 4. Also, Baker & McKenzie (S0124) suggests that an extension of time limit will weaken the justifications for a criminal prosecution. Please also refer to S0080 and S0156 of Annex 4.

Chapter Four: Proposals Not to be Taken Forward

4.1.1 The public and some organisations have expressed worries about some proposals on various aspects and have even raised strong objection to some proposals. Upon analysis, we do not intend to take forward these proposals. In addition, Annex 2 to the consultation document set out the proposals which the Administration had considered but was inclined not to pursue. Having considered the views received, we maintain our original stance of not taking forward these proposals.

Sensitive Personal Data

(38) Sensitive Personal Data (Proposal No. 1 in the Consultation Document)

Proposal in the Consultation Document

Whether sensitive personal data should be subject to more stringent regulation

4.2.1 The proposal examines whether sensitive personal data should be subject to more stringent regulation so as to provide a better protection for these data. A key consideration is whether the community is prepared to accept the additional implementation costs associated with such a regime and the impact on other public and social interests.

4.2.2 To facilitate the discussion, the consultation document set out a possible regulatory regime, covering such matters as the coverage of sensitive personal data, the circumstances under which the handling of sensitive personal data was allowed, sanctions, and the need for grandfathering or transitional arrangement. Paragraphs 4.2.3 to 4.2.6 below briefly summarise the possible regulatory model.

Coverage of sensitive personal data

4.2.3 Biometric data such as iris characteristics, hand contour reading and fingerprints are unique personal identifiers. Such data are irrevocable or unchangeable. Loss or mishandling of such

data can arouse grave privacy concerns in the community. One option proposed in the consultation document is to consider classifying biometric data as sensitive personal data.

Circumstances under which handling sensitive personal data would be allowed

4.2.4 The consultation document proposed that the collection, holding, processing and use ("handling") of sensitive personal data would be prohibited except under the following circumstances:

(a) the prescribed consent (i.e. express consent given voluntarily) of the data subject has been obtained;

(b) it is necessary for the data user to handle the data to exercise his right as conferred by law or perform his obligation as imposed by law;

(c) handling of the data is necessary for protecting the vital interests of the data subject or others where prescribed consent of the data subject cannot be obtained;

(d) handling of the data is in the course of the data user's lawful function and activities with appropriate safeguard against transfer or disclosure to third parties without prescribed consent of the data subject;

(e) the data has been manifestly made public by the data subject;

(f) handling of the data is necessary for medical purposes and is undertaken by a health professional or person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional; or

(g) handling of the data is necessary in connection with any legal proceedings.

Sanction for contravention of requirements

4.2.5 The consultation document mentioned that we would need to consider whether the handling of sensitive personal data under

circumstances other than those set out in paragraph 4.2.4 above should attract a higher level of fine. Also, under the PDPO, data users have to comply with the DPPs. Breach of a DPP itself is not an offence, while contravention of an enforcement notice served by the PCPD is an offence. As proposed in the consultation document, we may consider making non-compliance with DPPs in the handling of sensitive personal data an offence. An alternative option to be considered is simply extending the existing regulatory regime governing contravention of DPPs involving personal data to sensitive personal data also.

Grandfathering or transitional arrangement

4.2.6 As proposed in the consultation document, we may consider applying the new requirements only to sensitive personal data collected after the relevant legislative provision comes into force (i.e. grandfathering arrangement). Alternatively, we may consider specifying a transitional period following the enactment of the new provision during which the processing of sensitive personal data will be exempt from the additional requirements. After the transitional period, data users have to meet the new requirements in processing the sensitive personal data (i.e. transitional arrangement).

Views Received

4.2.7 Nearly half of the submissions received expressed views on whether sensitive personal data should be subject to more stringent regulation. This proposal was also deliberated in various public consultation activities by members of the public and, in particular, heatedly discussed by the information technology sector.

Whether sensitive personal data should be subject to more stringent regulation

4.2.8 Most of the views expressed in various consultation activities and in submissions received agree with the general direction of providing a higher degree of protection to sensitive personal data. However, there are also views that oppose the differentiation of personal data in two categories, namely those that are "sensitive" and those that are not, and are against the

introduction of different regulatory regimes.

4.2.9 Many members of information technology sector are deeply concerned about this proposal, in particular in the area of biometric technology. They are worried that the implementation of the proposal to tighten regulation would affect the daily operation of the sector.

4.2.10 Among the submissions received which are in favour of subjecting sensitive personal data to more stringent regulation, most have not clearly stated the reasons for their support[216]. There are some views that with the advance in technology, the harm and damage caused by leakage of sensitive personal data could be very substantial, and that to provide better protection for personal data privacy, the Government should exercise more stringent regulation on the handling of sensitive personal data[217].

4.2.11 As to how the proposed arrangements are to be implemented, there are views that the issuance of guidelines should be adopted in place of legislation to allow for more flexibility[218].

4.2.12 Respondents against classifying personal data into different categories and introducing different regulation regimes have provided the following rationales:

(a) currently, there is no internationally recognised set of sensitive personal data, and there is no urgency for Hong

---

216 Please refer to S0003, S0060, S0074 and S0149 of Annex 4.

217 For example, the Office of the PCPD (S0097) indicates that more stringent regulation of sensitive personal data is in line with international practices and standards. The European Union ("EU") Directive 95/46/EC on the "protection of individuals with regard to the processing of personal data and on the free movement of such data" contains provisions to subject the processing of sensitive personal data to extra restrictions. PCCW (S0066) agrees that a higher degree of protection should be afforded to personal data that may inflict grievous harm on data subjects in the event of improper disclosure or leakage, e.g. biometric information such as health conditions, genetic information and ethnic origins. However, PCCW also points out that the existing biometric technology is used only to collect the geometric readings of a few spots on a fingerprint image for conversion into a serial number which by itself could not reveal any biometric features of the data subject. The Office of the PCPD (S0097) refers to a paper entitled "Fingerprint Biometrics: Address Privacy Before Deployment" issued in November 2008 by the Information and Privacy Commissioner of Ontario which stated that a fingerprint image could be reconstructed from the stored biometric template and the reconstructed image was sufficient to obtain a positive match in more than 90% of cases for most minutiae matchers. Please also refer to S0083 and S0089 of Annex 4.

218 Please refer to S0122 and S0148 of Annex 4.

Kong to take the lead in this regard. It is not easy to define the coverage of sensitive personal data appropriately and precisely. As the harm that may be resulted from data leakage varies from case to case, it is not appropriate to adopt a single set of sensitive personal data across the board[219];

(b) introducing a new regulatory regime lightly may confuse the public. Imposing over-stringent regulation will not only increase the operational cost of enterprises and impose a burden on commercial operations, but also cause inconvenience to the public in their ordinary daily life[220];

(c) as the public have not yet had a thorough understanding of the existing legislation, which has already provided proper protection for personal data, it is not the appropriate time to introduce new definitions and regulatory regimes[221]; and

(d) the inclusion of certain kinds of personal data in the list of "sensitive personal data" may lead to neglect of affording protection to those "non-sensitive personal data" which are not included in the list[222].

Coverage of sensitive personal data

4.2.13 Views on the coverage of sensitive personal data are diverse. Some consider that reference could be made to the practice of overseas jurisdictions to classify racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade union, health condition, sexual life and criminal record as

---

219 For example, the Federation of Hong Kong and Kowloon Labour Unions (S0055) is of the view that any type of personal data has its own importance and specific functions, and so harm may be caused to the data subject in the event of leakage of any type of personal data. Please also refer to S0071, S0119, S0123 and S0136 of Annex 4.

220 For example, the Hospital Authority (S0080) considers that the proposal would impose onerous operational and financial burden on it bearing in mind handling of biometric data in the course of diagnosis and treatment is very common and of substantial volume. The Hong Kong Construction Association (S0093) also indicates that the implementation of the proposal would involve considerable financial and social costs. Please also refer to S0048, S0049, S0101 and S0138 of Annex 4.

221 For example, the Hong Kong Computer Society (S0150) considers that given the current immature state of inadequate awareness by the community is not yet prepared for accepting changes to the regulatory regime. Please also refer to S0068 and S0151 of Annex 4.

222 Please refer to S0055 of Annex 4.

sensitive personal data[223]. There are also suggestions to classify other personal data (e.g. sexual orientation, residential address and health record) as sensitive personal data. Some opine that the community has yet to reach a consensus on the definition of sensitive personal data, and therefore suggest that the Government should further consult the public[224].

4.2.14 Most of the views suggest that there should be a clear definition of sensitive personal data, and some suggest that a set of sensitive personal data should be specified. However, there are also opposite views that a flexible approach should be adopted so as to leave room for making timely amendments to the relevant definition in the future in the light of technological and social developments[225]. There are also views that it is not appropriate to lay down any sweeping criteria, but rather it should be determined by the consequences that could result from leakage of such data. There are views that the definition of sensitive personal data should not be included in legislation.

4.2.15 Some participants in the public consultation activities proposed that a set of principles should first be developed to define sensitive personal data before a decision is to be made on whether the handling of data should be subject to different forms of regulation based on different levels of sensitivity.

4.2.16 As for the proposal on classifying biometric data as sensitive personal data, we have received both supporting views[226] and

---

223 Please refer to S0124, S0126, S0134, S0157, S0162 and S0171 of Annex 4. The Office of the PCPD (S0097) also suggests that the Government should re-consider the option to single out biometric data to be classified as sensitive personal data and consider classifying other personal data suggested in the PCPD's original proposal as sensitive personal data.

224 Please refer to S0068, S0087, S0102, S0120, S0135 and S0157 of Annex 4. The eHR Working Group (S0156) opposes the classification of all health records as sensitive personal data.

225 For example, Yahoo! Hong Kong Limited (S0123) considers that if the term "sensitive personal data" is to be defined, its definition must be inclusive, specific and unambiguous and only include specific data that warrant more stringent rules and additional protection. The Society for Community Organisation (S0132) however considers that there should be room in the definition for making future amendments, if necessary.

226 Those supporting classifying biometric data as sensitive personal data consider that biometric data are unique and unchangeable and have a higher degree of sensitivity under most circumstances. Please refer to S0083, S0092, S0113, S0132, S0135, S0154 and S0178 of Annex 4.

opposing views[227]. Representatives from the information technology sector generally consider that the proposal of classifying biometric data as sensitive personal data is targeted at the information technology sector, and fear that the information technology sector would discontinue the use of biometric technology to avoid punishment, hence seriously hampering the development of the sector.

4.2.17 Representatives from the information technology sector point out that at present their sector only takes partial fingerprint characteristics for conversion into data. As these data are neither restorable nor unique (however, see the Office of the PCPD's comment in footnote 217), the collection and use of these data should not be subject to stringent restriction. They also consider that there is no difference between biometric data and other personal data (e.g. identity card number and health record) in terms of their nature and therefore, biometric data should not be singled out for labelling as sensitive personal data.

4.2.18 At the same time, some members of the information technology sector are of the view that the unchangeable nature of biometric data may make such data more important but not necessarily more "sensitive" than other personal data.

4.2.19 There are views that the existing legislation is adequate in terms of its regulatory functions. It is pointed out that biometric technology is a key area for development in the information technology sector. There is no precedent of classifying biometric data as sensitive personal data in other overseas jurisdictions. The Government should leave more room for development in the legislation to help facilitate the development of the information technology sector in a positive manner.

---

[227] The opposing views point out that the information technology sector currently only take some of the fingerprint characteristics for conversion into data for record purposes. As such data are neither restorable nor unique, the collection and use of these data should not be subject to more stringent regulation. The implementation of the proposal would adversely affect the biometric industry and weaken the competitiveness of Hong Kong in the long run. Please refer to S0052, S0109, S0119, S0121, S0122, S0145 and S0148 of Annex 4.

Circumstances under which handling sensitive personal data would be allowed

4.2.20 While there are views supporting the proposed requirements set out in paragraph 4.2.4 above[228], there are also views that the wording of the requirements should be more specific[229].

4.2.21 There are views that data users should be required to adopt more stringent security measures to prevent data leakage, instead of imposing more stringent requirements on the circumstances under which handling of sensitive personal data would be allowed, so as to enhance the protection for data subjects.

4.2.22 There are also views that promotional efforts should be stepped up on the proper ways to handle biometric data.

Sanction for contravention of requirements

4.2.23 Only the Office of the PCPD comments on the sanction for handling sensitive personal data under circumstances other than those set out in paragraph 4.2.4. The Office of the PCPD supports making such an act, without reasonable excuse, an offence. Since the proposed provision is new to the public, the Office of the PCPD suggests that any penalty should be restricted to the imposition of a fine but not a custodial sentence.

4.2.24 Of the respondents who express views on the proposal to make non-compliance with DPPs in the handling of sensitive personal data an offence, almost all are opposed to this proposal and consider the existing regulatory model adequate[230]. They consider that the DPPs under the PDPO are couched in generic terms and could be subject to a wide range of interpretations. It is therefore not appropriate to make non-compliance with DPPs an offence. Besides, there are also views expressing the concern that criminalisation would scare off businessmen and

---

228 Please refer to S0089, S0097, S0113, and S0162 of Annex 4.

229 Please refer to S0073 and S0124 of Annex 4.

230 Please refer to S0067, S0073, S0083, S0122, S0126, S0148 and S0157 of Annex 4.

force them to move their businesses out of Hong Kong in order to avoid falling foul of the law inadvertently.

Grandfathering or transitional arrangement

4.2.25 Most of the respondents who express views on this area support the transitional arrangement[231], so that a transitional period would be specified following the enactment of the new provision, during which the handling of sensitive personal data would be exempt from the additional requirements. After the transitional period, data users have to meet the new requirements in handling sensitive personal data.

Proposed Way Forward

4.2.26 The above analyses and findings show that most of the views support the general direction that a higher degree of protection should be afforded to certain types of personal data which are more sensitive. Nevertheless, views received are diverse with regard to the coverage of sensitive personal data with no mainstream consensus reached.

4.2.27 Views opposing the classification of biometric data as sensitive personal data are particularly strong, especially those from the information technology sector. As for whether other personal data should be covered, views are diverse as well. Taking health records as an example, there are views that such data should not be subject to more stringent regulation so as to avoid onerous operational and resources burden having regard to the large volume of data involved and more frequent handling and transfer of data for medical and related purposes. There are also quite a lot of views considering that the Government should consult the public further before arriving at any conclusion.

4.2.28 We recognise that this proposal will have a wide impact and that different sectors in the community have not yet reached a consensus on the coverage and regulatory model. In view of this, we do not intend to introduce a more stringent regulatory regime for sensitive personal data at this stage. We shall keep

---

[231] Please refer to S0067, S0073, S0126, S0157 and S0162 of Annex 4. The Office of the PCPD (S0097) also states that the transitional period to be imposed should not be longer than 12 months.

in view the community's discussion on whether sensitive personal data should be subject to more stringent regulation and the coverage of sensitive personal data, as well as the development and experience of overseas jurisdictions on regulation of sensitive personal data, before we further consider whether to take forward the proposal to introduce more stringent regulation of sensitive personal data, with a view to striking a balance between protecting personal data privacy and other interests of the public and the community.

4.2.29 We recognise the public's concerns about enhancing the protection of sensitive personal data. The information technology sector has been maintaining exchange with the PCPD on how to afford better protection for biometric data. Some representatives of the information technology sector hope that the use of biometric data will be regulated by way of a code of practice or guidelines, so as to provide better safeguard against abuse or inappropriate handling of these data. As such, we propose 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 in general, such as biometric data and health record; and

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

Statutory Powers and Functions of the PCPD

(39) Granting Criminal Investigation and Prosecution Power to the PCPD (Proposal No. 4 in the Consultation Document)

Proposal in the Consultation Document

4.3.1 The proposal examines whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

4.3.2 The PDPO confers powers on the PCPD 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. However, the PCPD cannot carry out criminal investigation or initiate prosecution on his own. Currently, criminal investigations are conducted by the Police and prosecutions, where necessary, are initiated by the Department of Justice.

4.3.3 The PCPD has proposed that the PCPD be given the power to investigate and prosecute offences on the following grounds:

(a) the PCPD possesses first-hand information obtained in the course of his investigations and can investigate into suspected commission of an offence speedily;

(b) as the regulator, the PCPD is proficient in interpreting and applying the provisions of the PDPO, and can assess the weight and relevance of the evidence in any given situation with ease; and

(c) time in referring cases to the Police can be saved, thus helping to meet the statutory time limit to lay prosecution, which is set at six months from commission of an offence.

4.3.4 Under the Basic Law, criminal prosecutions are vested with the Department of Justice. It would not be inconsistent with the Basic Law to confer prosecution power on the PCPD if the relevant legislation expressly states that the prosecutions to be brought thereunder are without prejudice to the powers of the Secretary for Justice in relation to prosecution of criminal offences. However, strong justifications are required for the prerogative of initiating criminal prosecution to be delegated in specific domains.

4.3.5 At present, a number of statutory bodies are empowered to institute prosecution on its own[232]. However, the EOC, an independent statutory body established under the Sex

---

[232] For instance, the Vocational Training Council, the Employees Compensation Assistance Fund Board, the Construction Workers Registration Authority and the Securities and Futures Commission are provided with direct prosecution power in relation to summary offences.

Discrimination Ordinance to implement anti-discrimination ordinances, is not provided with direct prosecution power.

4.3.6 The PCPD referred eight cases to the Police for prosecution in 2006. The referral figures were nine in 2007, five in 2008 and eight in 2009. The existing arrangement has been working smoothly. There is no strong case for change. The Office of the PCPD points out that whether or not to prosecute or whether a prosecution results in successful conviction is not in hands of the PCPD after referral. Also, factors such as the complaints sometimes being lodged after the tight time frame for prosecution may account for such a low referral figure. To address the problem relating to the tight statutory time limit for initiating prosecution, Proposal (37) of this report proposes to effect a technical amendment to the PDPO to extend the time limit for laying information for prosecution of an offence from six months to two years.

4.3.7 To enhance personal data privacy protection, this report further proposes to step up sanctions under the PDPO (i.e. Proposals (1) to (3), (18) and (19) of this report).

4.3.8 The consultation document pointed out that there was no strong case to give the PCPD the power to investigate into and prosecute criminal offence cases.

4.3.9 The consultation document invited the public to comment on whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

Views Received

4.3.10 Nearly half of the submissions received expressed views on this proposal, most of which were against the proposal to confer criminal investigation and prosecution power on the PCPD, as opposed to a few in support. A few thought that criminal investigation power could be granted to the PCPD on a limited basis but prosecution power should remain in the hands of the Department of Justice. During the consultation activities, the respondents commenting on this proposal were mainly in opposition to the proposal.

4.3.11 The justifications of opposing the proposal are mainly as follows:

- the present arrangements in which criminal investigations are conducted by the Police and prosecutions by the Department of Justice have been operating smoothly and need not be changed[233]. Although the consultation document already set out the arguments of the Office of the PCPD regarding its support to the proposal, quite a lot of respondents think that there is no compelling reason to grant criminal investigation and prosecution power to the PCPD[234];

- the Office of the PCPD will have excessive power if enforcement and prosecution powers are conferred on it. Criminal investigation and prosecution powers should be vested in different institutions to maintain checks and balances instead[235];

- some are of the view that prosecution power should be vested in an independent body in accordance with the existing constitutional framework. As the PCPD is the enforcement authority of PDPO, the proposal to confer criminal investigation and prosecution power on PCPD will give rise to conflict of interests[236];

- the role of the Office of the PCPD includes assisting data users to comply with the requirements of the PDPO. The

---

233 Please refer to S0071, S0083, S0119, S0121, S0123, S0131, S00134, S0135, S0136, S0151, S0152, S0166, S0173, S0177 and S0180 of Annex 4.

234 Please refer to S0056, S0071, S0121, S0124, S0131 and S0148 of Annex 4.

235 Please refer to S0052, S0055, S0056, S0092, S0116, S0124 and S0168 of Annex 4.

236 Please refer to the following extract of the minutes of special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009, "Dr (Margaret) NG said that she did not support Proposal No. 4 which sought to grant criminal investigation and prosecution power to PCPD. In her view, prosecution power should be vested in an independent body in accordance with the existing constitutional framework. She considered the present arrangement to empower executive departments such as the Customs and Excise Department and the Immigration Department with prosecution power not satisfactory. She pointed out that as PCPD was the enforcer of PDPO, the proposal to confer criminal investigation and prosecution power on PCPD would give rise to conflict of interests."

proposal may confuse the role of the Office of the PCPD and deter data users from seeking its help[237];

- the offences under the PDPO are not technical in nature, and involve fines and imprisonment. There are queries as to whether the PCPD possesses necessary expertise to conduct criminal investigation, and it is considered inappropriate to confer on the PCPD the power to prosecute relevant offences[238];

- there are views that the implementation of the proposal will necessitate a restructuring of the Office of the PCPD and an increase in funding and professional staff for the performance of the tasks, resulting in wastage of resources. Currently, the power to prosecute in cases handled by various government departments (including the Social Welfare Department, which has a large organisational structure) is vested in the Department of Justice. As the present number of referrals made by the Office of the PCPD for prosecution is not large and there is no reason to suggest that the number of such cases will increase substantially in future, it is considered more appropriate for the Department of Justice to continue with the prosecution work[239];

---

237 Please refer to S0119 and S0120 at Annex 4. Baker & McKenzie (S0124) points out in particular that the proposal is not in consonance with the intended spirit of the legislation which includes empowering the Office of the PCPD to educate the public and to monitor and supervise compliance with the PDPO. Under the present regime, data users are more likely to make voluntary disclosures to the Office of the PCPD and to work with it to improve their systems and to enhance protection of personal data. The granting of prosecution powers to the Office of the PCPD will dramatically reduce the number of voluntary disclosures and will materially alter the relationship between the Office of the PCPD and the public. Besides, Hong Kong Broadband Network Limited (S0103) submits that should the proposal be adopted, when handling complaints of a data user, the Office of the PCPD may suffer pressure from the complainant to prosecute, which are not only undesirable but may be counterproductive.

238 Please refer to S0066 and S0131 at Annex 4.

239 For example, the Hong Kong Broadband Network Limited (S0103) says that it would be more appropriate for the Department of Justice to continue with the prosecution work as it will be in a stronger position in possessing specialist knowledge to decide whether to prosecute. PCCW (S0066) expresses that considering the small number of prosecution, it is uneconomical to deploy public resources to set up a prosecution team in the Office of the PCPD. The Internet Professional Association (S0148) is of the view that the number of cases in which prosecution has to be instituted is manageable and do not see any trend of acute increase. Please also refer to S0048, S0049, S0056, S0101, S0122, S0124 and S0152 at Annex 4.

- the question of a tight timeframe for instituting prosecution raised by the Office of the PCPD can be solved by extending the time limit to two years (i.e. Proposal (37) of this report) or by other methods to shorten the time required for prosecution[240];

- other similar organisations (e.g. EOC) do not have the prosecution power either. The adoption of the proposal might trigger a chain effect affecting the existing judicial system[241]; and

- some participants in various public consultations indicate support for retaining the status quo but consider that the Office of the PCPD should seek additional resources to handle more cases and step up education and publicity.

4.3.12 In general, those respondents who support the proposal believe, mainly on the following grounds, that the proposal could enhance the effectiveness of the Office of the PCPD in its law enforcement efforts:

- as a human rights organisation, the Office of the PCPD should have extensive power (including the power to prosecute) to ensure effective implementation of the PDPO[242];

- since identity theft is getting more rampant and complicated, and the workload and pressure presently facing the Police are already so great that no more burden should be imposed, it is necessary to strengthen the investigative power of the Office of the PCPD[243];

---

240 Please refer to S0055 and S0067 of Annex 4. Baker & McKenzie (S0124) also points out that there was no evidence to demonstrate that the Department of Justice has failed to prosecute any claims within the statutory period.

241 Please refer to S0121 and S0134 of Annex 4.

242 Please refer to S0097 and S0132 of Annex 4. Hong Kong Human Rights Monitor (S0157) agrees to confer on the Office of the PCPD the prosecution power but cautions that it should be very careful in exercising this power. The Democratic Party (S0178) holds the view that the Office of the PCPD has better understanding on privacy issues and the related laws than other law enforcement agencies, it is appropriate for it to be responsible for criminal investigation.

243 Please refer to S0115 of Annex 4.

- the Office of the PCPD points out that if the Police or the Department of Justice is involved in a case, there might be a conflict of roles when they make criminal investigation into or prosecution decision on the case[244]; and

- the Office of the PCPD points out that, if the time limit for prosecution is to be extended to two years and other new offences are to be introduced as proposed in the consultation document, the number of prosecutions to be instituted by the PCPD will be much higher. The need for the Office of the PCPD to expand its investigative and prosecution power will be greater[245].

4.3.13 The Office of the PCPD also states that the proposal will not prejudice the Secretary for Justice's discretion to prosecute. It is because the granting of prosecution power to the PCPD entails only the carrying out of the prosecution work and it will be made explicit in the law that the PCPD's power to prosecute shall be subject to the consent of the Secretary for Justice.

Proposed Way Forward

4.3.14 To sum up, the public views received generally oppose to conferring criminal investigation and prosecution power on the Office of the PCPD.

4.3.15 The grounds raised in opposition of the proposal cover various aspects, including: since the existing arrangements have worked well, there is no convincing ground to change; the PCPD would have excessive power if conferred with the power to carry out criminal investigations and prosecutions in addition to enforcement and this would result in a loss of checks and balances; as the proposal to confer criminal investigation and prosecution power on the PCPD, the enforcement authority of the PDPO, would give rise to a conflict of interest, the powers should be vested in different institutions; it would be more appropriate for the Department of Justice to initiate prosecutions; conferring prosecution power on the Office of the PCPD would cause confusion over its role and deter data users from seeking help from the PCPD to comply with the

[244] Please refer to S0097 and S0132 of Annex 4.

[245] Please refer to S0097 of Annex 4.

requirements of the PDPO; and there would be an overlapping of structure and hence a waste of resources if an additional unit is to be established within the Office of the PCPD to handle the investigation and prosecution of criminal offence cases.

4.3.16 Based on the clear views and justifications stated above, we consider that the status quo should be maintained and the Office of the PCPD should not be given the power to investigate into or prosecute criminal offence cases.

(40) Empowering the PCPD to Award Compensation to Aggrieved Data Subjects (Proposal No. 6 in the Consultation Document)

Proposal in the Consultation Document

4.4.1 The proposal examines whether the PCPD should be empowered to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user, as another redress avenue apart from seeking compensation through the court as provided for under section 66 of the PDPO.

4.4.2 The appropriate body to determine compensation under the PDPO was thoroughly discussed in the Law Reform Commission ("LRC") "Report on Reform of the Law Relating to the Protection of Personal Data" issued in August 1994. The LRC opined that conferring power on a data protection authority to award compensation would vest in a single authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there had been a breach of the DPPs. It would be for a court to determine the appropriate amount of compensation payable.

4.4.3 The EOC is not provided with power to award compensation either.

4.4.4 The consultation document invited public views on whether the PCPD should be empowered to award compensation to aggrieved data subjects, as an additional redress avenue.

Views Received

4.4.5 Nearly 40% of the submissions received commented on this proposal. The majority were opposed to empowering the PCPD to award compensation to aggrieved data subjects while the minority supported. Some did not indicate a clear preference. In the public consultation activities, no specific views were given by participants on this proposal.

4.4.6 Most of the respondents who oppose this proposal agree that it is undesirable to vest in a single authority a combination of enforcement and punitive functions as recommended by the LRC in 1994[246]. The PCPD's role should be limited to determining whether there has been a breach of the DPPs. It should be for the court to determine the amount of compensation payable.

4.4.7 Some respondents who oppose this proposal opine that the current system has been working well. Aggrieved data subjects could seek compensation through the court as provided for under section 66 of the PDPO and the status quo should be maintained[247]. Some opine that there is no need to implement this proposal if the proposal of providing legal assistance to data subjects (i.e. Proposal (7) of this report) could be implemented as aggrieved data subjects would be given sufficient assistance to claim compensation by law[248].

---

246 Most of the organisations support the proposal in the LRC's Report issued in 1994. For example, Baker & McKenzie (S0124) doubts if the PCPD will be able to determine the amount of compensation through a process of mediation. It is also concerned that the proposal may lead to confusion as to the PCPD's role in an investigation. Both the Federation of Hong Kong Industries (S0122) and Internet Professional Association (S0148) are concerned whether the PCPD has the expertise to determine the compensation amount which is complex. Eventually, any dispute over the amount of compensation has to be settled in court. In addition, the process to claim compensation would be expedited since no legal proceedings are required by the proposal. This may lead to abuse of the mechanism, resulting in a heavy burden on resources of the Office of the PCPD. Please also refer to S0052, S0056, S0062, S0068, S0083, S0084, S0116, S0119, S0123, S0132, S0134, S0145, S0152, S0162, S0166, S0168 and S0177 of Annex 4.

247 For example, PCCW (S0066) considers that the current regime of issuing enforcement notice by the PCPD is an adequate and suitable means to protect the aggrieved data subjects. Hong Kong IT Alliance (S0109) considers that it is not necessary to empower the PCPD with this additional power and responsibility. Please also refer to S0080, S0113, S0120 and S0180 of Annex 4.

248 Please refer to S0056, S0067 and S0135 of Annex 4. In addition, Baker & McKenzie (S0124) considers that the proposal of empowering the PCPD with the authority to determine the amount of compensation payable to aggrieved data subjects may be inconsistent with that of providing legal assistance to aggrieved data subjects.

4.4.8 The Office of the PCPD points out that not every aggrieved data subject would be granted legal assistance due to resources constraints. Therefore, the legal assistance proposal could not replace the proposal to empower the PCPD to award compensation[249]. There are also supporting views which stress that even if this proposal is implemented, the PCPD should not be considered as seeking to exercise judicial power[250].

Proposed Way Forward

4.4.9 The above analyses reveal that the relevant views received generally oppose empowering the PCPD to award compensation to aggrieved data subjects. They also agree that it is undesirable to vest in a single authority both the enforcement and punitive functions.

4.4.10 The LRC pointed out in its "Report on Reform of the Law Relating to the Protection of Personal Data" issued in August 1994 that it is undesirable to vest in a single authority both enforcement and punitive functions. In common law systems, functions and powers relating to investigation, prosecution and adjudication are normally vested in different authorities in order to maintain checks and balances.

4.4.11 In view of the above, we do not intend to implement this proposal.

Offences and Sanctions

(41) Making Contravention of a Data Protection Principle an Offence (Proposal No. 7 in the Consultation Document)

Proposal in the Consultation Document

4.5.1 The proposal examines whether we should make contravention of a DPP an offence.

---

249 Please refer to S0097 of Annex 4.

250 For example, the Law Society of Hong Kong (S0073) states that they support the proposal on the condition that no compensation notices should be automatically enforceable as if they were court orders and the PCPD should not be considered as seeking to exercise judicial power.

4.5.2 At present, contravention of a DPP by itself is not an offence under the PDPO. However, the PCPD can remedy the breach by issuing an enforcement notice to direct the data user to take specified remedial steps within a specified period. If the data user contravenes the enforcement notice, he will commit an offence[251].

4.5.3 DPPs are couched in generic terms and can be subject to a wide range of interpretations. As stated in the consultation document, making contravention of a DPP an offence would have significant impact on civil liberties as an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO.

4.5.4 Thus, it might be more appropriate to adopt a selective approach by singling out particular acts or practices as offences having regard to the severity of such contravening acts or practices.

Views Received

4.5.5 Nearly half of the submissions received commented on this proposal. Of these submissions, the majority (including the Office of the PCPD) opposed making contravention of a DPP an offence and the minority supported the proposal, whereas some did not indicate a clear preference. All the participants who commented on this proposal in various public consultation activities were opposed to implementing the proposal.

4.5.6 Most of the opponents of this proposal agree with the viewpoints in the consultation document as set out in paragraph 4.5.3 above[252] and have further comments as follows:

- some consider the proposal going overboard. In general, contravention of a DPP is not serious enough to warrant criminal liability. In particular, in case of inadvertent contravention of DPPs, it would be too harsh to make such

---

251 An offender will be liable on conviction to a fine at Level 5 ($50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

252 Please refer to S0048, S0049, S0052, S0056, S0062, S0066, S0068, S0083, S0101, S0116, S0119, S0123, S0124, S0138, S0150, S0151, S0152, S0162, S0165, S0166, S0168 and S0178 of Annex 4.

an act an offence and it would have significant impact on the public's daily life[253];

- there are worries that data users would have to bear a heavy burden[254] as the proposal could not state clearly the specific circumstances under which the data user would be subject to criminal liability. There is opinion that in creating a new offence, we must abide by the basic legal principle of making the offence clear and specific, and it must be supported by full justifications in order to prevent injustice[255];

- some consider that DPPs are high-level guiding principles that should be as flexible as possible to conform with their original intent[256]; and

- some point out that it may not be an effective way to treat contravention of DPPs as a criminal offence[257]. A better

---

253 Please refer to S0040, S0055 and S0056 of Annex 4. In addition, the Hong Kong Jewelry Manufacturers' Association (S0071) considers that the Government should assess the level of public awareness and understanding of the existing PDPO before considering criminalising certain acts in contravention of the DPPs.

254 The Hong Kong Information Technology Federation (S0138) expresses concerns about the adverse effect that criminalisation would have on the information technology industry, where businesses are often engaged in new and innovative activities. Please also refer to S0109 and S0113 of Annex 4.

255 Please refer to the following extract of the minutes of special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009: "Dr Margaret NG said that in creating a new offence, one must abide by the basic legal principle of making specific the offence clear and with full justification in order to prevent injustice. While the enforcement of PDPO might not be satisfactory, measures to step up enforcement actions, instead of imposing more penalties, creating criminal offences and conferring more power on the Commissioner, could be an answer to the problem."

256 Freshfields Bruckhaus Deringer (S0087) does not consider the terms of the DPPs are sufficiently specific to form the basis for clear and justiciable criminal offences. The Hong Kong Investment Funds Association (S0056) opines that the DPPs are couched in generic terms and are subject to wide interpretations. Should the proposal be implemented, the DPPs would need to be redrafted in much stricter terms but it will make the DPPs overly prescriptive and inflexible. Please also refer to S0142 of Annex 4.

257 The Office of the PCPD (S0097) suggests that it is recognised under international jurisprudence that effective means of ensuring the proper behaviour and attitude towards protection of personal data privacy is by regulation rather than criminal sanction. DAB (S0145) opines that the handling of contravention of DPPs as criminal cases should not be taken lightly. If criminal liability is involved, data users and subjects would be put in diametrically opposing positions. Data users would make all efforts to protect themselves from criminal liability rather than taking immediate remedial measures when necessary. In the end, it might not be beneficial to the data subjects.

approach to get at the root of the problem is to step up publicity and education[258].

4.5.7 Those who support the implementation of this proposal point out that it would help tighten up the control over contravention of DPPs. There are also views that in order to prevent inadvertent violation of the law and to avoid negative impact on civil liberties, only intentional contravention should be made an offence while inadvertent act or omission should be exempt from criminal liability[259]. There are views agreeing with the consultation document that it would be more appropriate to adopt a selective approach by singling out particular contravening acts or practices which are more severe as offences[260]. Besides, a respondent opines that criminalisation should only be considered when it is the only and the most effective means of tackling the problem[261].

4.5.8 Some also suggest imposing a higher penalty level so as to enhance the deterrent effect of the Ordinance[262].

Proposed Way Forward

4.5.9 Views received generally oppose making contravention of a DPP an offence. Therefore, we do not intend to implement this proposal.

4.5.10 Besides, some respondents consider it more appropriate to single out particular contravening acts or practices which are of a more serious nature as offence. Proposal (2) of this report suggests making it an offence for a data user to sell personal

---

258 Please refer to S0084, S0142 and S0150 of Annex 4.

259 Please refer to S0011, S0073, S0121, S0134, S0135 and S0140 of Annex 4.

260 Please refer to S0056, S0068, S0087, S0089, S0097, S0124, S0132 and S0156 of Annex 4. Besides, Hong Kong Human Rights Monitor (S0157) suggests that the Office of the PCPD might draw on its past experience in handling the cases and decide what kind of serious contravention should be made a criminal offence.

261 Hong Kong General Chamber of Commerce (S0119) points out that every new offence represents a restriction of civil liberties and expansion of government power. Criminalisation should only be considered when the contravening acts are indisputably serious, and that criminalisation is the only and most effective means of tackling the problem.

262 Please refer to S0122 and S0148 of Annex 4.

data to another person for a monetary or in kind gain without the consent of the data subject. Proposal (3) suggests making it an offence for a person to disclose, for profits or malicious purposes, personal data obtained from a data user without the latter's consent. If these proposals are implemented, it could help deter serious contravention of DPPs.

(42) Imposing Monetary Penalty on Serious Contravention of Data Protection Principles (Proposal No. 10 in the Consultation Document)

Proposal in the Consultation Document

4.6.1 The proposal examines whether it is appropriate to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs in order to deter serious contravention of DPPs.

4.6.2 The consultation document pointed out that in Hong Kong, it was not common for non-judicial bodies to have the statutory power to impose monetary penalties. The few examples involve fixed penalty schemes and clearly defined offences[263].

4.6.3 Under the PDPO, DPPs are couched in generic terms and can be subject to a wide range of interpretation, and whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. It may be more appropriate to consider singling out particular acts or practices of contravention of DPPs of a serious nature and making them an offence.

4.6.4 The consultation document invited the public to comment on whether it was appropriate to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs.

Views Received

4.6.5 Of the submissions received, 40% commented on this proposal. Of these submissions, the majority were against the proposal,

[263] Such as Fixed Penalty (Traffic Contraventions) Ordinance (Cap. 237), Fixed Penalty (Public Cleanliness Offences) Ordinance (Cap. 570), and Fixed Penalty (Smoking Offences) Ordinance (Cap. 600).

some indicated support, while others made no clear indication of preference. Only a few participants put forth their views on this proposal in various consultation activities.

4.6.6 The majority of those who oppose this proposal agree that DPPs are couched in generic terms and can be subject to a wide range of interpretations. It is inevitably a matter of subjective judgment as to whether an act constitutes a serious contravention of a DPP. They are of the view that there will certainly be difficulties in enforcement if "serious contravention" of DPPs is not objectively and specifically defined[264].

4.6.7 There are views that the existing penalty on contravention of DPPs in Hong Kong is effective as a whole and should be retained. Section 66 of the PDPO has already provided an aggrieved data subject with an avenue to seek compensation through the Court. It is, therefore, considered not necessary to impose heavier penalty on persons who have seriously breached DPPs as a measure to protect data subjects[265].

4.6.8 As regards the authority vested with punitive power, there are views that the PCPD is not a judicial body and it is not common for non-judicial bodies to have the statutory power to impose penalty in Hong Kong. Empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs would vest the enforcement and punitive functions in a single

---

[264] Most of the organisations agree to the analysis in the consultation document. For examples, the Hong Kong Investment Funds Association (S0056) considers that as DPPs are couched in general terms, it is inappropriate for the PCPD to impose monetary penalties based purely on its own assessment of whether the breach constitutes a "serious contravention" of a DPP. Baker & McKenzie (S0124) holds that implementing this proposal would create an arbitrary hierarchy of DPPs between serious breaches and non-serious breaches. The Society for Community Organisation (S0132) points out that it is difficult to define "serious contravention of DPPs". Please also refer to S0048, S0049, S0052, S0062, S0066, S0071, S0087, S0116, S0119, S0156, S0162, S0166 and S0168 of Annex 4.

[265] For example, the Liberal Party (S0135) is of the view that aggrieved data subjects are currently allowed to seek compensation through civil remedy and the consultation document also suggests conferring power on the PCPD to offer, as circumstances warrant, appropriate legal assistance to the claimants. It is therefore not necessary to empower the PCPD to impose monetary penalty on persons who have seriously breached DPPs. Please also refer to S0080, S0083, S0113 and S0123 of Annex 4.

authority which is considered undesirable[266].

4.6.9 A few comment that it is more appropriate to consider singling out particular acts or practices of contravention of DPPs of a serious nature and making them an offence[267].

4.6.10 Some supporters of this proposal, including the Office of the PCPD, consider that the proposal could enhance the deterrent effect of the PDPO, and suggest that the Government should make reference to the amendment to the UK Data Protection Act outlined in the consultation document[268].

Proposed Way Forward

4.6.11 The above analysis indicates that the submissions received are generally against empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs, and a few submissions consider that it would be more appropriate to make serious contravention a criminal offence.

---

266 For example, the Society for Community Organisation (S0132) points out that the PCPD will, if the proposal is implemented, play overlapping roles of a law enforcer and an adjudicator. Such an arrangement does not align with the procedural fairness. It is also difficult for an authority to control and monitor its power. PCCW (S0066) points out that the DPPs are couched in generic terms and can be subject to wide interpretation. It would therefore be more appropriate for the judiciary to retain jurisdiction of determining the seriousness of contravention. Please also refer to S0052, S0067, S0071, S0084, S0119, S0120, S0122, S0136, S0148 and S0162 of Annex 4.

267 The eHR Working Group (S0156) proposes that monetary penalty or criminal liability be imposed according to the seriousness of each contravening act. Please also refer to S0068, S0124, S0126 and S0151 of Annex 4.

268 The Office of the PCPD (S0097) proposes to make reference to the amendment (which came into force on 6 April 2010 by virtue of the Data Protection (Monetary Penalties) Order) to the UK Data Protection Act 1998. Under the amendment, the UK Information Commissioner may serve a data controller with a monetary penalty notice where the Commissioner is satisfied that (a) there has been a serious contravention of the data protection principles; (b) the contravention is of a kind likely to cause substantial damage or distress; and (c) the data controller knows or ought to have known a risk of contravention of a kind likely to cause substantial damage or distress but he failed to take reasonable steps to prevent the contravention. The amount of penalty determined by the Information Commissioner must not exceed the amount as prescribed by the Secretary of State. The regulatory regime also provides for an appeal mechanism. The Information Commissioner has published a "Guidance about the issue of Monetary Penalties prepared and issued under section 55C(1) of the Data Protection Act 1998". The Guidance sets out the criteria or factors the Information Commissioner considers appropriate to impose monetary penalty, including the circumstances he considers appropriate to impose monetary penalty. Please also refer to S0157 of Annex 4.

4.6.12 It is clearly stated in the Report on Reform of the Law Relating to the Protection of Personal Data published by the LRC in August 1994 that it is undesirable to vest in a single authority with both the enforcement and punitive functions. Moreover, under the common law system, the roles of investigation, prosecution and adjudication should be performed by different institutions for checks and balances.

4.6.13 Therefore, we do not intend to implement this proposal. As regards making serious contravention a criminal offence, Proposal (2) of this report suggests making it an offence for a data user to sell personal data to another person for a monetary or in kind gain without the consent of the data subject. Proposal (3) suggests making it an offence for a person to disclose, for profits or malicious purposes, personal data obtained from a data user without the latter's consent. If these proposals are implemented, it would help deter serious contravention of DPPs.

Access to Personal Data

(43) Parents' Right to Access Personal Data of Minors (Proposal No. 14 in the Consultation Document)

Proposal in the Consultation Document

4.7.1 The proposal examines whether new provisions should be introduced 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 the minor) on behalf of a minor in order to protect the interests of minors.

4.7.2 Under section 18(1) of the PDPO, a "relevant person", on behalf of a data subject, has the right to make a request to a data user to access the data subject's personal data. Under section 2(1) of the PDPO, if the individual is a minor, "relevant person" means a person who has parental responsibility for the minor concerned.

4.7.3 Acceding to a data access request made by a "relevant person" on behalf of a minor may not be in the interests of the minor under certain circumstances, such as:

(a) where an estranged parent makes a data access request to the school for his/her child's location data to trace the whereabouts of the child or the ex-spouse;

(b) where a parent is suspected to have committed child abuse on his/her child; and

(c) where the child has expressed to the data user his/her disagreement to the disclosure of his/her personal data to his/her parents.

4.7.4 To strike a balance between respecting parents' role in taking care of their children and respecting children's privacy right, it was proposed in the consultation document that data users should be allowed to refuse to comply with a data access request if they had reasonable grounds to believe that compliance with the request of a "relevant person" would not be in the best interests of the minors concerned. It was further proposed that some factors should be specified to enable data users to assess whether there were reasonable grounds to refuse a data access request made by a "relevant person".

Views Received

4.7.5 Close to 30% of the submissions received commented on this proposal. Of these submissions, views were divided on whether the proposal should be implemented. Many respondents who supported the general direction of this proposal were not totally agreeable to the proposed implementation approach. In other public consultation activities, most participants commenting on this proposal expressed reservations.

4.7.6 Respondents who support the general direction of this proposal suggest that only under very special and exceptional circumstances should a data user be allowed to refuse parents' data access requests when there are reasonable grounds to believe that such requests would not be in the best interests of

the minors[269]. They also raise the following considerations:

- the data user might not be capable of judging whether a parent's data access request is in the best interests of the data subject and to decide whether to refuse such a request. As such, there are views suggesting that the Office of the PCPD should provide due assistance to data users by, for example, formulating guidelines in this respect[270];

- in order not to place unreasonable burden on the data user, there is a suggestion that the assessment of and decision to refuse a parent's data access request should be regarded as "an exercisable right" rather than "an obligation" of the data user[271];

- when introducing new provisions, certain consideration factors, such as the wish of a minor, should be included for the data user to assess if there are reasonable grounds to refuse a parent's request[272].

4.7.7 The main arguments of those who object to this proposal are as follows :

(i) protection against child harassment or abuse is not privacy-related issue. It is, therefore, inappropriate to set

---

269 The Office of the PCPD (S0097) points out that it is not the intention of the proposal to deny the parents' rights and obligations in caring for their children, and parents may lodge a complaint with the Office if they are not satisfied with the decision made by the data user. The Boys' and Girls' Clubs Association of Hong Kong (S0143) supports the proposal and opines that a minor's right to privacy with regard to personal data should be respected as communication between children and parents should be based on mutual trust, not by means of data access made in private and through a third party. The Democratic Party (S0178) agrees the proposal in principle, but holds the view that the situations which do not meet the "best interests" criteria should be clearly stated.

270 Please refer to S0099 and S0126 of Annex 4. Besides, Hong Kong Human Rights Monitor (S0157) suggests that the PCPD should be empowered to give advice to the data user in respect of a parent's data access request, and that an appeal mechanism should be put in place, so that a "relevant person" being rejected may lodge an appeal.

271 Please refer to S0066 of Annex 4.

272 For example, the Hong Kong Christian Service (S0079) suggests that data users should be required to duly consider the wish of a minor, the safety of the data subject as well as the court's decision. Similarly, the Hong Kong Family Welfare Society (S0099) opines that data users should duly consider the wish of a minor wherever practicable. The Society further suggests that the definition of "relevant person" should exclude parents suspected of child abuse to prevent parents from exploiting the mechanism to abuse their children. Please also refer to S0132 of Annex 4.

up a separate framework under the PDPO to regulate these conducts[273];

(ii) the proposal seems to give excessive discretion to data users. The decision on whether a data access request is in the best interests of a minor should rest with his/her parents or legal guardians. There are also views that only the court is in a position to decide and it might be unfair and inappropriate to place such a heavy responsibility on data users[274];

(iii) the proposal requires data users to gather justifications and to make appropriate assessment, after striking a balance among all different factors, in particular the wish and the best interests of minors, on whether there are reasonable grounds to believe that a data access request would not be in the interests of minors. There would be considerable difficulties in implementation. The proposal is therefore impracticable;

(iv) currently, the court encourages both parents to share the responsibility to take care of their children even if they are separated. Should this proposal be implemented, a parent may find it difficult to fulfill such a responsibility. As youth problems are worsening and minors may not be capable of exercising their rights in a sensible way, if parents are denied access to the relevant data of their

---

273 For example, the Parents for the Family Association (S0105) proposes that if there are sufficient grounds to believe that the interests of a minor would be jeopardised upon disclosure of his/her personal data to his/her parents, the Government should put the minor under the care of another person who would temporarily take up the parental duties, and leave the responsibilities of the "relevant person" to the surrogate parent. The Federation of Hong Kong Industries (S0122) and the Internet Professional Association (S0148) both remark that where a parent is suspected to have committed child abuse on his/her child, the data user should report to the relevant authority and the case should be brought to court to determine whether the data access request should be acceded to. Please refer also to S0068 and S0140 of Annex 4.

274 For example, the Hong Kong Association of Banks (S0068) points out that it would be difficult in practice for banks to determine whether a data access request is in the best interests of a minor given the nature of banking business and transactions. The Hospital Authority (S0080) holds similar views that the data user may not have the information or ability adequate to make the relevant decision. DAB (S0145) suggests that the data user should merely record the reason for the data access request raised by the parents instead of having the authority to refuse to comply with the request after making an assessment. The Society for Truth and Light (S0125) points out that in case the children have unfortunately made a wrong decision, the consequences would be borne by the children themselves and their parents but not the data user. Parents' access to relevant data, therefore, should not be determined by the data user. Please refer also to S0102, S0122 and S0156 of Annex 4.

children, timely assistance may not be given to the children. This would be a very inappropriate and dangerous move;

(v) while it may be understandable to refuse a parent's data access request on grounds of protecting the interests and safety of children as illustrated in scenarios (a) and (b) in paragraph 4.7.3 above, it is inappropriate to include scenario (c) for consideration. The respondents consider that the Government should not overact and take away parents' right to access the data of their children unreasonably, as this is crucial to them in fulfilling their parental responsibility[275]; and

(vi) the proposal, intending to restrict parents' right to access personal data of their underage children, is premised on the assumption that many parents would make use of the data access mechanism to obtain their children's personal data for their own purpose rather than for the children's well-being. The assumption has distorted the image of parents[276].

4.7.8 Some respondents who have no comments on this proposal also express concern over point (i) in the above paragraph. They consider that even if the proposal is implemented eventually, such a heavy responsibility should not be imposed on data users[277].

---

275 For example, the Society for Truth and Light (S0125) expresses concern over scenario (c), arguing that minors under the age of 18 may not be sufficiently informed to make appropriate decisions. As such, it may be inappropriate for them to have the right of self-determination to refuse their parents' access to their personal data. It is also extremely controversial to set a suitable age of full capacity. The existing practice, therefore, should continue. The Liberal Party (S0135) also expresses strong opposition to scenario (c), believing that the parent-child relationship would be affected, and it would impede parents from finding out any deviant behaviours of their children before it is too late. Please refer also to S0003 and S0055 of Annex 4.

276 Please refer to the following extract of the minutes of the special meeting of the LegCo Panel on Constitutional Affairs held on 11 September 2009: "Dr Priscilla LEUNG expressed concern about the negative approach adopted for formulating Proposal Nos. 14 and 27 which had projected a negative image of parents. She considered that the proposals which sought to restrict parents' right to access personal data of minors are premised on the assumption that many parents are irresponsible and they may abuse the data access mechanism to obtain the personal data of the child for the parents' own purpose rather than for the interests of the child."

277 Please refer to S0048 and S0049 of Annex 4. In addition, Baker & McKenzie (S0124) considers that the proposal of allowing data users to judge whether a parent's data access request is in the best interests of a minor and to decide whether to reject the request should be regarded as their "right" but not "obligation".

Proposed Way Forward

4.7.9 The above analysis indicates that views received generally have reservations about the implementation of the proposal or its operation, and express grave concern over its possible consequences.

4.7.10 With respect to the operation of the proposal, there are quite a number of views suggesting that leaving data users to decide whether parents' data access requests will be in the best interests of the minor is not appropriate and there will be practical difficulties in operation. Although consideration may be given to providing data users with assistance and guidelines, it is hardly avoidable that implementation of the proposal will place an unfair burden on data users.

4.7.11 There are also views expressing worries that the restriction of parents' right of access to their children's personal data may jeopardise the fulfillment of their parental responsibility in daily life, hence generating other family problems.

4.7.12 In addition, from the perspective of the fundamental objective of the proposal, there are opposing views pointing out that it is not appropriate for the Government to protect children from being harassed or abused by a "relevant person" through the PDPO. It is suggested that such issues should be dealt with under other relevant legislation.

4.7.13 In fact, the PDPO does not stipulate that data users have the absolute obligation to accede to data access requests made by "relevant persons". Under section 18 of the PDPO, a "relevant person", on behalf of a data subject, has the right to make a request to a data user to access the data subject's personal data. If in any particular cases showing that the "relevant person" is not genuinely making a data access request on behalf of the concerned minor, the data user may refuse to comply with the request.

4.7.14 In the light of the above analysis, we do not intend to implement this proposal.

(44) Fee Charging for Handling Data Access Requests (Proposal No. 18 in the Consultation Document)

Proposal in the Consultation Document

4.8.1 The proposal examines whether, for the purpose of imposition of a fee for complying with a data access request, a fee schedule should be provided in the PDPO and a data user should be required not to charge fees in excess of the prescribed maximum as set out in the said fee schedule.

4.8.2 Section 28 of the PDPO provides that a data user may, in complying with a data access request, impose a fee on a requestor for a copy of the personal data to be supplied and the fee thus imposed shall not be excessive. However, the term "excessive" is not defined in the PDPO. Over the years, the PCPD have received a number of complaints alleging that the fees charged by some data users were excessive.

4.8.3 In the UK, there are similar fee charging requirements for complying with data access requests. Under the UK Data Protection Act, a blanket statutory maximum fee at £10 for compliance with a data access request as prescribed by the Secretary of State by regulation is to apply except for prescribed cases governing access to credit reference records, manual health records and education records where separate prescribed limits are imposed.

4.8.4 One possible option suggested in the consultation document is to require a data user to set the fee for complying with a data access request at a level not exceeding the maximum permissible as prescribed in a fee schedule under the PDPO. To facilitate the determination of an appropriate fee for charging, the maximum level of fees for chargeable items will be prescribed in the fee schedule. These chargeable items may, among others, include photocopying, computer print-out, duplicate CD-Rom/DVD+R optical disc for audio recordings or visual images, duplicate of radiological imaging records, transcription of voice recording, postage and courier service charges. Where a chargeable item is not covered by the fee schedule, a data user may suitably impose a charge on condition that it is not excessive. The suggested maximum for the chargeable items may be set by reference to the costs involved

including labour costs and actual out-of-pocket expenses involved in locating, retrieving and reproducing the requested personal data.

4.8.5 The consultation document invited comments on the following:

(a) whether a data user should be required not to charge fees for complying with a data access request in excess of the prescribed maximum as set out in a fee schedule in the PDPO; and

(b) if yes, the parameters for setting the prescribed maximum in respect of any proposed fee charging model.

Views Received

4.8.6 Of the submissions received, 15% commented on this proposal. Of these, the majority were against implementing the proposal, some indicated support, while others made no clear indication of preference. Comments on the proposal were also received at the various consultation activities.

4.8.7 The main views of those who oppose the implementation of the proposal are as follows:

(i) as the system for storing personal data and the administrative situation may vary from one organisation (i.e. data user) to another, and the nature of personal data requested may also vary, it will be difficult to prescribe appropriate and standardised levels of maximum fees for all chargeable items[278];

(ii) with the advent of new technologies, the appropriate levels of maximum fees for various items may also have to be adjusted to keep pace with the rapid changes in technology. It may not be appropriate to prescribe a fee schedule in the legislation[279];

(iii) the present mechanism is effective. It gives data users the

---

278 Please refer to S0052, S0084, S0152 and S0156 of Annex 4.

279 Please refer to S0048, S0049, S0101 and S0156 of Annex 4.

flexibility of imposing charges according to their respective operational conditions. Also, it has already been provided in the PDPO that the fee imposed shall not be excessive. There are not sufficient justifications to introduce any change at present[280];

(iv) instead of rigidly defining what is "excessive", a more flexible approach should be adopted[281]; and

(v) a more appropriate approach is for the industry to introduce self-regulation. It is suggested that the relevant professional organisations or sector representatives should jointly formulate a set of proposed fee schedules for reference of the industry[282].

4.8.8 Respondents who support the implementation of this proposal raised the following views on details of implementation and individual submissions have commented on parameters for fee charging[283] as follows:

- the levels of maximum fees should reflect the nature of the data requested. The fees should cover both fixed and variable costs. The fixed cost should be paid at the time when an access of data request is lodged[284];

- in setting the fee levels, chargeable items should not be confined to general items but should cover administrative

---

280 For example, the Hong Kong Association of Banks (S0068) considers that the present mechanism should be retained as a complicated fee schedule may not only increase the administrative burden on data users, increase the cost of calculating fee charges in processing data access requests, but also more likely to encourage to disputes. The Hong Kong General Chamber of Commerce (S0119) points out that the present mechanism allows data users to charge a fee based on their operation costs. This could help to deter frivolous and irresponsible data access requests.

281 For example, PCCW (S0066) points out that retrieval of personal data in some major organisations, in particular those where new technologies are used to store personal data, could involve tiers of security checks or even higher ranking staff. As such, the costs in such organisations may not be the same as that assumed as handled by clerical or administrative staff.

282 Please refer to S0062 of Annex 4.

283 Please refer to S0104 and S0132 of Annex 4.

284 Please refer to S0080 of Annex 4. The Law Society of Hong Kong (S0073) and Hong Kong Human Rights Monitor (S0157) suggest that in addition to the payment of charges as suggested in the fee schedule, data requestors should be required to pay an administrative fee of $50 at the time of submitting the requests.

costs incurred in processing the requests, including expenditures associated with the involvement of various tiers of staff in complying with a data access request[285]; and

- the principle of not being "excessive" should be maintained so that data users will not be fixing charges at the maximum permissible levels in the schedule[286].

4.8.9 Some of those who support the general direction of the proposal share the concern as stated in paragraph 4.8.7(i) above[287]. There are views that a condition should be added such that data users would be allowed to charge above the maximum permissible if the data users could prove that the administrative cost incurred was higher than that prescribed in the schedule[288].

4.8.10 A respondent suggests that the public should be further consulted before the setting of parameters[289]. There are also views that instead of incorporating the fee schedule in the legislation, the schedule could be published and reviewed from time to time by the PCPD[290].

Proposed Way Forward

4.8.11 To sum up, the majority of the comments received are against implementing this proposal. Quite a number of respondents express concerns about how appropriate levels of maximum charges are to be determined. There are also comments that it is not appropriate to include in the legislation a fee schedule that requires revisions from time to time in the light of technological advancements. For the above reasons, we do not intend to take forward this proposal.

---

285 Please refer to S0091, S0124 and S0162 of Annex 4.

286 Please refer to S0080 of Annex 4.

287 Please refer to S0073 and S0080 of Annex 4.

288 Please refer to S0124 of Annex 4. Baker & McKenzie (S0124) points out that some data access requests require a data user to retrieve files dating many years back and thus incur a high time cost. Permitting organisations to charge requestors for the administrative costs incurred may help to deter some unreasonable or onerous data access requests.

289 Please refer to S0151 of Annex 4.

290 Please refer to S0124 of Annex 4.

Proposals Not to be Pursued as Indicated in the Consultation Document

4.9.1 Annex 2 to the consultation document set out a few proposals which we had considered but were inclined not to pursue. Having regard to the views received, we maintain the original stance of not pursuing those proposals. Annex 5 summarises those proposals, views received and our analyses.

Chapter Five: Conclusion

5.1 There is increasing concern about personal data privacy among the public. In this round of public consultation, the public put forward quite a number of views and concerns about various proposals.

5.2 As reflected from the views received, many proposals to strengthen the protection of personal data privacy in the consultation document have gained general support from the public. These include 37 major and miscellaneous amendment proposals set out in Chapter Three of this report such as strengthening regulation of data processors and sub-contracting activities, empowering the PCPD to provide legal assistance to an aggrieved data subject, making it an offence for a person who discloses for profits or malicious purposes personal data which he obtained from a data user without the latter's consent and empowering a third party to give prescribed consent to change of use of personal data. These proposals can enhance the protection of personal data privacy, or help address the practical problems encountered in the implementation of the current legislation. We intend to implement these proposals.

5.3 To address community concerns arising from the recent series of incidents of transfer of massive customer personal data by enterprises for direct marketing purposes without explicitly and specifically informing customers of the purpose of the transfer and the identity of the transferees and seeking the customers' consent, we have put forward a number of new proposals in Chapter Three to strengthen protection of personal data privacy in this regard.

5.4 On the other hand, the public are concerned about some proposals in the consultation document and have expressed worries about the implementation of some proposals. These proposals include those set out in Chapter Four of this report such as tightening the regulation of sensitive personal data, granting criminal investigation and prosecution power to the PCPD, making contravention of a DPP an offence, and restricting parents' right to access personal data of minors under certain circumstances. Respondents have expressed the following views :

(a) some proposals over-emphasise the protection of personal data privacy, failing to strike a balance between the protection of personal data privacy and other rights and public and social interests;

(b) for some proposals, having regard to the local situations, it is not the right time to implement those proposed new requirements;

(c) some legislative proposals will make the PDPO less flexible; and

(d) some proposals will impose onerous burden on business operations and individual data users, hinder continued development of information and communications technology, and undermine Hong Kong's competitiveness and economic efficiency as an international city.

5.5 Having regard to the principles guiding this review as set out in Chapter One of this report and the importance of a consensus in the community on the proposed requirements, we do not intend to take forward the proposals set out in Chapter Four.

5.6 We have formulated general directions on the way forward. We welcome public views on the specific arrangements and details of the proposals planned to be taken forward. In addition, we shall arrange to meet with relevant organisations or stakeholders for in-depth discussions on the details of the proposals planned to be take forward, including the contents of the legislative amendments, so as to ensure smooth operation of the amended PDPO.

An 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.

Annex 2

Summary of the First Public Forum

Date: 18 September 2009 (Friday)
Time: 7:00 p.m. – 9:00 p.m.
Venue: Youth Square, Chai Wan
Organiser: Constitutional and Mainland Affairs Bureau

Sensitive Personal Data

1. A participant was of the view that with the rapid development of technologies, leakage of sensitive personal data could cause very harmful damage. To better protect personal data privacy, the Government should impose more stringent regulation on the processing of sensitive personal data. The participant also supported the classification of biometric data as sensitive personal data for more stringent control.

2. However, some participants expressed concern about the enormous difficulties that the proposal would pose to the information technology sector in the implementation of systems which identified individuals by means of their fingerprints. They pointed out that under the current practice of the information technology sector, only a few attributes of fingerprints were taken and digitalised for record purpose. Since the digital data were not reversible, they should not be regarded as personal data, and in particular, as sensitive personal data. The collection and use of these data should not be subject to stringent restriction.

3. Moreover, they pointed out that apart from biometric data, many other types of personal data, for example, personal health records, were sensitive in nature. They, therefore, considered that the Government should not single biometric data out as sensitive personal data, which would undermine the development of the industry.

4. A participant raised the point that a lot of employers requested their staff to provide biometric data for security and attendance record purposes. Very often, the staff acceded to their employers' request reluctantly. After collecting the data, however, the employers might not be able to safeguard the security of the data

properly. It was, therefore, hoped that the Administration and the Office of the PCPD would step up publicity on the proper processing of biometric data.

Regulation of Data Processors and Sub-contracting Activities

5. A participant agreed that there was a need for data users to assume a more proactive role in monitoring the performance of data processors with regard to data security. He also supported the imposition of specific duties and obligations upon data processors to adopt of suitable security safeguards to protect the security of personal data transferred to them for handling.

6. The participant supported direct regulation on the activities of data processors as he reckoned that indirect regulation would not be an effective means. He suggested that the Government should consider requiring mandatory registration for both data processors and data users by making reference to overseas practice in this regard.

Personal Data Security Breach Notification

7. Participants agreed that a privacy breach notification system should be instituted to require the organisations concerned to notify the PCPD and affected individuals when there was leakage of personal data so as to mitigate the potential damage to the affected individuals.

8. A participant was of the view that maximum effectiveness could not be achieved unless the privacy breach notification system was made mandatory. He opined that if the privacy breach notification system was introduced on a voluntary basis, there would not be sufficient incentive for data users to give notification of data leakage incidents, and the system might hence not be able to provide adequate safeguard to data subjects.

9. A participant also suggested that the privacy breach notification system should equally apply to data processors if the proposal was to be implemented.

Raising Penalty for Misuse of Personal Data in Direct Marketing

10. Most of the participants had the experience of receiving direct marketing calls and found the calls annoying. Concerned about the current practice of direct marketing companies, they considered that the Administration should enhance regulation and take measures to contain the problem as soon as possible.

11. Specifically, a participant suggested that the Administration should take measures to stem the unauthorised sale of customers' personal data to direct marketing companies, lest the personal data privacy of data subjects would be damaged.

Erasure of Personal Data

12. A participant expressed his support for the relaxation of the current statutory requirement for erasure of personal data so that the provisions concerned would be regarded as having been complied with if a data user could prove that he had taken all reasonably practicable steps to erase personal data no longer required for the fulfillment of the purpose of use. The participant was of the view that it could effectively relieve the administrative burden on companies if the proposal was implemented.

Balance between Personal Data Privacy Protection and Ethical and Moral Values

13. A participant raised the paramount importance of striking a balance between personal data privacy protection and ethical and moral values. The point was therefore put forward that the coverage of the Ordinance should not be extended indefinitely, and that in particular, parents' responsibilities over their children should not be denied on the ground of privacy protection.

Other Views

14. At the forum, some participants enquired about the definition of personal data and the regulation on data security under the current legislation.

Summary of the Second Public Forum

Date: 30 October 2009 (Friday)
Time: 7:00 p.m. – 9:00 p.m.
Venue: Cultural Activities Hall of Tsuen Wan Town Hall
Organiser: Constitutional and Mainland Affairs Bureau

Personal Data Security Breach Notification

1. Regarding the proposal for a privacy breach notification system, participants concurred that the spate of personal data leakage incidents had aroused concern within the community and that measures should be taken to mitigate the potential damage to individuals affected by leakage of personal data.

2. Nevertheless, a participant was of the view that instead of requiring organisations to notify the Office of the PCPD and affected individuals whenever there was leakage of personal data, the Office of the PCPD should formulate a code of best practice for organisations to follow in case of personal data leakage.

Parents' Right to Access Personal Data of Minors

3. A participant agreed that data users should be given the authority to decide whether a data access request made by a "relevant person" on behalf of a minor should be refused, provided that the decision was made in the best interests of the minor.

4. He made a point that the general principles in respect of the proposal should be laid down by the Office of the PCPD. However, in view of the different operational problems encountered by different sectors in processing personal data, he suggested that professional organisations should be allowed to make their own decisions on the implementation details.

5. On the other hand, a participant, while stating that he understood this proposal was meant for the interests of the minors, stressed that the Administration had to respect and safeguard parents' responsibilities for taking care of their children as well. Another participant expressed concern about the implementation details of the proposal. He pointed out that in deciding whether the access

requests made by parents should be denied, data users might not be able to judge whether the requests were in the best interests of the data subjects.

6. In view of the deteriorating youth problem in particular, a participant opined that while protection of personal data should be enhanced, it had to be ensured that the amendments would not become a barrier to parents taking care of their children.

Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

7. A participant agreed that data users should be allowed to transfer, of their own accord, the personal data of minors to their parents or guardians, provided that this was in the best interests of the minors.

8. A participant stated that while he understood that this proposal was meant for the interests of minors, the wishes of the minors should also be respected.

Territorial Scope of the PDPO

9. At present, the PDPO applies where a data user controls the processing of data in or from Hong Kong even if the whole data processing cycle occurs outside Hong Kong. The PCPD proposes that the PDPO should not apply where none of the acts of the data processing cycle takes place in Hong Kong.

10. A participant pointed out that more and more companies were engaged in contracts for processing personal data outside Hong Kong. If the proposal was implemented, there should be a corresponding mechanism for follow-up actions so as to plug the loopholes in case of data leakage. In addition, data subjects should be notified of the identities of data processors to facilitate their consideration of the choice of service.

Strengthening of Education and Publicity

11. At the public forum, some participants were of the view that public awareness of protection for personal data privacy was insufficient. They suggested that education and publicity be strengthened to promote public vigilance towards protection of personal data privacy. More importantly, data users should be helped to clearly

understand the relevant legislation.

Obligations on Data Users

12. In addition, some participants stated that data users (particularly commercial organisations which used data for commercial purposes) should have the responsibility to pay the cost for ensuring protection of personal data privacy, rather than unilaterally considering cost-effectiveness only.

Other Views

13. At the forum, some participants enquired how personal data privacy was monitored and protected under the current legislation in certain circumstances, e.g. in the collection of personal data for the purpose of mailing election-related materials during the election period, in the collection of personal data by individual companies for promotion purpose, and in the collection of personal data by companies during job interviews.

Annex 3

List of Organisations Met by the Administration during the Consultation Period

	Organisation	Date of Meeting
1.	Technology and Creative Industry Group of the Professional Affairs Committee of the Democratic Alliance for the Betterment and Progress of Hong Kong	22 September
2.	Children's Rights Forum	25 September
3.	Internet Professional Association and Office of the Hon. Samson Tam (Information Technology)	5 October
4.	Hong Kong Information Technology Federation, Information and Software Industry Association, Hong Kong Wireless Technology Industry Association, Internet Society Hong Kong, Professional Information Security Association, Hong Kong Internet Service Providers Association and Hong Kong Association of Interactive Marketing	14 October
5.	Human Rights Forum	22 October
6.	Hong Kong Institution of Engineers	22 October
7.	Hong Kong Jewelry Manufacturers' Association and Hong Kong Chamber of Small and Medium Business Ltd.	3 November
8.	Hong Kong Institute of Human Resource Management	6 November
9.	Children's Rights Forum	13 November
10.	Law and Technology Centre of the Faculty of Law of the University of Hong Kong	16 November

Annex 4

Written Submissions

Annex 4 is available for public inspection at the Public Enquiry Service Centres of the District Offices of the Home Affairs Department or can be downloaded from the CMAB website (http://www.cmab.gov.hk).

Proposals Not to be Pursued as Indicated in the Consultation Document

1. Annex 2 to the consultation document set out a few proposals which we had considered but were inclined not to pursue. The following paragraphs summarise these proposals and the views received. Having considered the views received, we maintain the original stance that we do not intend to pursue these proposals.

Scope of Regulation under the PDPO

Internet Protocol Address as Personal Data (A.2 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

2. The consultation document indicated that we did not intend to regard an Internet Protocol address ("IP address") alone as personal data as defined under the PDPO.

3. Under the PDPO, personal data means any data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

4. An IP address is a unique number to enable electronic devices to identify and communicate with each other on a computer network. When an electronic device communicates with others through the Internet, an IP address has to be assigned to it for identification purpose.

5. In March 2006, the PCPD received a complaint alleging that the disclosure of an e-mail subscriber's personal data by an e-mail service provider had infringed the provisions of the PDPO. In his investigation report issued in March 2007, the PCPD took the view that an IP address *per se* does not meet the definition of "personal data", because IP address is about an inanimate device, not an individual. It alone can neither reveal the exact location of the

electronic device concerned nor the identity of the user.

6. There is a need to strike a balance between protection of personal data privacy and normal business operation. Deeming IP address *per se* as personal data would pose unreasonable burden on and serious compliance problems for players in the information technology industry. For instance, it is not practicable for the industry to comply with DPP 4 (security of personal data principle). In transmitting information on the Internet, such as sending e-mail or browsing websites, the server will collect and display the IP addresses of the sender and the recipient to ensure delivery of information to the intended address. If IP address *per se* is regarded as personal data, then all Internet service providers have to act according to DPP 1 to inform each and every Internet user of the purpose for which the data are to be collected and the classes of persons to whom the data may be transferred. This will impose onerous burden upon Internet service providers.

7. In the light of the above, the consultation document considered it inappropriate to deem IP address *per se* as personal data under the PDPO. However, if an IP address is combined with other identifying particulars of an individual making them capable of identifying a particular individual through tracing, they will be afforded protection under the PDPO.

Views Received

8. Of the submissions received, only a few expressed views on this proposal. During the consultation activities, there were individual participants who gave their views on this.

9. Of the submissions which have expressed views on this matter, the majority agree to the Administration's stance of not taking this proposal forward. There are also individual views that the proposal should be implemented or an open mind be adopted.

10. Those who support not implementing the proposal all agree with the justifications mentioned in the consultation document. They point out that IP address is about an inanimate device which alone can neither reveal the exact location of the electronic device concerned nor the identity of the user. Therefore, IP address

should not be regarded as personal data[291].

11. A respondent who holds an open mind also agree with the considerations set out in the consultation document. In particular, they point out that IP addresses are dynamic (as a new IP address will be given to an electronic device each time when it communicates with other devices through the Internet) and may not be able to reveal the identity of the user[292].

12. Respondents who suggest following up the proposal point out that IP address if disclosed together with other identifying personal particulars may identify the user concerned. They suggest that it may not be impracticable to regard IP address as personal data and require the industry to comply with the requirements. They suggest that the Government should conduct another comprehensive public consultation exercise on the premise of offering the best protection for personal data[293].

Proposed Way Forward

13. IP address, whether dynamic or permanent, will not change its nature. IP address alone can neither reveal the exact location of the electronic device concerned nor the identity of the user. For example, even if an electronic device is given a permanent IP address, it may be owned or used by more than one person. Therefore, IP address alone cannot identify the user and so it does not fall within the definition of "personal data".

14. Moreover, if an IP address is used in conjunction with other identifying particulars of an individual, those data are already afforded protection under the PDPO.

15. In the light of the above, we maintain the stance that IP address

---

291 Please refer to S0124 and S0135 of Annex 4. The Liberal Party (S0135) agrees with the considerations in the consultation document and considers it not necessary to include IP address as personal data at this stage but suggests a review at an appropriate time as technology develops.

292 While the Office of the PCPD (S0097) is open-minded about the proposal, it points out that as IP address will appear on the first page of an e-mail, subjecting it to the protection of the PDPO may give rise to practical difficulties. This may also impose an onerous burden on Internet service providers and e-mail service providers, in particular that they have no intention to collect any personal data when distributing IP addresses randomly.

293 Please refer to S0157 and S0178 of Annex 4.

should not be regarded as "personal data" as defined under the PDPO.

Territorial Scope of the PDPO
(A.3 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

16. It was stated in the consultation document that the following proposal was not intended to be pursued: to narrow the territorial scope of the PDPO so much so that where none of the acts of the data processing cycle took place in Hong Kong, the PDPO should not apply.

17. At present, the PDPO applies where a data user controls the processing of data in or from Hong Kong even if the whole data processing cycle occurs outside Hong Kong. The territorial scope of the data protection law for Hong Kong was thoroughly discussed by the LRC in 1994, on the basis of which the Administration decided on the scope of control under the PDPO. We also made reference to the model of the UK when formulating the existing regulatory provisions. The LRC considered it important that data protection law of Hong Kong should apply to a data user within its jurisdiction, even where the data have been transferred to or are being processed in another jurisdiction. This approach also applies to the provisions relating to cross-border data flow.

18. This proposal, if implemented, might create a loophole in our control regime in that a company in Hong Kong can bypass the PDPO by arranging offshore collection of personal data through an agent and outsourcing the holding, processing and use of the personal data to offshore agent(s). This may risk Hong Kong losing effective control on personal data, which would not be in the interest of promoting the free flow of data to Hong Kong.

Views Received

19. Of the submissions received, only a few expressed views on this proposal. During the consultation activities, only individual participants expressed views on this proposal.

20. Of the submissions received, some agreed with the position in the consultation document of not pursuing the proposal while some considered that the proposal should be implemented.

21. Respondents who agree not to pursue the proposal concur with the analysis in the consultation document that the proposal could create loopholes in the regulatory regime of personal data and turn Hong Kong into a data haven without effective control on personal data[294].

22. Respondents who consider that the proposal should be implemented suggest that the Administration should consider putting in place a mechanism to plug the possible loopholes in the law[295].

23. Also, some views point out that the proposal, if implemented, should make it mandatory to inform the data subject of the identity of the data processor (i.e. the service provider), whether the processing is done outside Hong Kong and whether the processing is subject to the regulation of the PDPO, for the data subject's reference in choosing the service provider.

Proposed Way Forward

24. Precedents show that in handling cases where the data processing cycle takes place outside Hong Kong, the Office of the PCPD could still obtain evidence and conduct investigation pursuant to the PDPO.

25. The proposal, if implemented, will narrow the territorial scope of the PDPO. Even though the data user is in Hong Kong or controls the data processing from Hong Kong, so long as the processing cycle does not take place in Hong Kong, the personal

---

294 Please refer to S0157 of Annex 4.

295 Please refer to S0124 of Annex 4. The Office of the PCPD (S0097) also supports the implementation of the proposal as the PCPD encounters practical difficulties in collecting evidence or enforcing the law where data cycle of personal data in question takes place outside Hong Kong. Owners of overseas businesses or factories could not have expected that they have to comply with the PDPO, being a Hong Kong law, in protecting the personal data of the overseas employees. In addition, where there is a conflict of law situation, the owner will face the dilemma of either breaching the PDPO if it authorises disclosure of the personal data to a foreign law enforcement authority or face the legal consequence (sometimes involving criminal sanction) under the applicable foreign law if it fails to comply with the lawful order issued under that law.

data involved will not be subject to the regulation of the PDPO. This may create loopholes in our regulatory regime.

26. In view of the above, we maintain the stance in the consultation document that we do not intend to take forward this proposal.

Exemptions

Public Interest Determination
(B.1 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

27. The proposal examines whether to empower the PCPD to, upon application by the relevant data user, make a public interest determination and impose conditions on a case-by-case basis.

28. At present, specific exemptions from access to personal data by the data subject (DPP 6 and section 18(1)(b) of the PDPO) and Use Limitation Principle (DPP 3) are provided for under Part VIII of the PDPO on grounds of specified public interests, including security in respect of Hong Kong (section 57), crime (section 58) and health (section 59). The PDPO, however, does not contain a general provision that makes the protection of public interest itself a justification for exemption.

29. To provide for regulatory flexibility when public interest outweighs the protection of personal data privacy, we have considered whether to add a new provision to empower the PCPD to, upon application by the relevant data user, make a public interest determination (including a temporary public interest determination for applications which require urgent decision) and impose conditions on a case-by-case basis.

30. Nevertheless, the abovementioned public interest determination mechanism will operate on an ad hoc and a case-by-case basis. Such a mechanism will undermine the certainty of personal data privacy protection afforded by the PDPO to data subjects. As such, the consultation document indicated reservation on this proposal and considered that if there were justifications to grant exemption on specific grounds, it would be more appropriate to address them by way of specific public interest exemptions.

Views Received

31. Of the submissions received, only a few expressed views on this proposal. During the consultation activities, no participants expressed views on this proposal.

32. Of the submissions received which expressed views on this proposal, the majority agreed with the consultation document that the proposal should not be pursued[296] while a minority suggested pursuing the proposal[297]. There were also individual respondents who indicated that they had no comment.

Proposed Way Forward

33. The existing exemptions provisions under the PDPO already grant exemptions under specific circumstances. This strikes a balance between protecting personal data privacy and public interest.

34. Respondents also agree in general that the proposal should not be pursued. We maintain the stance in the consultation document that we do not intend to take forward this proposal.

Public Domain Exemption
(B.2 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

35. The proposal examines whether to provide an exemption from the Use Limitation Principle (DPP 3) for personal data available in the public domain.

36. In making this proposal, the PCPD also acknowledges that there are problems of using publicly available information for secondary purposes. These include the use of property owners' records from the Land Registry to make a search of an individual's property ownership, the use of personal data contained in public registers for

296 Please refer to S0048, S0049, S0080 and S0101 of Annex 4.

297 The Office of the PCPD (S0097) points out that the proposal provides a direct solution to enable a data user to release the relevant data in the public interest without contravening DPP 3 where the circumstances require a timely disclosure. Also, a general public interest exemption would provide flexibility for and encompass all appropriate case if there is justification to grant the exemption on specific grounds. Baker & McKenzie (S0124) does not object to this proposal on the assumption that the PCPD would not abuse the exemption. Please also refer to S0157 of Annex 4.

direct marketing activities, and the improper use of personal data available on the Internet arising from data leakage incidents. On the other hand, there may be legitimate purposes to serve in checking an individual's financial status, such as property ownership, before deciding whether to institute legal proceedings or pursue enforcement actions against that individual.

37. The LRC had carefully deliberated on whether data protection laws should completely exempt public registers. The LRC expressed concerns that such an exemption would sanction data collected for specific purposes being used for another purpose not originally envisaged by the person furnishing the data. The LRC concluded that "there should be an exemption from the application of the Use Limitation Principle (i.e. DPP 3) for data which are required by or under any enactment to be made available to the public" but "should the data be applied for another purpose, the data protection law would apply at that point."

38. There is no public domain exemption in personal data protection laws of the UK, New Zealand and Australia. The consultation document was of the view that putting personal data in the public domain did not make the data available for use for any purpose. If the test for exemption is simply whether the data are in the public domain, data users may get around the law by publicising the data. The proposal could result in abuse in the use of information available in the public domain, such as improper use of personal data available on the Internet arising from data leakage incidents. We do not see sufficient justifications for taking this proposal forward. We, therefore, stated in the consultation document that we did not intend to pursue this proposal.

Views Received

39. Of the submissions received, only a few expressed views on this proposal. During the consultation activities, no participants expressed views on this proposal.

40. Of the submissions received which expressed views on this proposal, the majority agreed with the consultation document that the proposal should not be pursued[298]. No other views indicated support for the proposal. There were individual respondents who

[298] Please refer to S0048, S0049, S0080, S0101, S0124 and S0157 of Annex 4.

indicated they had no comment.

Proposed Way Forward

41. In the light of the analyses in paragraphs 36 to 38 above and that the views received agree in general that this proposal should not be pursued, we maintain the stance in the consultation document that we do not intend to take forward this proposal.

Powers of the PCPD

Power to Search and Seize Evidence (C.1 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

42. The proposal examines whether the PCPD should be empowered to search and seize evidence in order to gather evidence for prosecution proceedings.

43. The PCPD is empowered under the PDPO to be furnished with any information, document or thing from any person, enter premises, summon witnesses, and conduct hearing. The PCPD, however, has no power to search and seize evidence. The PCPD proposes that he should be empowered to search and seize evidence in order to gather evidence for prosecution proceedings.

44. The existing provisions of the PDPO are to address the concern raised during the legislative process that this newly established investigative body should not be vested with full powers of search and seizure. Similar concern was raised by the LRC. While the LRC considered that powers to enter premises and obtain evidence are necessary to enable the PCPD to carry out his functions, the data user's consent should first be sought and if that is not forthcoming, it should be for the court to make an appropriate order for entry and seizure.

45. It was mentioned in the consultation document that the additional powers proposed were to facilitate the PCPD to carry out criminal investigations. Since we do not see a strong case to grant the PCPD criminal investigation and direct prosecution power, there is no need to provide these additional powers to the PCPD. We also consider the existing investigative power of the PCPD adequate.

In the circumstances, we are not inclined to take forward the proposal.

Views Received

46. Of the submissions received, only a handful of respondents commented on this proposal. During the various consultation activities, no participants expressed views on this proposal.

47. Of the submissions which expressed views on this proposal, the majority agree with the consultation document that the proposal should not be pursued[299] and a minority suggest pursuing the proposal[300]. There are also respondents who indicate that they have no comment.

Proposed Way Forward

48. The additional powers proposed are to facilitate the PCPD to carry out criminal investigations. Since we do not see a strong case to grant the PCPD criminal investigation and direct prosecution power (see Proposal (39) of this report), there is no need to provide these additional powers to the PCPD. Also, having regard to the consideration in paragraph 44, we maintain the stance in the consultation document that we do not intend to take forward this proposal.

Power to Call upon Public Officers for Assistance (C.2 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

49. The proposal examines whether the PCPD should be empowered to call upon public officers to assist him in his discharge of investigation and inspections.

50. In the exercise of his investigation and inspection power, the PCPD may need to enter premises. Where resistance or obstruction is encountered, the PCPD would need to seek assistance from the

---

299 Please refer to S0048, S0049, S0080, S0101 and S0124 of Annex 4.

300 Please refer to S0097 and S0157 of Annex 4. The Office of the PCPD (S0097) points out that this proposal and the proposal to grant criminal investigation and prosecution power to the PCPD (Proposal (39) of this report) should be bundled with each other and considered together.

Police. Expert advice and assistance are also required in investigation. At present, the PCPD is not empowered under the PDPO to call upon public officers to assist him in his discharge of investigation and inspections. He can only rely on the goodwill of public officers for assistance. The PCPD proposes to provide the PCPD with an express power to call upon public officers to assist him in performing the regulatory functions under the PDPO. The PCPD envisages that an express provision would be necessary when he is conferred with the power to investigate offence and institute prosecution.

51. Public officers have all along been providing assistance to the PCPD in the discharge of his regulatory functions in the absence of a specific provision to such effect in the PDPO. We do not see a need for specific provisions in the PDPO if the PCPD simply requests assistance of officers of Government departments. In this regard, it is an offence under section 64(9) of the PDPO for a person to, without lawful excuse, obstruct, hinder or resist the PCPD or any other person in the performance of the PCPD's functions or the exercise of his powers under Part VII (inspections, complaints and investigations). In the circumstances, the consultation document suggested that this proposal needed not be pursued.

Views Received

52. Of the submissions received, only a handful of respondents commented on this proposal. During the various consultation activities, no participants expressed views on this proposal.

53. Of the submissions which expressed views on this proposal, the majority agree with the consultation document that the proposal should not be pursued[301]. A minority suggest pursuing the proposal[302]. There are also respondents who indicate that they have no comment.

---

301 Please refer to S0048, S0049, S0080 and S0101 of Annex 4.

302 Baker & McKenzie (S0124) considers that if public officers have all along been providing assistance to the PCPD in the discharge of his regulatory functions as suggested in the consultation document, then the making of an express provision in the law should not be objectionable. The Office of the PCPD (S0097) points out that this proposal and the proposal to grant criminal investigation and prosecution power to the PCPD should be bundled with each other and considered together. Please also refer to S0157 of Annex 4.

Proposed Way Forward

54. Public officers have all along been providing assistance to the PCPD in the discharge of his regulatory functions. Furthermore, we do not intend to empower the PCPD to conduct criminal investigation and prosecution (please see Proposal (39) of this report). So, there is no need to add the proposed express provision in the PDPO. The submissions received in general also agree that the proposal should not be pursued. We maintain the stance in the consultation document that we do not intend to take forward this proposal.

Power to Conduct Hearing in Public
(C.3 in Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

55. The proposal examines whether the PCPD should be conferred the power to decide whether a hearing should be held in public having regard to all the circumstances of the case.

56. Section 43(2) of the PDPO provides that any hearing for the purpose of an investigation shall be carried out in public unless the PCPD considers otherwise or the complainant requests that the hearing be held in private. We have considered whether the PCPD should be conferred the power to decide whether a hearing should be held in public having regard to all the circumstances of the case including any request made by a complainant.

57. The right to demand a private hearing by the data subject is a conscious recommendation made by the LRC on grounds that the prospect of a public hearing could act as a real disincentive to the lodging of a complaint. As regards overseas practices, Australia requires conferences in relation to a complaint to be conducted in private, and New Zealand has similar requirement for the conduct of investigations.

58. The LRC's considerations for granting the data subject the right to demand a private hearing are still valid today. The consultation document stated that we did not see a need to change the system. In this regard, section 48(2) of the PDPO empowers the PCPD to publish a report on the result of the investigation as well as the recommendations thereof, if he is in the opinion that it is in the

public interest to do so. The right of the public to know and be informed can, to a certain extent, be taken care of in that context.

Views Received

59. Of the submissions received, only a handful of respondents commented on this proposal. During the various consultation activities, no participants expressed views on this proposal.

60. Of the submissions which expressed views on this proposal, the majority agree with the consultation document that the proposal should not be pursued[303]. A minority suggest pursuing the proposal[304]. Respondents mostly did not give details of the reason for support or objection. There are also respondents who have no comment.

Proposed Way Forward

61. Taking into consideration the concerns in paragraphs 57 to 58 above, and that the submissions received in general agree that the proposal should not be pursued, we maintain the stance in the consultation document that we do not intend to take forward this proposal.

Time Limit for Responding to PCPD's Investigation / Inspection Report
(C.4 of Annex 2 to the Consultation Document)

Proposal not to be pursued as indicated in the consultation document

62. The proposal examines whether the time limit for responding to PCPD's investigation/inspection report should be shortened from 28 days to 14 days.

63. A data user is currently allowed under section 46(4)(b) to advise the PCPD within 28 days whether he objects to the disclosure in inspection / investigation report prepared by the PCPD any personal data that are exempt from the provisions of DPP 6 by

---

303 Please refer to S0048, S0049, S0080, S0101, S0124 and S0175 of Annex 4.

304 The Office of the PCPD (S0097) opines that the provision under section 48(2) is too restrictive. In cases when issues of public interest and importance are involved, members of the public should have a genuine right to know and to be informed. Please also refer to S0157 of Annex 4.

virtue of Part VIII (exemptions) of the PDPO before its publication. The PCPD proposes to shorten the period from 28 days to 14 days on the ground that the present response period of 28 days hinders timely reporting of matters of public interest.

64. Data users in some cases may need to circulate the report for comments and seek legal advice before they can provide a formal response to the PCPD. Such a course of action takes time. A response period of 14 days is unreasonably tight. Furthermore, shortening of the response period by 14 days will not significantly improve the timeliness of publication of an inspection or investigation report. The consultation document did not consider it appropriate to take forward the proposal.

Views Received

65. Of the submissions received, only a handful of respondents expressed views on this proposal. During the consultation activities, no participant expressed any views on this proposal.

66. Of the submissions which expressed views on this proposal, the majority agree with the consultation document that the proposal should not be pursued[305]. The PCPD suggests pursuing the proposal[306] while nobody else express support for the proposal. There are individuals who said they had no comment.

Proposed Way Forward

67. Taking into consideration the concerns in paragraph 64 above and also that the submissions received generally agree that the proposal should not be pursued, we maintain the stance in the consultation document that we do not intend to take forward this proposal.

---

[305] Please refer to S0048, S0049, S0080, S0101, S0124, S0156 and S0157 of Annex 4.

[306] Please refer to S0097 of Annex 4.