Consultation Document on Review of the Personal Data (Privacy) Ordinance

August 2009

Contents

Foreword

The Constitutional and Mainland Affairs Bureau, with the support of the Privacy Commissioner for Personal Data ("PCPD"), has conducted a comprehensive review of the Personal Data (Privacy) Ordinance ("PDPO") to examine whether the existing provisions of the Ordinance still afford adequate protection to personal data having regard to developments, including advancement in technology, in the last decade. This document sets out the findings of the review.

The proposed amendments to the PDPO may have profound impact on various sectors of the community, public and private organizations as well as members of the public. We see the need to conduct a public consultation exercise to gauge public views on the proposals, before deciding on the way forward.

Please send us your views and comments by mail, facsimile or email **on or before 30 November 2009** :

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

It is voluntary for any member of the public to supply his/her personal data upon providing views on the consultation document. Any personal data provided with a submission will only be used for the purpose of this consultation exercise.

The submissions and personal data collected may be transferred to the relevant Government bureaux and departments and the Office of the PCPD for purposes directly related to this consultation exercise. The Government bureaux and departments, and the Office of the PCPD receiving the data are bound by such purposes in their subsequent use of such data.

The names and views of individuals and organisations which put forth submissions in response to the consultation document ("senders") may be published for public viewing after conclusion of the public consultation exercise. This Bureau may, either in discussion with others or in any subsequent report, whether privately or publicly, attribute comments submitted in response to the consultation paper. We will respect the wish of senders to remain anonymous and/or keep the views confidential in relation to all or part of a submission; but if no such wish is indicated, it will be assumed that the sender can be named.

Any sender providing personal data to this Bureau 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 to:

Assistant Secretary (Constitutional and Mainland Affairs)4B
3/F, East Wing
Central Government Offices
Lower Albert Road
Hong Kong
Fax number: 2523 0565
(Email Address: pdpo_consultation@cmab.gov.hk)

Constitutional and Mainland Affairs Bureau
August 2009

Executive Summary

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

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

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

Guiding Principles

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

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

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

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

(d) the need to avoid putting onerous burden on business operations

and individual data users;

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

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

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

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

Invitation of Views

5. A considerable number of the proposals identified in the review will impact on various sectors of the community, public and private organizations as well as members of the public. We have an open mind on the proposals and we welcome your views in this regard. Following this round of public consultation, we will consolidate the views received. When we have general directions on the way forward, we will arrange for further public discussions on possible legislative proposals.

Proposals

6. The key proposals concerning sensitive personal data, data security, enforcement powers of the PCPD, and offences and sanctions are set out in Chapters Three to Six of the consultation paper. Other proposals which have considerable impact on the community on which comments are invited are set out in Annex 1. Those proposals which the Administration has considered but is inclined not to pursue are set out in Annex 2. Miscellaneous proposals which include mainly operational and procedural amendments to streamline the operation of the PDPO and address technical and operational problems encountered in the implementation of the PDPO are at Annex 3.

7. The key proposals are highlighted in paragraphs 8 to 23 below.

Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

8. At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. More stringent regulation of sensitive personal data is in line with international practices. However, there is no universally agreed set of sensitive personal data and perception of sensitive personal data is culture-bound. Given the challenges posed by the development of biometric technology on an individual's privacy, as a start we may consider classifying biometric data (such as iris characteristics, hand contour reading and fingerprints) as sensitive personal data.

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

Data Security

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

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

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

12. As part of the options, we can consider directly regulating data processors by imposing obligations on them. They would be required to exercise the same level of due diligence as the data user with regard to security, retention and use of the personal data thus entrusted.

Recognising that compliance with certain requirements may pose problems for some data processors due to the operational constraints unique to specific industry sectors, we have also included the option of subjecting different categories of data processors to different obligations.

Proposal No. 3: Personal Data Security Breach Notification

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

Enforcement Powers of the PCPD

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

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

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

15. Under Section 66 of the Ordinance, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user. The PDPO does not empower the PCPD to provide

assistance to aggrieved data subjects in respect of legal proceedings. To achieve greater deterrent effect on acts or practices which intrude into personal data privacy and enhance the overall effectiveness of sanctions provided for under the PDPO, views are invited on whether the PCPD should be conferred the power to provide legal assistance to an aggrieved data subject.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

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

Offences and Sanctions

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

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

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

should make contravention of a DPP an offence.

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

19. Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. To curb irresponsible dissemination of leaked personal data, we may consider making it an offence if a person obtains personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes.

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

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

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

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

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

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

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

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

Chapter One : Introduction

1.01 The Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) has been in force since 1996. During the last decade, we witnessed the rapid advancement in information technology, prevalence of the Internet and exponential growth of e-commerce. Increasing use of information and communications technology is important for moving business and production up the value-chain and improving the quality of life of our citizens. It also helps enhance Hong Kong's competitiveness and efficiency, and bring more convenient and user-friendly services to the community. At the same time, it has brought new challenges to the protection of personal data privacy, because such technological advancements have made possible almost instant acquisition and retention, processing, retrieval and transfer of vast amounts of personal data. It is important to ascertain the adequacy of the PDPO in coping with the challenges posed in this information age. A review of the Ordinance is therefore timely.

1.02 In the international scene, a number of governments and privacy regulators see a need to review their data protection laws to address the privacy impact brought about by such technological advancements. For example, Australia, Canada, New Zealand and the United Kingdom are reviewing their data protection laws.

1.03 Locally, the series of personal data leakage incidents as well as instances of dissemination of leaked personal data on the Internet have aroused community concern with regard to the serious intrusion into personal data privacy, as well as the risk of identity theft and identify fraud. Some legislators have expressed concern about the lack of a system to notify the Privacy Commissioner for Personal Data ("PCPD") and affected data subjects in the event of personal data security breach. There were suggestions that the Administration should consider giving more power to the PCPD to enforce the PDPO. Questions were also raised as to whether the existing sanctions provided for under the PDPO are adequate to achieve deterrent effect.

1.04 Separately, the PCPD has, in the light of his regulatory experience in discharging his functions and powers under the PDPO, come up with proposals to improve the implementation of the Ordinance and to clarify certain provisions.

1.05 With the support of the PCPD, we have conducted this comprehensive review of the PDPO to examine whether the existing provisions of the Ordinance still afford adequate protection to personal data having regard to the following :

(a) the privacy impact of technological advancements in this electronic age which facilitate the collection, holding, processing and transmission of massive personal data almost instantaneously;

(b) the regulatory experience of the PCPD in discharging his functions and powers;

(c) the difficulties so far encountered in the implementation of certain provisions of the Ordinance; and

(d) the development of international personal data privacy laws and standards since the enactment of the Ordinance.

In the process, we have, among others, reviewed privacy issues emanating from technological advancements, the scope of control of the Ordinance, data security, powers of the PCPD, and adequacy of sanctions in combating invasions of personal data privacy.

1.06 In conducting the review, we are guided by the following :

(a) while the PDPO should provide adequate protection to personal data, the right of individuals to privacy is not absolute. It must be balanced against other rights, as well as certain public and social interests and with reference to the particular circumstances in which they arise;

(b) the need to balance the interests of different sectors/stakeholders. For instance, a suitable 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 in complying with the requirements of the PDPO;

(e) while we see a need to keep abreast of the development of international privacy laws and standards, due account should be given to local situations as perceptions of privacy are dynamic and culture-bound;

(f) the need to ensure that the PDPO would remain flexible and relevant in spite of technological change, and that the provisions in the PDPO should remain technologically neutral as far as possible;

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

(h) a reasonable degree of consensus in the community about the privacy issues is important for providing a stable environment for implementation of the legislation.

1.07 The review of the PDPO covers fundamental issues which affect the rights and civil liberties of individuals. A considerable number of the proposals will impact on various sectors of the community, public and private organizations as well as members of the public. A number of amendment proposals, especially those relating to the regulation of sensitive personal data and data processors and personal data security breach notifications, might incur additional compliance cost for business operations. On the other hand, enhancing the protection to personal data privacy would safeguard the free flow of personal data involved in financial and economic activities to Hong Kong, which would be in the interests of business operations of Hong Kong. A balance has to be struck between the compliance cost for the community as against the benefits of enhanced personal data protection. Any amendments to the PDPO should not be at the expense of Hong Kong's competitiveness.

1.08 PCPD would require considerable increase in manpower and expertise to implement the proposals if they are pursued, such as enhanced protection of sensitive personal data, regulation of data

processors, criminalizing unauthorized obtaining, disclosure and sale of personal data, and wider discretion for the PCPD to issue enforcement notice.

1.09 The key proposals are dealt with in Chapter Three (Sensitive Personal Data), Chapter Four (Data Security), Chapter Five (Enforcement Powers of the PCPD), and Chapter Six (Offences and Sanctions). Comments are also invited on other proposals at Annex 1 which have considerable impact on the community. Those proposals which the Administration has considered but is inclined not to pursue are set out in Annex 2. At Annex 3 are miscellaneous proposals which include mainly operational and procedural amendments to streamline the operation of the PDPO and address technical and operational problems encountered in the implementation of the PDPO.

1.10 We have an open mind on the various amendment proposals and we welcome views from the community in this regard. Following this round of public consultation, we will consolidate the views received. When we have general directions on the way forward, we will arrange for further public discussions on possible legislative proposals.

Chapter Two : An Overview of the Personal Data (Privacy) Ordinance

Major Provisions of the Personal Data (Privacy) Ordinance

2.01 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 Law Reform Commission ("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.

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

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

(a) DPP 1 (purpose and manner of collection of personal data) which provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user who is to use the data. Only personal data that are necessary for or directly related to the purpose should be collected, and that the data collected should be adequate but

not excessive for those purposes. In addition, it provides for the lawful and fair means of collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject;

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

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

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

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

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

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

2.05 The PDPO imposes conditions on the use of personal data in automated matching processes and conditions (which have not yet commenced operation) on transfer of personal data to places outside Hong Kong. The Ordinance also regulates the use of

personal data in direct marketing by data users.

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

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

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

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

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

2.07 Under the PDPO, contravention of a DPP by itself is not an offence. If, following the completion of an investigation, the PCPD is of the opinion that a data user is contravening a requirement (including a DPP) under the PDPO or has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated, the PCPD may, having regard to the damage or distress caused to the data subject, serve an enforcement notice on the data user, directing him to take such steps as are specified in the notice to remedy the contravention. If the data user fails to comply with the enforcement notice issued by the PCPD, he is liable to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily fine of $1,000.

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

under the PDPO.

2.09 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.

The Privacy Commissioner for Personal Data

2.10 The PDPO establishes the PCPD, an independent statutory authority, to promote compliance with and enforce the Ordinance. The Privacy Commissioner is empowered to approve and issue codes of practice, give guidance on, promote awareness of and supervise compliance with the Ordinance, inspect personal data systems and investigate suspected breaches of the Ordinance, examine any proposed legislation that may impact on the privacy of an individual's personal data, specify classes of data users required to submit annual returns on the kinds of personal data they hold and purposes for which the data are collected, held, processed or used, and compile a central register of such data users.

2.11 The major caseload statistics of the PCPD in the last three years are as follows:

Cases handled	2006	2007	2008
Enquiries	14 614	13 170	13 112
New applications for approval to carry out matching procedure	9	15	16
Complaints	1 208	1 074	946
Compliance checks	79	86	96
Enforcement notices issued	66*	14	7
Referrals for prosecution	8	9	5
Successful convictions	2	3	2

*Of these 66 enforcement notices issued, 46 notices related to the same data leakage case.

2.12 To promote public awareness of protection of personal data privacy, the PCPD organizes thematic seminars or workshops for a wide spectrum of data users from different sectors and seminars on “Introduction to the PDPO” for the general public. Since 2007, the PCPD has been organizing the “Privacy Awareness Week” as a regional initiative to promote awareness of the importance of protecting personal data privacy. Guidance and booklets are published from time to time to assist compliance with the statutory requirements of the PDPO by specific industry sectors including property management, IT practitioners, estate agents and mobile service operators.

Chapter Three : Sensitive Personal Data

Proposal No. 1 : Sensitive Personal Data

Issue to be addressed

3.01 The PDPO regulates any data relating directly or indirectly to a living individual, from which it is practicable to ascertain the identity of the individual and which are in a form in which access to or processing of is practicable. Advances in information technology have brought challenges to the existing regulatory regime of personal data privacy. With the increasing prevalence of storage, transmission and processing of personal data in electronic form, the harm and damage caused by data leakage is far more pervasive. This is particularly the case if the data involved are sensitive. At present, the PDPO does not differentiate personal data that are "sensitive" from those that are not. We need to consider whether the processing of sensitive personal data should be subject to more stringent data protection requirements to better protect the personal data privacy of individuals.

Considerations

3.02 More stringent regulation of sensitive personal data is in line with international practices and standards. The European Union 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 ("EU Directive"), which regulates the processing of personal data within the European Union, contains provisions to subject the processing of sensitive personal data to extra restrictions. The legislation of some overseas jurisdictions, such as the Data Protection Act 1998 of the United Kingdom ("UK Data Protection Act") and the Privacy Act 1988 of Australia ("Australian Privacy Act"), contains specific provisions regulating the handling of sensitive personal data.

3.03 Personal data commonly regarded as sensitive by overseas jurisdictions include racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade union, health condition, and sexual life. In addition to these types of data, the UK and Australia also classify criminal record as sensitive personal data, while Australia also regards genetic

information as sensitive personal data. However, a universally agreed set of sensitive data is not available. This is understandable as perception of sensitive personal data is culture-bound. That said, the following standards are generally adopted in deciding whether certain kinds of personal data are sensitive :

(a) intimate data about an individual, for instance, physical attributes, health or personal beliefs; and

(b) data likely to be utilized in discriminatory decisions.

3.04 The personal data privacy legislation of overseas jurisdictions which contains provisions that regulate sensitive personal data generally prescribes preconditions to be met for the processing of such data, including :

(a) where the data subject has given explicit consent;

(b) where the collection is required by law; or

(c) where the collection is necessary to prevent or lessen a threat to the life or health of an individual.

3.05 From the perspective of data protection, a higher degree of protection should be afforded to sensitive personal data given the gravity of harm that may be inflicted upon the data subject in the event of data leakage or accidental disclosure to third parties. Limiting the handling of sensitive personal data to specified circumstances would narrow down the scope of collection and use of such data, thus providing better safeguard against indiscriminate use and inappropriate handling.

3.06 As technology advances, biometric systems, which capture unique behavioral or physiological attributes of individuals, are increasingly being used for identification and authentication. Biometric systems enable extensive monitoring of the activities of individuals, as well as identification of individuals without their knowledge or consent. Biometric information could reveal sensitive personal information such as health, genetic information or ethnic origin. Any security failure in biometric systems could result in sensitive personal information of individuals being compromised. Furthermore, by virtue of the unchangeable

nature of biometric information, a biometric identifier cannot be cancelled or reissued and the harm caused to an individual is substantial in any biometric system security failure. The increasing use of such biometric systems for commercial and human resource management purposes raises privacy concerns.

Possible Regulatory Model

3.07 We have an open mind on whether to subject sensitive personal data to more stringent data protection. 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. To facilitate the discussion, we have drawn up a possible regulatory model.

Coverage of sensitive personal data

3.08 As explained in paragraph 3.03 above, there is no universally agreed set of sensitive data and the perception of such data is culture-bound. We need to consider the coverage of sensitive personal data. In this regard, 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 have grave privacy concerns as explained in paragraph 3.06 above. One option is to consider classifying biometric data as sensitive personal data.

Requirements in handling sensitive personal data

3.09 The collection, holding, processing and use ("handling") of sensitive personal data would be prohibited except in 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.

3.10 In addition to the additional requirements on the handling of sensitive personal data as set out in paragraph 3.09 above, data users who collect, hold, process or use sensitive personal data must also comply with the DPPs. The exemption provisions under Part VIII of the PDPO would apply to the proposed category of sensitive personal data.

Sanction for contravention of requirements

3.11 At present, failure to comply with any requirement under the PDPO (other than a contravention of a DPP) for which no penalty is specified in Section 64 (offences) is subject to a fine at Level 3 (up to $10,000). We need to consider whether contravention of the prescribed requirements governing the handling of sensitive personal data by a data user as set out in paragraph 3.09 should attract a higher level of fine.

3.12 At present, breach of a DPP is not an offence in itself. The PCPD is empowered to direct the data user concerned to remedy the breach by issuing an enforcement notice. Contravention of an enforcement notice is an offence and on conviction the offender is liable to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000. DPPs are couched in generic terms and can be subject to a wide range of interpretations. We may consider making non-compliance with

DPPs with regard to handling of sensitive personal data an offence. However, this will have a significant impact on civil liberty if a data user could face criminal liability for an inadvertent act or omission. Alternatively, we can consider whether we should simply extend the existing regulatory regime governing contravention of DPPs involving personal data to sensitive personal data also.

Need for grandfathering or transitional arrangement

3.13 If new requirements are imposed on sensitive personal data, application of the new requirement to data already collected will likely pose serious practical difficulties to data users as they would need to seek retrospective consent from data subjects for the collection and holding of the data unless the handling of the data could meet any of the other prescribed requirements set out in (b) to (g) of paragraph 3.09 above. It may be advisable to apply the new requirements only to sensitive personal data collected after the relevant legislative provision comes into force ("grandfathering"). In other words, a data user who has collected any sensitive personal data before the relevant legislative provision commences operation may continue to hold, process and use the data already collected without the risk of being held liable for contravening the additional requirements of the PDPO in relation to sensitive personal data.

3.14 Alternatively, we may specify a transitional period following the enactment of the new provision during which the processing of sensitive personal data will be exempted from the additional requirements. After the transitional period, data users have to meet the new requirements in processing the sensitive personal data.

<u>Invitation of Comments</u>

3.15 Comments are invited on :

(a) whether there is 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

(b) if yes, whether the possible regulatory regime, including

coverage of sensitive personal data, related regulatory measures, sanctions and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14 above, is appropriate.

Chapter Four : Data Security

(A) Introduction

4.01 Handling of personal data in electronic form increases the privacy risks to which such data are exposed as any loss, accidental or unauthorized alteration, access, disclosure or processing can occur speedily and result in significant and far-reaching damage to the affected data subjects. This is particularly the case when sensitive personal data in electronic form are transmitted to an outsourced agent or contractor for handling. Data security measures would need to be stepped up, particularly where outsourcing is involved, as a preventive measure. On the remedial front, measures would need to be mapped out to contain the damage to individuals affected by data leakage incidents.

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

Issue to be addressed

4.02 To address public concern that security breach by data processors may result in the leakage of vast amount of personal data on the Internet, we need to consider means to strengthen various security measures governing personal data entrusted to an agent for processing. At present, the PDPO does not directly regulate the activities of an agent which processes personal data ("data processor") for its principal ("data user"). Under Section 2(12) of the PDPO, a person 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. The protection afforded to the data subjects under the current law is for the data user who engages the agent to process the personal data to be held liable for any acts done by its agent with its authority (whether express or implied, whether precedent or subsequent) by virtue of Section 65(2) of the PDPO.

4.03 The trend of sub-contracting and entrusting personal data processing work to third parties has been on the rise. There is increasing concern about the need for a data user to assume a more proactive role in monitoring the performance of the data

processor with regard to data security, as well as the adequacy of security safeguards currently imposed on data processors to protect security of personal data transferred to them for handling.

Considerations

4.04 It is common international practice to impose specific duties and obligations upon a data user to ensure security of personal data entrusted to a data processor. Examples include :

(a) the European Union Directive on the protection of personal data requires the data controller to choose a processor who provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing of data, and to ensure compliance with those measures. A duty of confidentiality with regard to processing is also imposed on the data processor. However, the EU Directive is not directly binding on data processors and Member States do not have to impose the duty directly as a matter of public law;

(b) the UK Data Protection Act imposes upon the data controller the duty to implement appropriate technical and organizational measures to protect the personal data entrusted to the processor, including choosing a data processor who can provide sufficient guarantees in respect of the technical and organizational security measures governing the processing of the data. The data controller is also required to take reasonable steps to ensure compliance with the security measures by the data processor;

(c) Canada imposes obligations upon an organisation to make use of contractual or other means to ensure that their sub-contractors and agents will comply with the Personal Information Protection and Electronic Documents Act which governs the private sector;

(d) the Privacy Act of New Zealand requires an agency to ensure everything reasonably within its power is done to prevent unauthorized use or disclosure of the information given to someone in connection with the provision of a service to the agency; and

(e) the Australian Privacy Act imposes a duty upon a record keeper, who entrusts privacy information records to a service provider, to do everything that is reasonable within its power to prevent unauthorized use or disclosure of personal information contained in the records so entrusted.

4.05 Both Canada and Australia do not distinguish between data users and data processors. Organizations, whether they are data users or data processors, are required to comply with the relevant information/privacy principles, including principles similar to DPP 2 (2) (retention), 3 (use) and 4 (security) under the PDPO.

4.06 Imposing specific obligations on data users and data processors with regard to the processing of outsourced personal data would have significant implications for organizations in general and the information technology sector in particular. In mapping out the way forward, we would need to take the following into consideration :

(a) the need to look after the interests and address concerns of relevant stakeholders (including the community and the specific industry sector);

(b) the need to strike an appropriate balance between protection of personal data privacy and normal business operation;

(c) any regulatory scope should be wide enough to provide an adequate protection net, but without catching unintended parties;

(d) the need to ensure the free flow of information on the Internet;

(e) the impact on Hong Kong's attractiveness as a location for Internet-related businesses and next generation data centres;

(f) the proposed measures should be enforceable and reasonably practicable for compliance by different businesses; and

(g) the prevailing international regulatory standards and practices.

Possible Regulatory Model

4.07 The objective of any regulatory model should be to ensure that a data subject's personal data privacy is protected under the law, whether his personal data are handled by a data user directly, or by a data processor acting on behalf of a data user. Regulatory options to achieve this objective might include placing specific obligations on data users who engage data processors, directly regulating data processors themselves, or a combination of the two.

4.08 To facilitate the discussion, we have worked out possible regulatory options to strengthen the protection of personal data handled by a party other than the data user. In this connection, "data processor" would mean any party, other than an employee, who holds, processes or uses personal data solely on behalf of a data user, and does not hold, process or use those data for any of his own purposes. Examples of data processors include traditional providers of IT outsourcing, application outsourcing and business process outsourcing, companies engaged in Internet activities (such as Internet service providers ("ISPs"), website hosting companies, operators of social networking sites and providers of "software as a service"), service providers engaged by contract to provide computer personal data inputting services and contractors engaged to shred confidential documents which contain personal data. The options include specifying an explicit obligation on the data user who entrusts the data to a data processor, and imposing additional obligations on the data processor who is entrusted with the outsourced personal data. They are outlined in paragraphs 4.09 to 4.20 below.

Obligations on Data Users

4.09 We may expressly require a data user who transfers personal data to a data processor for holding, processing or use to use contractual or other means to ensure that his data processor and any sub-contractors will take all practicable steps to ensure the security and safekeeping of the data, to ensure that the data are not misused and are deleted when no longer required. The requirement is to be applied to contractors and their sub-contractors, whether within Hong Kong or offshore. This imposes upon the data user an explicit duty to ensure his sub-contractor behaves for the purpose of compliance with the

data user's own obligations under the PDPO.

4.10 The objective of imposing specific obligations on a data user is to ensure that the data user will discharge his duty to protect personal data when it entrusts such data to a data processor. Such specific obligations as detailed in paragraph 4.09 above on a data user would be incorporated into the relevant DPPs or otherwise by requiring the data user to use contractual or other means to ensure that the data processor delivers these obligations of the data user. Contravention of the requirement would render the data user liable to enforcement action by the PCPD, including the serving of an enforcement notice.

Obligations on Data Processors

4.11 Given that the definition of "data processor" would cover business operators of different nature and scale, in examining the application of the requirements to data processors, we need to give due regard to the practical issues in relation to compliance. Options available range from direct regulation to indirect regulation. These are discussed in paragraphs 4.12 to 4.20 below.

4.12 For the considerations explained below, it may not be adequate to only rely on the data user to ensure personal data privacy protection by data processor:

(a) since it is commonplace that personal data are entrusted with data processors for processing, keeping and transfer, data subjects may have an expectation that their personal data should have the same protection as they are held by data users, and data processors should be subject to specific regulation in the law; and

(b) 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(s) the data processing activities in whole or in part to other agents for processing. Without direct regulation on data processors under the law, 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 the data user has no direct contractual relations. Data users may

argue that this would pose an onerous burden on them.

4.13 However, there are difficulties in defining generic obligations for data processors. The PDPO relies on concepts such as the "purpose for which data were to be used at the time of collection". Many Internet-related businesses will be unaware of the nature of the data, including the purpose for which it was originally collected. Moreover, some Internet-related businesses process the same data on behalf of several users – a social networking site, for instance, processes personal data on behalf of both the user who posts the data and on behalf of those who search for the data, who are alerted to the posting of the data and who read the data. This may make it difficult to specify detailed obligations in generally applicable legislation without a risk of causing unintended consequences for current or future Internet-related businesses. There is also a risk that placing wide-ranging obligations on data processors could interfere with the free flow of information on the Internet, if businesses set up to facilitate the free flow of information were given obligations that they could not fulfill without assessing whether the information they were storing, indexing, transmitting, serving, etc. was personal data and whether such information was being used for a purpose entrusted by the data user.

Direct Regulation

4.14 If it were considered necessary to directly regulate the activities of a data processor entrusted by a data user with personal data under the PDPO, one option would be to require the data processor to :

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

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

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

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

4.15 There are concerns that the additional requirements may pose problems of compliance for the Internet-related businesses, such as ISPs and providers of web-based services. Such data processors typically have no knowledge of whether the data they are holding are personal data. Compliance with the requirements may frustrate free flow of information on the Internet, to the detriment of the flourishing Internet-related businesses. It is, therefore, necessary to work out arrangements to ensure that the requirements are practicable and workable for Internet-related businesses.

4.16 Requirement (a) of paragraph 4.14 is fundamental in the protection of personal data privacy. It serves to confine the use of personal data entrusted to a data processor to limited purposes. However, it may not be straightforward for a data processor to determine what the permitted purposes are when the data processor is an Internet-related business that processes the same data for different purposes on behalf of multiple users. For instance, an advertising-funded webmail provider might transmit personal data on behalf of the sender, store, forward and index personal data on behalf of the recipient and process the data on behalf of third parties for the purpose of targeting marketing messages. There may be uncertainty about whether any of these is a purpose for which the data were entrusted to the provider by the sender or by his email service provider.

4.17 Requirement (b) in paragraph 4.14 is a basic security requirement for handling personal data. The proposed requirement does not impose an absolute duty on data processors. Data processors are not required to provide an absolute guarantee of data security. Where all reasonably practicable steps have been taken to protect personal data against security risks, data processors would not be caught for breach of the requirement. This requirement should not impose extra burden on the Internet-related businesses, as they should have already adopted appropriate measures to safeguard data security of their system and network. However, the business purpose of many Internet-related businesses is to facilitate access to data. Such data processors may be left uncertain as to what constitutes unauthorized access to personal

data. For instance, a search engine that caches data might fall foul of this obligation if it indexes and caches personal data and then provides the data to users, despite the fact that it may have no knowledge that the data in question are personal data.

4.18 The purpose of imposing requirement (c) in paragraph 4.14 on a data processor is to prevent retention of data it processes indefinitely, thereby increasing security risk. We appreciate that Internet-related businesses would have concern as to how they could comply with the requirement on timely erasure of personal data in their custody given that they have no knowledge of whether the data they are processing contain personal data. It is for consideration whether different obligations should apply to different categories of data processors, having regard to the operational constraints unique to specific industry sectors.

4.19 However carefully drafted the law is to address specific issues for specific types of Internet-related business, the Internet environment is fast-evolving and it is important that privacy laws do not inhibit the development of desirable new Internet-related services. In practice, many Internet-related businesses achieve the necessary flexibility by adopting a privacy policy that is appropriate to their business and which is acceptable to their customers. This risk of inhibiting new Internet-related businesses might therefore be ameliorated by making 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 4.14 should be construed as a requirement to honour the relevant terms of such privacy policy. Failure to comply with its own privacy policy in respect of such requirements would render a data processor liable to the enforcement actions of the PCPD, including the serving of an enforcement notice. This would enable data processors to adopt a privacy policy appropriate to their business and would give them certainty that their statutory obligations aligned with their privacy policies. Many data subjects and Internet-related businesses are familiar with the self-regulatory mechanism of the privacy policy, a mechanism that has proved workable in practice. The risk that privacy policies will be too liberal might be mitigated because a data user would be in breach of his own obligations under the PDPO if he chose a data processor whose privacy policy was too lax.

Indirect Regulation

4.20 We may also consider the option of indirect regulation in the event that it is not practicable to apply the requirements in paragraphs 4.14 to 4.19 above to data processors. We may, as a first step, rely on the data user to ensure that its data processors provide security protection to personal data at a level comparable to itself without imposing explicit obligations under the PDPO on the data processor. This approach, if adopted, would mean that the PCPD cannot directly intervene 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 under the data processor. However, the data user would still have redress under contractual law, and the data subject would have redress against the data user. Together these enforcement mechanisms should provide a reasonable degree of protection for personal data handled by data processors.

Invitation of Comments

4.21 Comments are invited on the possible regulatory model as set out in paragraphs 4.07 to 4.20 above :

(a) whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;

(b) whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means; and

(c) if activities of data processors were to be directly regulated under the PDPO, 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.

(C) Proposal No. 3 : Personal Data Security Breach Notification

Issue to be addressed

4.22 The spate of personal data leakage incidents has aroused concern within the community. At present, there is no requirement under the PDPO for a data user to notify the PCPD or individuals affected by a data leakage incident. We need to consider whether a personal data security breach notification ("privacy breach notification") system should be instituted to require organizations 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.

Considerations

4.23 With advances in technology, many organizations are storing vast amount of identifying personal information electronically, thereby posing privacy risks in the event of data leakage. The consequences of personal data leakage is further exacerbated with the prevalence of the Internet as the leaked data can be downloaded and retained by countless unauthorized users, and further disseminated by reckless unauthorized users soon after the leakage.

4.24 The objective of privacy breach notification is to provide individuals who may be affected adversely by a breach with an early warning so that they can take steps to protect themselves against the consequences of such breach, thereby minimizing their exposure to possible damages or the risks of identity theft or fraud. Such a notification is particularly important when a significant number of data subjects are affected by a breach which involves loss or leakage of sensitive personal data.

4.25 On the other hand, notifying the PCPD ensures that a record is kept of all personal data privacy breaches, allows for oversight of organization practices, and offers the potential for organizations to obtain guidance from the PCPD regarding notification obligations and methods.

4.26 A requirement to notify all affected parties of each and every personal data leakage incident is costly to organizations. Moreover, individuals receiving too many breach notices may

have difficulty to assess which ones carry a real risk of harm and which ones are minor in nature and consequence. Or they may become desensitized to the notices and ignore some of the notices. Indeed, the Australian Law Reform Commission warned of the risk of "notification fatigue" arising from over-notification. Bearing in mind that some breaches may not pose a real threat in causing serious harm or damage to the individuals, a selective approach in notification is a rational course and is in line with the international norm.

4.27 In November 2008, the Government introduced a notification mechanism for electronic personal data leakage incidents whereby bureaux and departments are required to report such incidents to the PCPD as soon as possible and notify affected individuals as far as practicable. Exemption from reporting has to be justified and approved by the head of bureau or department.

4.28 In respect of the banking sector, the Hong Kong Monetary Authority requires that in the event of any incidents that may have an impact on the protection of the personal data of customers, banks should notify affected customers as soon as practicable after ascertaining the extent of impacts on the customers' data, the level of risk of information leakage and the number of affected customers. Banks should also clearly explain the impacts of the incidents on customers, the follow-up actions implemented by banks concerning the incidents and the steps that ought to be taken by customers.

4.29 Privacy breach notification is a new development in personal data privacy laws. The US is in the forefront in legislating on such requirement. Over 30 states have incorporated in their state laws a duty to notify individuals of certain defined security breaches of personal information, namely unencrypted personal information involving a person's name in combination with certain sensitive personal information such as social security number, credit card number and driver's licence number.

4.30 The European Parliament has in May 2009 adopted a legislative resolution to amend Directive 2002/58 EC on privacy and electronic communications to require the provider of publicly available electronic communications services to notify, without undue delay, a personal data breach to the competent national authority, and affected subscribers or individuals when the breach

is likely to adversely affect the personal data and privacy of the individuals. The notification to affected parties shall describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the national authority shall, in addition, describe the consequence of, and the measures proposed or taken by the provider to address the personal data breach. The national authorities within the European Union may adopt guidelines and issue instructions concerning the circumstances that trigger notification, the format and the manner of notification. Although the legislative requirement on mandatory notification is only limited to the electronic communications sector, the European Commission undertook to consult stakeholders and present proposals about extending mandatory notification to all sectors by 2011.

4.31 The UK, New Zealand, Australia and Canada do not have provisions regarding privacy breach notification in their personal data privacy laws. They have, however, promulgated voluntary guidelines for organizations to follow in the event of personal data breach.

4.32 The Australian Law Reform Commission has, in its report on Australian Privacy Law and Practice published in May 2008, recommended to include data breach notification in the Australian privacy law by requiring an organization to notify the Privacy Commissioner and affected individuals of confirmed or reasonably suspected breach of data security of specified personal information where the unauthorized acquisition may give rise to a real risk of serious harm to any affected individual. The UK Information Commissioner has also proposed to include in the law a requirement to notify the Information Commissioner's Office, and the individuals affected, where data security breach presents a real risk causing substantial damage or distress to individuals.

4.33 The following considerations support the introduction of some form of privacy breach notification in Hong Kong :

(a) there is a need to mitigate the potential damage to individuals affected by personal data leakage;

(b) data users, especially those that hold vast amount of sensitive personal data, have the obligation to ensure proper security measures are in place to protect the personal data in their custody; and

(c) frequent incidents of electronic data losses were reported locally and internationally, particularly in association with the widespread use of portable electronic devices.

Such notification requirement may either be mandatory or in the form of voluntary guidelines. Any reporting requirement has to be proportionate to the potential harm caused by the breach, and the cost to the community arising from over-notification should be taken into account.

4.34 The impact of mandatory privacy breach notification on businesses cannot be underestimated. Bearing in mind that a number of overseas jurisdictions adopt voluntary guidelines on privacy breach notifications, we consider it more prudent to start with a voluntary breach notification system so that we can assess the impact of breach notifications more precisely, and fine-tune the notification requirements to make them reasonable and practicable, without causing onerous burden on the community. For this purpose, the PCPD can issue guidelines on voluntary privacy breach notifications.

4.35 As explained in paragraph 4.27 above, the Government has already instituted a notification mechanism to require bureaux and departments to notify the PCPD and affected individuals in the event of electronic personal data leakage. It is important that, if a voluntary notification mechanism is to be introduced, it should cover both the Government, public bodies and all private organizations in order to achieve the purpose of mitigating the potential damage to individuals affected by personal data leakage.

<u>Possible Notification Mechanism</u>

4.36 To facilitate the discussion, we have outlined in paragraphs 4.37 to 4.42 below a possible option on notification mechanism.

4.37 A data user will need to take immediate steps to limit the data security breach and assess the risks associated with the breach. Generally, the more sensitive the personal data involved, the

higher the risk of harm or damage will cause to the affected individuals. The data user will be required to notify the PCPD when a personal data security breach may result in a high risk of significant harm to individuals or organizations. Notice of data security breach will have to be made to the PCPD within five business days of discovery of the breach. The PCPD will issue guidelines on circumstances that would trigger the notification.

4.38 The data user involved in a personal data leakage will decide whether notifications should also be sent to individuals affected by the breach based on an assessment of the level of risk of harm on a case-by-case basis. In this regard, the data user concerned will need to assess the risks involved and make a prompt determination regarding whether, when and how to proceed to notify the individuals concerned, law enforcement agencies, business partners and/or the general public.

4.39 The notice may include the following information :

(a) a general description of what occurred;

(b) the date and time of the breach;

(c) the date and time the breach was discovered;

(d) the source of the breach (either the organization itself or the third party that maintained personal data on its behalf);

(e) a list of the type of personal data involved;

(f) an assessment of the risk of identity fraud as a result of the breach;

(g) a description of the measures taken or that will be taken to prevent further unauthorized access to the personal data;

(h) contact information for affected individuals to obtain more information and assistance; and

(i) information and advice on what individuals can do to protect themselves against identity theft or fraud.

4.40 As for timing of the notice, the notification will be made as soon

as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has, for investigative purpose, made a written request for a delay.

4.41 The notification to affected individuals will generally be sent by regular mail, but electronic notice will be permitted if the individual concerned has consented explicitly receiving important notices by email. Substitute method of notice, such as posting notice in newspapers, may be allowed where large number of individuals have to be notified or where the total cost of individual notification is extraordinary.

4.42 In the event that a mandatory privacy breach notification is adopted in the longer term, the PCPD will be empowered to order an organization to issue notifications to the affected data subjects. If so, failure to notify individuals and organizations affected by the breach as required by law, as well as failure to comply with the order of the PCPD will be subject to a monetary penalty.

Invitation of Comments

4.43 Comments are invited on :

(a) the need to institute a voluntary privacy breach notification system in Hong Kong;

(b) the components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42 above, including -

(i) the circumstances under which notification should be triggered;

(ii) to whom the notice of breach should be sent;

(iii) timing of the notice;

(iv) by what means should the notice be sent;

(v) the content to be covered in the notice; and

(vi) the consequences of failing to give notification.

Chapter Five : Enforcement Powers of the Privacy Commissioner for Personal Data

(A) Introduction

5.01 To better safeguard personal data privacy rights and to enhance the efficacy of regulation under the PDPO, the PCPD has proposed that the PCPD be given more power to enforce the PDPO. At present, the PCPD is empowered under the PDPO to investigate suspected breaches of the PDPO's requirements and issue enforcement notices to data users as appropriate, as well as inspect personal data systems and make recommendations on compliance with the provisions of the PDPO. In this chapter, we will examine whether it is appropriate to provide additional enforcement powers to the PCPD.

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

Issue to be addressed

5.02 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 such persons to furnish any information to the Privacy Commissioner. However, the PCPD cannot conduct search for or seize evidence, carry out criminal investigation or initiate prosecution on his own. Criminal investigations are conducted by the Police and prosecutions, where necessary, are initiated by the Department of Justice.

5.03 The PCPD has proposed that the Privacy Commissioner be given the power to investigate and prosecute offences, as well as incidental powers to search and seize evidence, etc., for more effective enforcement of the PDPO 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 confidence; and

(c) to save time on referring cases to the Police, hence, to help meet the statutory time limit to lay prosecution which is set at six months from commission of an offence.

Considerations

5.04 Under the Basic Law, the control of criminal prosecutions is vested with the Department of Justice. The existing prosecution arrangement in relation to the PDPO is in line with the Basic Law. Although 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, our policy assessment is that strong justifications are required for the prerogative of initiating criminal prosecution to be delegated in specific domains.

5.05 A number of statutory bodies are empowered to institute prosecution on its own. For instance, the Vocational Training Council, the Employees Compensation Assistance Fund Board, the Construction Workers Registration Authority and the Security and Futures Commission are provided with direct prosecution power in relation to summary offences. On the other hand, the Equal Opportunities Commission ("EOC"), an independent statutory body established under the Sex Discrimination Ordinance to implement anti-discrimination ordinances, is not provided with direct prosecution power.

5.06 Some of the new offences proposed in Chapter Six of this document are not technical in nature, and may involve a fine and imprisonment. These include contravening the prescribed requirements governing the handling of sensitive personal data, knowingly or recklessly obtaining personal data without consent of a data user and disclosing the personal data so obtained for profits or malicious purposes, etc. There could be community concerns, if the power to prosecute these offences were delegated to the PCPD.

5.07 The PCPD referred eight cases to the Police for prosecution in 2006. The referral figure was nine for 2007 and five for 2008.

The existing arrangement has been working smoothly. There is no strong case for change. To address the problem relating to the tight statutory time limit for initiating prosecution, we plan 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 (please refer to Proposal No. 40 in Annex 3).

5.08 Furthermore, whether the PDPO can afford effective protection to personal data privacy hinges on the adequacy of penalty sanction, rather than on who the party responsible for initiating prosecution is. In this regard we have put forth in Chapter Six proposals to step up the sanctions provided for in the PDPO.

Invitation of Comments

5.09 On balance, we do not see a strong case to give the PCPD the power to investigate into and prosecute criminal offence cases. Comments are invited 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.

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

Issue to be addressed

5.10 At present, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled under Section 66 of the Ordinance to compensation from the data user for that damage. The PDPO, however, does not empower the PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings under Section 66. These individuals would have to bear all the legal costs themselves unless they are qualified for and have successfully obtained legal aid.

Considerations

5.11 The EOC is empowered under the anti-discrimination ordinances (namely, the Sex Discrimination Ordinance (Cap. 480), the Disability Discrimination Ordinance (Cap. 487), the Family Status Discrimination Ordinance (Cap. 527)) and the Race

Discrimination Ordinance (Cap. 602) 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.

5.12 To ensure good use of public funds, the relevant legislation empowers the EOC to accede to a request for legal assistance if :

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

(b) it is unreasonable to expect the applicant for legal assistance 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.

5.13 We note that although the PDPO provides for recourse to civil remedy in case of intrusion into personal data privacy, this has seldom been invoked. If the PCPD is empowered to offer legal assistance to an aggrieved data subject who suffers damage to seek redress under the PDPO, the aggrieved party will be in a better position to assess the chance of success of his civil claim and will not be inhibited to file a lawsuit due to cost considerations. This proposal, if pursued, could achieve greater deterrent effect on acts or practices which intrude into personal data privacy, and enhance the overall effectiveness of sanctions provided for under the PDPO.

Invitation of Comments

5.14 We invite comments on 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 EOC model.

(D) Proposal No. 6 : Award Compensation to Aggrieved Data Subjects

Issue to be addressed

5.15 A data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user in relation to his personal data is entitled to compensation from the data user for that damage under Section 66 of the PDPO. Over the years, this provision was seldom invoked probably because court proceedings could be lengthy and costly and the outcome of a civil claim is unpredictable. We have considered the option of empowering the Privacy Commissioner to determine the amount of compensation, so as to provide a quick and effective redress to the aggrieved party through mediation.

Considerations

5.16 The option could provide the aggrieved party with an alternative to redress as against the institution of court action which is generally lengthy and costly. It may also lessen the burden of the courts in dealing with civil claims invoked under the PDPO.

5.17 The Australian Privacy Act empowers its Privacy Commissioner to determine after investigation a specified amount by way of compensation to a complainant for the loss and damage suffered (including injury to feelings and humiliation suffered) by reason of the act or practice complained against. The Commissioner may also determine such amount to be reimbursed to the complainant for expenses reasonably incurred in connection with the making of the complaint and the investigation. It should, however, be noted that Australia adopts a conciliatory approach in handling privacy complaints. A complainant may demand an apology, an explanation or financial compensation. The Privacy Commissioner will serve as a conciliator between the complainant and the complainee.

5.18 The appropriate body to determine compensation under the PDPO was thoroughly discussed in the LRC Report on Reform of the Law Relating to the Protection of Personal Data issued in August 1994. The LRC opined that conferring power on a data protection authority to award compensation would vest in a single

authority an undesirable combination of enforcement and punitive functions. The LRC recommended that the PCPD's role should be limited to determining whether there has been a breach of the principles. It would be for a court to determine the appropriate amount of compensation payable. Section 66 of the PDPO was enacted against such considerations.

5.19 A few statutory bodies in Hong Kong (such as The Medical Council of Hong Kong, The Nursing Council of Hong Kong and The Hong Kong Planners Registration Board) are conferred with a narrow power to award a person summoned to attend inquiries certain sum expended by that person by reason of such attendance. However, none of these statutory bodies are empowered to determine compensation to complainants for loss and damages. The EOC is not provided with power to award compensation.

5.20 Australia advocates settlement of complaints by conciliation which is in stark contrast to the Hong Kong regulatory regime. The power to determine the amount of compensation for any loss or damage suffered is part and parcel of the Australian Privacy Commissioner's power of investigation. It may not be appropriate to simply adopt this part of the Australian model in the regulatory regime of Hong Kong.

5.21 Furthermore, Section 66 of the PDPO already provides an aggrieved data subject with an avenue to seek compensation through the Court. We have put forth Proposal No. 5 to empower the PCPD to provide legal assistance to an aggrieved party in seeking redress through civil remedy as a measure to assist aggrieved data subjects.

Invitation of Comments

5.22 Comments are invited on whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Chapter Six : Offences and Sanctions

(A) Introduction

6.01 The series of recent personal data leakage incidents have raised the question of whether the existing sanctions provided for under the PDPO are adequate to achieve deterrent effect. Questions were raised on whether contravention of a DPP should be made an offence, whether repeated contravening act or practice for which an enforcement notice was previously issued should constitute an offence, whether particular acts of contravention of the requirements of the PDPO should be made an offence and the need to impose heavier penalties for existing offences. We will examine in this chapter various options to step up sanctions under the PDPO.

6.02 The current provisions of the PDPO are in line with international jurisprudence governing personal data privacy legislation. As proposals on criminalization would affect the community at large, and in particular data users and members of the public, there is a need to strike carefully a balance between protection of personal data privacy and other competing rights and interests such as the civil liberty of individuals and freedom of information. In the process, we have due regard to the following :

(a) the severity of the contravening act or the act to be regulated, including the seriousness of intrusion into personal data privacy, harm or damage caused to the affected data subjects and the culpability of the act;

(b) the relative importance of the rights to be protected under the PDPO;

(c) the existing penalty levels provided for in the PDPO;

(d) since imposing criminal sanctions would have significant impact on the civil liberties of individuals, any proposed new offence should be so circumscribed such that its scope would not be unduly wide as to catch unintended activities; and

(e) the enforceability of any proposed new offence.

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

Issue to be addressed

6.03 At present, 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. It is only when the data user contravenes the enforcement notice will he commit an offence under Section 64(7), and be liable on conviction to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

Considerations

6.04 DPPs are couched in generic terms and can be subject to a wide range of interpretations. To make contravention of a DPP an offence would have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability. Moreover, this would be moving away from the original intent of adopting the DPPs in the PDPO. It would be more appropriate to adopt a selective approach by singling out particular acts or practices as offence having regard to the severity of such contravening acts or practices.

Invitation of Comments

6.05 Comments are invited on whether we should make contravention of a DPP an offence.

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

Issue to be addressed

6.06 Incidents of blatant dissemination of leaked personal data on the Internet have aroused widespread concern in the community regarding the possible misuse of leaked personal data, such as fraud or identity theft. Unauthorised use of personal data may also intrude into personal data privacy and may cause damage to data subjects. This may include :

(a) unauthorised access and collection of customers' personal data by staff of a company for sale to third parties such as direct marketing companies, debt collection agents, etc. for profits; and

(b) unauthorised disclosure of a patient's sensitive health records by hospital staff to third parties.

At present, use of personal data is regulated by DPP 3, and contravention of any DPPs *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 cause to the data subjects as a result of the intentional or willful act of the person in flagrant disregard of the personal data privacy of others, we have to seriously consider whether such blatant acts should be subject to criminal sanction.

Considerations

6.07 Unlawful obtaining, disclosure or sale of personal data is an offence in the UK. Section 55 of the UK Data Protection Act makes it an offence for any person who :

(a) knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data or procures such disclosure, unless any of the defences in paragraph 6.08 are applicable; or

(b) sells or offers to sell the personal data so obtained.

6.08 The UK legislation also 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 authorized 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 of 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 purpose, 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.

6.09 We have considered the possibility of introducing a new offence modelled on Section 55 of the UK Data Protection Act. Such proposal seeks to protect data subjects whose personal data were leaked and to deter irresponsible acts of those who obtain or disclose such leaked data without consent of the data user, which seriously intrudes into the personal data privacy of the data subjects concerned. It is, however, not our intention to impose criminal liabilities on data users for accidental leakage of personal data not resulting in substantial harm.

6.10 There are concerns that the proposed offence may interfere with the normal and innocuous browsing activities of web-users. For instance, the act of downloading personal data that had been leaked on the Internet might be caught as "knowingly obtaining personal data". Given the advances in information technology and the inability of users to fully comprehend the risks involved in the use of computer software, personal data may be disseminated unintentionally through the use of a computer software and such act could be caught as "reckless disclosure" under the proposed offence.

6.11 While there is a need to curb blatant privacy intrusive acts, a more confined offence to catch such culpable acts could address the concerns about uncertainty of law. One possible option is to make it an offence if a person knowingly or recklessly obtained the personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes. 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 fine currently imposed under the PDPO is at Level 5 (i.e. up to $50,000).

Invitation of Comments

6.12 We invite comments on the following:

(a) whether we should 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; and

(b) if yes, the need for defence provisions and the appropriate level of penalty.

(D) Proposal No. 9 : Repeated Contravention of a Data Protection Principle on Same Facts

Issue to be addressed

6.13 At present, if a data user breaches a DPP, the PCPD is empowered under Section 50 of the PDPO 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 will commit an offence under Section 64(7), and be liable on conviction to a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, to a daily penalty of $1,000.

6.14 It is possible that a data user, may resume the same contravening act or practice shortly after compliance with an enforcement notice issued against him. Under the existing provisions, the enforcement action at the disposal of the PCPD will be to issue yet another enforcement notice.

Considerations

6.15 To forestall possible circumvention of the regulatory regime, we may consider making 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. However, this would

be moving away from the original intent of adopting the DPPs in the PDPO. Moreover, since the enactment of the PDPO, the PCPD has not come across any such case of circumvention as depicted in paragraph 6.14 above. There does not appear to be a strong need to make such an act an offence.

Invitation of Comments

6.16 Comments are invited on :

(a) whether it is appropriate 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; and

(b) if yes, the appropriate penalty level for the offence, bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.

(E) Proposal No. 10 : Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

Issue to be addressed

6.17 To strengthen the enforcement of the PDPO and to deter serious contravention of DPPs, we have considered empowering the PCPD to require data users to pay monetary penalty for serious contravention of DPPs.

Considerations

6.18 Under the amendment (which is not yet in operation) to the UK Data Protection Act, 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 Information Commissioner is required to issue guidance on how he proposes to exercise his power to impose monetary penalty, including the circumstances he considers appropriate to issue a monetary penalty notice. The regulatory regime also provides for an appeal mechanism.

6.19 In Hong Kong, it is not common for non-judicial bodies to have the statutory power to impose monetary penalties. One of the few examples is the power bestowed upon the Telecommunications Authority under the Unsolicited Electronic Messages Ordinance (Cap. 593) ("UEMO") to impose financial penalties on a telecommunications service provider that fails to comply with a direction issued by the Authority. Public officers may be authorized under various fixed penalty ordinances, such as the Fixed Penalty (Criminal Proceedings) Ordinance (Cap. 240), Fixed Penalty (Traffic Contraventions) Ordinance (Cap. 237), Fixed Penalty (Public Cleanliness Offences) Ordinance (Cap. 570), and Fixed Penalty (Smoking Offences) Ordinance (Cap. 600), to hand out fixed penalty notices to offenders.

6.20 Monetary penalty sanction fits in well with fixed penalty schemes and clearly defined offences as in the case of the UEMO. Under the PDPO, the DPPs are couched in generic terms and can be subject to a wide range of interpretations. Although the PCPD may issue guidance on the circumstances he considers appropriate to issue a monetary penalty notice, whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. Instead of empowering the Privacy Commissioner to require data users to pay monetary penalty, 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.

Invitation of Comments

6.21 Comments are invited on whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

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

Issue to be addressed

6.22 At present, 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 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000. The PDPO does not provide for heavier sanction for repeated offenders of Section 64(7). We have considered the option to subject a repeated offender to heavier penalty to achieve greater deterrent effect.

Considerations

6.23 Various pieces of local legislation also impose heavier penalty for repeated offenders. The magnitude of the penalty level for subsequent convictions varies.

6.24 Since the enactment of the PDPO, no data user has been prosecuted more than once for contravention of an enforcement notice. There has not been a serious problem with repeated offenders.

Invitation of Comments

6.25 We invite comments on the following :

(a) whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and

(b) if yes, the appropriate penalty level, bearing in mind the existing penalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in the case of a continuing offence, a daily fine of $1,000.

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

Issue to be addressed

6.26 Section 34 of the PDPO regulates the use of personal data in carrying out direct marketing activities by data users. Pursuant to Section 34(1)(ii) of the Ordinance, a data user shall not use any personal data for the purpose of carrying out direct marketing activities, if the individual who is the subject of the data has previously requested the data user to cease to so use his personal data. A data user who, without reasonable excuse, contravenes Section 34(1)(ii) commits an offence under Section 64(10) and is liable on conviction to a fine at Level 3 (up to $10,000).

6.27 Direct marketing activities are prevalent in Hong Kong. Direct marketing calls are often a cause of complaint and nuisance to the data subjects. The PCPD is of the view that the existing level of penalty may not be sufficient to act as an effective deterrent to contain the problem and recommends the penalty level be raised. There were also calls within the community to raise the penalty level to curb these annoying direct marketing calls. In a case brought before the court concerning the making of direct marketing calls by a telecommunications company, the Magistrate remarked that the maximum penalty of $10,000 under the PDPO can hardly act as an effective deterrent for large companies.

Considerations

6.28 The PCPD received 59 complaints about misuse of personal data (involving contravention of Section 34 or breach of DPP) in direct marketing activities in 2006, 87 in 2007 and 67 in 2008. There was one successful prosecution on direct marketing in 2006, three in 2007 and nil in 2008.

6.29 Direct marketing calls may be annoying and may intrude into the privacy of individuals. That said, direct marketing has its economic values with regard to provision of job opportunities and information on products and services available to consumers. An unduly heavy penalty for related offence may frustrate normal and legitimate marketing activities.

6.30 To curb misuse of personal data in direct marketing activities, we can consider raising the penalty level for contravention of Section 34 (1)(ii) of the PDPO. In deciding on the appropriate level of penalty for misuse of personal data in direct marketing, one relevant consideration is whether such calls would bring about serious damage to the personal data privacy of the data subject concerned.

Invitation of Comments

6.31 Comments are invited on :

(a) whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and

(b) if yes, the appropriate level of penalty.

Chapter Seven : Summary of Proposals for Comments

7.01 Comments are invited on the key proposals as summarised below :

Proposal No. 1 : Sensitive Personal Data

- Whether there is 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

- If yes, whether the possible regulatory regime, including coverage of sensitive personal data, related regulatory measures, sanctions, and the need for grandfathering or transitional arrangement as set out in paragraphs 3.08 to 3.14, is appropriate.

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

- Whether a data user should be required to use contractual or other measures to secure compliance with relevant PDPO obligations when contracting out the processing of personal data to third parties;

- Whether the activities of a data processor should be directly regulated under the PDPO or whether it is sufficient to indirectly regulate the data processor through the data user by contractual or other means; and

- If activities of data processors were to be directly regulated under the PDPO, 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.

Proposal No. 3 : Personal Data Security Breach Notification

- The need to institute a voluntary privacy breach notification system in Hong Kong.

- The components of a breach notification mechanism as set out in paragraphs 4.37 to 4.42, including :

  (i) the circumstances under which notification should be

triggered;

(ii) to whom the notice of breach should be sent;

(iii) timing of the notice;

(iv) by what means should the notice be sent;

(v) the content to be covered in the notice; and

(vi) the consequences of failing to give notification.

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

- Whether the PCPD should be conferred with the power to carry out criminal investigations and prosecutions or whether the status quo should be maintained.

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

- 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 EOC model.

Proposal No. 6 : Award Compensation to Aggrieved Data Subjects

- Whether it is appropriate to introduce at this stage an additional redress avenue by empowering the PCPD to award compensation to aggrieved data subjects.

Proposal No. 7 : Making Contravention of a DPP an offence

- Whether we should make contravention of a DPP an offence.

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

- Whether we should 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; and

- If yes, the need for defence provisions and the appropriate level of penalty.

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

- Whether it is appropriate 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; and

- If yes, the appropriate penalty level for the offence bearing in mind that non-compliance with an enforcement notice is subject to a fine of $50,000 and to imprisonment for two years.

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

- Whether it is appropriate to empower the PCPD to impose monetary penalty on serious contravention of DPPs.

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

- Whether heavier penalty should be imposed for a second or subsequent conviction of Section 64(7); and

- If yes, the appropriate penalty level, bearing in mind the existing penalty level for contravention of an enforcement notice which is a fine at Level 5 (up to $50,000) and imprisonment for two years, and in case of a continuing offence, a daily fine of $1,000.

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

- Whether the penalty for misuse of personal data in direct marketing (i.e. contravention of the requirement under Section 34(1)(ii)) should be raised; and

- If yes, the appropriate level of penalty.

7.02 We also welcome comments on the proposals set out at Annexes 1 to 3.

Annex 1

Other Proposals : Invitation for Comments

1. Apart from Proposals No.1 to 12 in Chapters Three to Six of the consultation document, we have also examined another 15 proposals covering the following areas :

   (a) the rights of data subjects under the PDPO;

   (b) the rights and obligations of data users under the PDPO;

   (c) enforcement powers of the PCPD; and

   (d) exemptions from the requirements of the PDPO.

   Comments are invited on these proposals which are set out in the following paragraphs.

(A) Rights of Data Subjects

Proposal No. 13 : Third Party to Give Prescribed Consent to Change of Use of Personal Data

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. Certain data subjects, such as minors or mentally incapacitated persons, may not possess the mental capacity to appreciate and understand the privacy impact relating to the change of use of their personal data by data users. This is particularly of concern when the handling of their personal data may have profound impact on the provision of essential services such as healthcare, education and social services.

3. Views are invited on whether we should safeguard the vital interest of vulnerable classes of data subjects by devising a system which empowers a specified third party (the definition of which will be set out in the amendment legislation) to give consent to the change of use of personal data of such data subjects when it is in their best interests to do so. The third party will be allowed to give prescribed consent on behalf of a data subject on condition that :

   (a) the data subject is incapable of giving prescribed consent as

he does not have a sufficient understanding or intelligence to enable 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.

4. To guard against possible abuse, a data user who intends to use personal data of the data subject on reliance of the consent given by the third party is required to act with caution and make necessary enquiries to form a reasonable belief that both conditions are fulfilled, failing which the data user is liable for contravention of the requirement of the PDPO.

5. As regards the definition of the "third party", building on the existing framework of the PDPO, one option is to allow a "relevant person" of the data subject as defined in Section 2(1) of the PDPO to give prescribed consent on behalf of a data subject. In this regard, the term "relevant person" in relation to an individual is defined in 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.

The definition may also be expanded to cover a third category of person if our separate proposal in Proposal No. 37 of Annex 3 (i.e. to expand the definition of "relevant person" under Section 2 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)) is adopted.

6. Adopting the definition of "relevant person" under the PDPO as the definition of third party to give consent to the change of use of personal data of vulnerable classes of data subjects is one possible option. There may be concerns that allowing only the "relevant person" to give prescribed consent to the change of use of the data subject's personal data may pose difficulties or prolong the process for the data subject concerned to access essential services. This may happen in situations where the

minor is entrusted to the care of relatives or various types of child care placement because "the person who has parental responsibility for the minors" is untraceable or does not exercise proper care for the best interest of the minor. Such concern can be accommodated by including the parties in question as "third party" under this proposal. Views are invited on the definition of third party which is empowered to give prescribed consent under this proposal.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

7. Under Section 18(1) of the PDPO, a data subject or a "relevant person" on his behalf has the right to make a request to a data user to access the data subject's personal data. A "relevant person" in relation to an individual is defined under Section 2(1) of the PDPO to mean, among others, "where the individual is a minor, a person who has parental responsibility for the minor".

8. Questions arise as to whether a data user shall, pursuant to a data access request made by a parent, release the personal data of a child to the parent in circumstances such as :

(a) where the parent may abuse the data access mechanism to obtain the personal data of the child for the parent's own purpose rather than making it "on behalf of" the child. For instance, an estranged parent may make a data access request to the school or social welfare organizations for his/her child's location data to trace the whereabouts of the child or the other parent of the child;

(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.

9. Any proposal to restrict parents' right of access to his/her child's personal data is controversial, as it touches on the sensitive issues of the rights and obligations of parents in caring for their children. Parents are under a legal responsibility to exercise proper care of their children under the age of 18. These include managing their children's health, education, or other children or youth affairs.

As such, the right to access their children's data is important in their performance of this duty. For instance, parents have a principal role to play in combating the problem of youth drug abuse. In this regard, parents may wish to know what has happened to their children, and their access to such information should not be unreasonably restricted.

10. On the other hand, we also need to respect the right of the child to his or her personal data privacy. As explained in paragraph 8 above, there may be circumstances where a parent may not be genuinely making a data access request on behalf of his child. That apart, where a child has given the information to a social worker in confidence, the social worker will be in a dilemma if he has to accede to the parent's data access request as he is required by ethical code to maintain confidentiality.

11. To strike a balance between respecting parents' role in taking care of their children and respecting children's privacy right, one possible option is to allow a data user to refuse to comply with a data access request made by a "relevant person" on behalf of a minor if the data user has reasonable grounds to believe that compliance with the request would not be in the best interests of the minor. Consideration may also be given to specifying some factors to enable the data user to assess whether there are reasonable grounds to refuse a parent's data access request.

12. Views are invited on the following :

(a) whether new provisions should be introduced to permit a data user to refuse a data access request made by a "relevant person" on behalf of a minor in order to protect the interests of minors taking into account the need for parents to exercise their rights and responsibilities over their children for the proper care of them; and

(b) if new provisions should be introduced, whether the possible option set out in paragraph 11 above is appropriate; and whether some factors should be specified to enable the data user to assess if there are reasonable grounds in refusing such a data access request.

Proposal No. 15 : Access to Personal Data in Dispute

13. A data subject may 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 (data access request). In the course of enquiry or investigation, the PCPD may request production of the requested data for examination and may keep a copy of the requested data for record. After the PCPD makes a decision, the aggrieved party may lodge an appeal with the Administrative Appeals Board ("AAB") or apply for a judicial review. Under the Administrative Appeals Board 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. The standing instruction made by the AAB would normally require the PCPD to serve on the AAB, the appellant and the party bound by the decision 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.

14. The discovery process 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 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 was lawful.

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

16. To address the problem mentioned in paragraphs 13 to 14 above, we may consider adding a provision under 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 the AAB, the court or magistrate, whether by discovery or otherwise, pending a determination in favour of the requestor. We would like to invite comments on this proposal.

(B) Rights and Obligations of Data Users

Proposal No. 16 : Refusal to Comply with a Data Access Request on Ground of Compliance with Other Legislation

17. Section 19 of the PDPO requires a data user to comply with a data access request subject to various grounds for refusal specified in Sections 20 and 28(5). However, the grounds for refusal do not cover the situation where a data user is obliged or entitled under any other ordinances not to disclose the personal data. 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, which would attract penal consequences. On the other hand, the PCPD's decision may be challenged if it accepts a data user's compliance with a statutory secrecy requirement or a statutory right on non-disclosure as a ground for refusing a data access request, which does not fall within any of the grounds of refusal under Sections 20 and 28(5).

18. A number of local ordinances impose a statutory duty of "secrecy" or a duty not to disclose information. Examples include Section 74 of Sex Discrimination Ordinance (Cap. 480) and Section 15 of The Ombudsman Ordinance (Cap. 397).

19. The personal data privacy legislation of Australia, New Zealand and the UK waives the need for a data user to comply with the data access requirement governing personal data when there is competing statutory requirement governing non-disclosure of information.

20. To solve the predicament, we may consider 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 is obliged or entitled under any other ordinances not to disclose the personal data. In this regard, we need to take into account various considerations, including the need for data users to comply with

any relevant statutory requirement governing non-disclosure of information in other ordinances and the interests of data subjects who request access to the personal data. We would like to invite comments on this proposal.

Proposal No. 17 : Erasure of Personal Data

21. According to Section 26 of the 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) that the data are 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. The duty is an absolute one, and the burden imposed on data users is onerous.

22. In a number of overseas jurisdictions (including Australia, Canada, New Zealand and the UK), data users are generally regarded to have fulfilled similar requirement by taking reasonably practicable steps to erase obsolete personal data.

23. Whilst timely erasure of obsolete personal data is important, any PDPO requirements should not be such as to pose an excessive burden to businesses. Section 26 and DPP 2(2) impose an absolute duty on a data user to erase obsolete personal data. We may consider amending the PDPO so that the provisions 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. For example, a data user would not be in breach of Section 26 and DPP 2(2) if it is not practicable for him to erase only those obsolete personal data from a microfilmed document. We would like to invite comments on this proposal.

Proposal No. 18 : Fee Charging for Handling Data Access Requests

24. Section 28(2) of the PDPO provides that a data user may, in complying with to a data access request, impose a fee on a requestor for a copy of the personal data to be supplied. Section 28(3) requires that the fee thus imposed shall not be excessive. The data user may, under Section 28(5), refuse to comply with a

data access request unless and until the fee charged for the request has been paid. The rationale for requiring the fee to be charged for compliance with a data access request should not be excessive is to protect a data subject's right to gain access to his own personal data. An excessive fee may deter an individual from making a data access request. However, the term "excessive" is not defined in the PDPO.

25. The fee charged for supplying a copy of the requested data in a data access request varies considerably from one data user to another. This disparity may be due to the difference in the operation costs of different data users. Over the years, the PCPD has received a number of complaints alleging that the fees charged by some data users were excessive.

26. 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. Data users are not allowed to charge a fee that exceeds the prescribed maximum.

27. There may be merits in setting the maximum fee for handling a data access request for the purpose of complying with the requirement of Section 28(3) of the PDPO. This may deter the imposition of an excessive charge for data access by a data user. It would also let a data subject have a rough idea on the likely fee he has to pay for a copy of his own personal data.

28. One possible option 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 optical disc/DVD+R optical disc for audio recordings or visual images, duplicate of radiological imaging records (e.g. X-ray film, magnetic resonance imaging (MRI), computerized tomography (CT) scan, positive emission

tomography (PET) scan, ultrasound), 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.

29. Comments are invited on the following :

(a) whether for the purpose of complying with Section 28(3), 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.

Proposal No. 19 : Response to Data Access Requests in Writing and Within 40 days

30. At present, a data subject may make two types of data access requests to a data user under Section 18(1), namely:

(a) a request to inform him whether the data user holds his personal data; and
(b) if the data user holds such data, a requestor to be supplied by the data user with a copy of such data.

A data user is required under Section 19(1) 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 that the data user is required to inform the requestor in writing of this.

31. From the personal data protection perspective, we see a justified case to pursue a proposal which requires a data user to inform a requestor in writing if he does not hold the requested personal data, bearing in mind that a data access request (and also a data correction request) is required to be made in writing, and Section 19(2) of the PDPO requires notice to the requestor to be in

writing if a data user is unable to comply with a data access request within 40 days.

32. However, the proposal will pose serious problems for the Police in handling personal data access requests in respect of criminal conviction records. At present, in handling such requests, the Police will only orally advise a person with a clear record. This practice is underpinned by rehabilitation considerations for ex-offenders as well as concerns about possible forgery of/unauthorized alterations to documents issued by the Police to confirm a clear record. If the proposal also covers such requests, it may produce "underclass" citizens who cannot produce clear criminal conviction records. This will deal a serious blow to the rehabilitation of ex-offenders. One option is to exempt a reply from the Police on clear record in respect of a request for access to criminal conviction record data from the proposed requirement for a written response.

33. As a related issue, if a requestor asks to be provided with a copy of his personal data (as mentioned in paragraph 30(b) above) and the data user does not hold the personal data requested, there is nothing in the request for the data user to comply with for the purpose of Section 19(1). It would appear that the data user is not required to give any response to the requestor. It would be against the legislative intent of the PDPO, if the data user were under no duty to respond to the requestor within 40 days that it did not hold the data.

34. To rectify the anomaly, we propose to make it clear that the obligation for a data user to respond to a data access request within 40 days under Section 19(1) shall also apply even if the data user does not hold the data concerned. In line with the rationale in paragraph 31, the response should be in writing. In the case of criminal conviction record, if the Police does not hold criminal conviction record data of the individual, the verbal response should also be given within 40 days.

35. Comments are invited on the following:

(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; and

(b) whether a data user is 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.

(C) Enforcement Powers of the PCPD

Proposal No. 20 : Circumstances for Issue of an Enforcement Notice

36. Section 50 of the PDPO provides that the PCPD, following the completion of an investigation, may issue an enforcement notice to direct a data user to take such steps as are specified in the notice to remedy the contravention or the matters occasioning it. The PCPD may serve an enforcement notice on a data user where 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.

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.

37. Under the provisions in Section 50 of the PDPO, the PCPD is unable to issue an enforcement notice on a data user if the act or practice has ceased and there is no likelihood of repetition, even if such an act has caused harm or damage to the data subject.

38. The powers granted to the Information Commissioner of the UK in similar circumstances are not as restrictive as those for the PCPD.

39. To enhance the effectiveness of the PDPO in the protection of personal data privacy, one option is to allow discretion for the PCPD to serve an enforcement notice under any of the following circumstances:

(a) whether the act of contravention is continuing;

(b) whether the contravention will continue or be repeated;

(c) whether the contravention has caused or is likely to cause damage or distress to the data subject.

Comments are invited on this option.

Proposal No. 21 : Clarifying Power to Direct Remedial Steps in an Enforcement Notice

40. 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, where the PCPD is of the opinion that the relevant data user should desist from doing an act or engaging in a practice, it is not appropriate to specify a period for compliance. Imposing such a requirement may be misconstrued as suggesting that a data user is only required to desist from doing an act or engaging in a practice within that specific period, but not thereafter. To clear up this grey area, we propose to specify in Section 50(1) that the PCPD has the power to direct the relevant data user in an enforcement notice to desist from doing an act or engaging in a practice. Comments are invited on this proposal.

Proposal No. 22 : Removing the Time Limit to Discontinue an Investigation

41. Under Section 39(3) of the PDPO, 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. Accordingly, after the expiry of the 45-day time frame, the PCPD may have to continue an investigation even if he subsequently finds that further investigation is not warranted (e.g. the complaint was not made in good faith) or is unnecessary (e.g. the party being complained against has already taken remedial action and there is no indication of recurrence of the alleged contravention). The continuation of such an investigation is not fair to the party complained against. Neither is it conducive to the optimal use of PCPD's resources.

42. The EOC and The Ombudsman, as well as overseas privacy authorities we are aware of, are not subject to similar statutory

requirement to notify their complainants within a prescribed time limit of their decision to refuse to carry out or continue an investigation.

43. One option to address the aforesaid problem is to remove the time limit imposed under Section 39(3) with regard to a decision to discontinue an investigation. However, the existing requirement under Section 39(3) that the PCPD should notify a complainant in writing his decision not to continue the investigation and the reasons for the decision should remain. The complainant will continue to have the right to appeal against the PCPD's decision not to carry out or to discontinue an investigation under Section 39(4). Comments on this option are welcome.

Proposal No. 23 : Additional Grounds for Refusing to Investigate

44. 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;

(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.

45. The PCPD has a wide discretion to refuse to carry out or continue an investigation on the last ground, i.e. that 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.

46. One option is to include such scenarios 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 an investigation. It would help minimize potential contention about the exercise of discretion by the PCPD under Section 39(2)(d) (i.e. "any investigation or further investigation is for any other reason unnecessary") and hence reduce the chances of complainants taking the cases to the AAB. We have considered the scenarios identified by the PCPD, and have reservations in including as a ground of refusal if a complaint relates to an action for which the complainant has a remedy in any court or tribunal (i.e. paragraph 45(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 into a complaint on the aforesaid ground would deprive an aggrieved party of an alternative for redress.

47. Moreover, the inclusion of these additional specific grounds for refusal to investigate (particularly paragraph 45(a)) 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 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 PCPD to refuse investigation.

48. 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 law enforcement agencies.

(D) Introducing New Exemptions

Proposal No. 24 : Transfer of Personal Data in Business Mergers or Acquisition

49. During the due diligence stage of merger, amalgamation, transfer or sale of businesses, business information which may contain personal data held by one business 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 from 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.

50. It would be in the economic interest of the community to facilitate the transfer of the control of businesses. However, any proposed regulatory framework governing transfer of personal data in business merger or acquisition must strike a proper balance between the protection of personal data privacy interests of the data subjects concerned and the business interests in general.

51. 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.

52. A possible option is to exempt personal data used for the purpose of effecting a merger, acquisition or transfer of business from DPP 3 on condition that :

(a) the resultant organization or the business transferee will provide essentially the same or similar service to the data subjects as 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 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.

To safeguard the exemption from being abused, consideration may be given to impose a fine for contravention of the requirements on the retention and restriction on the use of personal data mentioned in (d) and (e) above.

53. Comments are invited on the following :

(a) whether an exemption from DPP 3 should be provided for the transfer or disclosure of personal data in intended merger,

acquisition or transfer of businesses subject to the condition that the resultant organization will offer substantially similar service as the original data user; and

(b) if yes, whether the option set out in paragraph 52 above is appropriate.

Proposal No. 25 : Provision of Identity and Location Data on Health Grounds

54. Under Section 59 of the PDPO, 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 other types of personal data, such as location and identity, of the data subject.

55. The provision of personal data relating to the identity and the location of the data subject can facilitate immediate access and rescue actions. For example, the supply of the location data about the "999" emergency caller by the telephone company can speed up rescue actions by the Police. Provision of the identity and location data of an individual suspected to have a social or mental problem by the Police to the Social Welfare Department can enable the latter to offer prompt assistance to the benefit of the individual concerned. In emergency crisis, such as the 2004 East Asian tsunami catastrophe, the Immigration Department can supply the location data of missing Hong Kong people to the rescue teams and/or their relatives. There is genuine operational need to provide personal data other than physical or mental health of a data subject for the benefit of the data subject or any other individuals in such circumstances.

56. 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.

57. The disclosure of identity and location of a data subject would have significant impact on personal data privacy of individuals. In this regard, we need to consider the following :

(a) whether the well being of the individual and public interest at stake outweigh the intrusion into personal data privacy; and

(b) whether the extent of disclosure is proportionate to the benefits to be achieved, i.e. the prevention of serious bodily or mental harm to the data subject or any other individuals in this case.

58. One option is 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. Comments are invited on this option.

Proposal No. 26 : Handling Personal Data in Emergency Situations

59. 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, law enforcement agencies (LEAs) as well as rescue and relief agencies can only share personal data where the use of such data for accident or emergency rescue was envisaged at the time of their collection. The same applies to the provision of data by third parties to these agencies. Personal data which could assist these agencies to carry out the rescue-related tasks would typically include the identity, location, movement history, next-of-kin details etc. of the individuals concerned.

60. 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 an organization or a third party holding relevant personal data to assist in rescue related work. They have to notify the relatives or next-of-kin of the victims that the victims were injured and to which hospital the victims have been admitted. Although it is possible for these agencies to collect personal data directly from the victims who are conscious at the scene or in the hospital for the purpose of contacting their family

members, compliance with the requirement under DPP 1(3)[1] in time-critical rescue would cause delay for the victims to receive medical treatment or be delivered to the hospital. Relief agencies need to collect the names and other relevant personal particulars of individuals involved in the emergency for registration to facilitate the provision of relief services and handle enquiries on whether an individual is involved in that emergency. Exemption from DPP 1(3) and DPP 3 would be essential for these operations and in the interests of the victims.

61. We may consider exempting personal data held by any data user from the provisions of DPP 1(3) and DPP 3 in any case related to rescue and relief work by LEAs and rescue and relief agencies 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).

62. Any proposed mechanism which grants exemption for handling personal data in an emergency situation would have significant impact on personal data privacy. In granting such exemption, we need to consider whether the public interest in protecting the well-being of the data subjects in question is significant enough to justify the extent of intrusion into their personal data privacy. The permitted purposes of use, the duration and restrictions imposed regarding the use of personal data under the emergency or catastrophic situation have to be specified clearly to contain the risk of improper or unauthorized handling of personal data.

63. Comments are invited on whether specific exemption from DPP 1(3) and DPP 3 of the PDPO should be granted in the handling of accidents or other life-threatening situations by LEAs

[1] DPP 1(3) requires a data user to take all practicable steps to provide a data subject with certain requisite information (including purpose of collection and to whom the personal data may be transferred) at the time of collection of personal data from the data subject.

and rescue and relief agencies.

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

64. Parents and guardians have a primary responsibility for the upbringing and development of their children. This responsibility to exercise proper care and guardianship of children under the age of 18 is also recognized under the Protection of Children and Juvenile Ordinance (Cap. 213). Section 34 of Cap. 213 authorises a Juvenile Court to issue a Care and Protection Order to order a minor's parent or guardian to enter into recognizance to exercise proper care and guardianship. Parents and guardians may not be able to carry out their responsibility effectively without reasonable access to their children's personal data.

65. Section 18(1) of the PDPO allows parents or guardians of minors to access the personal data of the minors. However, the Ordinance does not allow data users to transfer, of their own accord, the personal data of minors to their parents or guardians, even if such transfer is to the benefit of the minor concerned. Examples of such needed transfer include transferring the personal data of a minor to his parents or guardian when the minor gets into trouble (e.g. being arrested or charged for a criminal offence), or when a minor suffering from the scourge of drugs refuses help by professionals. Where the Police have concrete proof that the minor will likely commit a crime, or will become a repeat offender, and that the knowledge of the parents or guardian of the matter will help prevent the committing of the offence, the Police would be able to invoke the exemption under Section 58 of the PDPO in relation to crime prevention, and transfer such data to the parents or guardians of the minor. However, such concrete proof is not easily available, and it makes the transfer of such data not possible in some cases without the consent of the minor.

66. We may consider providing an exemption under the PDPO to allow data users to transfer personal data of a minor that are relevant to parental care and guardianship to the parents or guardian of the minor, so that the latter can better fulfill their responsibility to exercise proper care and guardianship of their

children under the age of 18. Since such exemption would intrude into the personal data privacy of minors, a balance has to be struck on the need to protect the well-being of minors at risk as against protection of their personal data privacy. Any exemption to be granted has to be narrowly defined. We have to consider how to define the circumstances to invoke such exemption, such as restricting the disclosure to minor "at risk" cases, and on condition that the transfer is in the best interests of the minor.

67. Comments are invited on :

(a) whether an exemption from DPP 3 should be provided to permit transfer of personal data of minors to their parents or guardians to enhance the protection of vulnerable minors and those at risk so that parents and guardians can properly discharge their responsibility on proper care and guardianship;

(b) if yes, what specific conditions should be attached to restrict the transfer to cases which are absolutely necessary.

Annex 2

Proposals not to be Pursued

1. We have considered a number of proposals relating to scope of regulation of the PDPO, and exemptions from the provisions of the PDPO. After deliberating on the implications of the proposals, we are not inclined to pursue them. They are set out in paragraphs 2 to 29 below.

(A) Scope of Regulation under the PDPO

A.1 Revamping Regulatory Regime of Direct Marketing

2. Section 34 of the PDPO regulates the use of personal data in carrying out direct marketing activities by data users. It requires a data user who has obtained personal data and use such data for direct marketing purposes to inform the data subject of his opt-out right. The data user shall not use such personal data for carrying out direct marketing activities, if the data subject has requested the data user to cease to so use his personal 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 (up to $10,000).

3. To address the proliferation of uncontrolled direct marketing activities, we have examined the possibility of revamping the regulatory regime for direct marketing activities under the PDPO. The options include :

   (a) to introduce a new requirement that when personal data are used for direct marketing for the first time, the data user has to obtain the explicit consent of the data subject for the use of the latter's personal data (i.e. "opt-in" choice); and

   (b) to set up a territorial wide central Do-not-call register against direct marketing activities.

4. The objective of the PDPO is to protect personal data privacy of individuals. Section 34 of the PDPO already regulates 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 of contravention of the requirements under Section 34 (please refer to Proposal No. 12).

5. Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the UEMO. The Administration is monitoring the situation of using person-to-person calls for telemarketing purpose and will consider the possibility of regulating such activities under the UEMO if the problem grows in future.

6. In the circumstances, we do not consider it appropriate to make further amendments to Section 34 of the PDPO.

A.2 Internet Protocol Address as Personal Data

7. In March 2006, the PCPD received a complaint alleging the disclosure of an email subscriber's personal data by email service provider had infringed the provisions of the PDPO. One of the crucial issues to be considered was whether an Internet Protocol address ("IP address") alone would be regarded as personal data within the definition of the PDPO. Separately, there were suggestions that the Government should review the PDPO and adopt measures to prohibit the disclosure of IP addresses to third parties by email service providers without the authorization of the subscribers.

8. 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. In his investigation report dated March 2007 on the above-mentioned complaint case, 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.

9. There is a lack of judicial authority on whether IP address constitutes personal data. There is also no universally or internationally recognized definition on personal data. For reference, the Data Protection Working Party of the European Union ("EU") considered that in most cases IP addresses relate to identifiable persons. In this regard, personal data is defined in Article 2(a) of the EU Directive as any information relating to an identified or identifiable natural person, and an identifiable

person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

10. 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 various industry 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) because an IP address is a piece of addressing information that flows through different parties in the Internet world outside the control of a single ISP or network operator. Moreover, an IP address, if combined with other identifying particulars of an individual, will be afforded protection under the PDPO. Deeming an IP address as personal data also begs the question as to why cookies, email address, mobile phone number, vehicle registration mark, Autotoll tag number, Octopus card number, etc, cannot likewise be regarded as personal data under the PDPO since they are also capable of "indirectly" identifying a particular individual through tracing. In the circumstances, we do not consider it appropriate to deem IP address per se as personal data under the PDPO.

A.3 Territorial Scope of the PDPO

11. 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, mainly because of enforcement difficulties. In their view, the mere presence, without more, of a person in Hong Kong who has the ability to control his business abroad, which collects, holds, processes or uses personal data, is generally not sufficient to attract or to enable the PCPD to assume jurisdiction under the Ordinance.

12. 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 span of control under the PDPO. This was based on the model of the United Kingdom.

The LRC considered it important that data protection law in Hong Kong should apply to a data user within the 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 transborder data flow.

13. The proposal in paragraph 11 above 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 outsource the holding, processing and use of personal data to offshore agent(s). This may risk Hong Kong being turned into a data haven free of effective controls on personal data, which would not be in the interest of promoting the free flow of data to Hong Kong. We are not inclined to pursue this proposal.

(B) Exemptions

B.1 Public Interest Determination

14. At present, specific exemptions from subject access (DPP 6 and Section 18(1)(b)) and DPP 3 are provided for under Part VIII of the PDPO on grounds of specified public interests, including security, defence and international relations in respect of Hong Kong (Section 57), law enforcement and regulation (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.

15. To provide for regulatory flexibility when public interest outweighs the degree of intrusion into personal data privacy, we may consider adding a new provision to empower the Privacy Commissioner to make a public interest determination (including a temporary public interest determination for applications which require urgent decision), with conditions, if any, imposed on a case-by-case basis upon application by the relevant data user.

16. The existing exemptions provisions under the PDPO strikes a balance between privacy rights and public interest in specific circumstances. The proposed public interest determination provision will be operated on an ad hoc and a case by case basis. Such a mechanism if instituted will undermine the certainty of personal data privacy protection afforded to data subjects. As

such, we do not consider it appropriate to pursue such a proposed provision. If there are justifications to grant exemption on specific grounds, it is more appropriate to address them by way of specific public interest exemptions.

B.2 Public Domain Exemption

17. The PCPD proposes to provide for a new exemption from DPP 3 (use of personal data principle) for personal data available in the public domain. In making this proposal, the PCPD 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 provide a search of an individual's property ownership, the use of personal data contained in public register for 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.

18. The LRC had carefully deliberated on whether data protection laws should completely exempt public registers. The LRC expressed concerns that an exemption would sanction data collected for specific purposes being used for another purpose not originally envisaged by the person furnishing the data. They 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."

19. There is no public domain exemption in personal data protection laws of the UK, New Zealand and Australia. In our view, putting personal data in the public domain does 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, it would provide data users with the opportunity to subvert the law by publicizing 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 a case to take this proposal forward.

(C) Powers of the PCPD

C.1 Power to Search and Seize Evidence

20. 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 Privacy Commissioner, however, has no power to search and seize evidence. The PCPD proposes that the Commissioner be equipped with the power to search and seize evidence in order to gather evidence for prosecution proceedings.

21. The existing provisions of the PDPO are to address the concern voiced during the legislative process that this newly established investigative body should not be vested with full powers of search and seizure. Similar concern was shared by the LRC. While the LRC believed that powers to enter premises and obtain evidence are necessary to enable the Commissioner to carry out his functions, the data user's consent should first be sought but, if that is not forthcoming, the court should be empowered to make an appropriate order for entry and seizure.

22. 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 4 in Chapter 5), there is no need to provide these additional powers to the Privacy Commissioner. We also consider the existing investigative power of the PCPD adequate. In the circumstances, we are not inclined to take forward the proposal.

C.2 Power to Call upon Public Officers for Assistance

23. In the exercise of the PCPD's power of investigation and inspection, the Privacy Commissioner may need to enter premises. Where resistance or obstruction is encountered, the PCPD would need to seek assistance from the police. Expert advice and assistance are also required in investigation. These include information technology and computer forensics, identification of suspects by use of digital images, and reconstruction of criminal

activities requiring software analysis, reverse engineering decryption and presentation of digital data. 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 Privacy Commissioner 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.

24. 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 Privacy Commissioner 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 who, without lawful excuse, obstructs, hinders or resists the Privacy Commissioner or any other person in the performance of his functions or the exercise of his powers under Part VII (inspections, complaints and investigations). In the circumstances, an express provision as proposed by the PCPD would not be necessary.

C.3 Power to Conduct Hearing in Public

25. Section 43(2) of the PDPO provides that any hearing for the purpose of an investigation shall be carried out in public unless the Privacy Commissioner considers otherwise or the complainant requests that the hearing be held in private. The PCPD opines that the provision will hinder the Commissioner from holding the hearing in public, particularly when issues of public interest and importance are involved and when members of the public have a genuine right to know and to be informed. We have considered whether the Privacy Commissioner 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.

26. 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 practice, Australia requires conferences in relation to a complaint to be conducted in private, and New Zealand has similar requirement for the conduct of investigations.

27. The LRC considerations for granting the data subject the right to demand a private hearing are still valid today. We do not see a need to change the system. In this regard, Section 48(2) of the PDPO empowers the Privacy Commissioner 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.

C.4 Time Limit for Responding to PCPD's Investigation/Inspection Report

28. A data user is currently allowed under Section 46(4)(b) to advise the Privacy Commissioner within 28 days whether he objects to the disclosure in the report on inspection or investigation prepared by the PCPD any personal data that are exempt from the provisions of DPP 6 by 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.

29. We envisage that data users in some cases may need to circulate the report for comments and seek legal advice before they can provide an official response to the PCPD. Such a course of action takes time. A response period of 14 days is unreasonably tight. In our view, shortening of the response period by 14 days will not significantly improve the timeliness of publication of an inspection or investigation report. We do not consider it appropriate to take forward the proposal.

Annex 3

Miscellaneous Proposed Amendments to the PDPO

(A) Statutory Powers and Functions of PCPD

Proposal No. 28 : Relieve PCPD's Obligation to Notify the Complainant who Has Withdrawn his Complaint of Investigation Result

- **To relieve the PCPD's obligation to notify the complainant of the investigation result and related matters under Section 47(3) when the complainant has withdrawn his complaint.**

(Background: 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 Commissioner 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. 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 proposed to serve an enforcement notice on the relevant data user in consequence of the investigation and such 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 aims to remove the notification requirement in such circumstance.)

Proposal No. 29 : PCPD to Disclose Information in the Performance of Functions

- **To amend Section 46 to allow the PCPD and his prescribed officers to disclose information reasonably necessary for the proper performance of his functions and exercise of his powers.**

(Background: Section 46 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 limited specified circumstances. These include :

(i) court proceedings for an offence under the PDPO;
(ii) reporting evidence of any crime; or
(iii) disclosing to a person any matter which in the PCPD's opinion may be ground for a complaint by that person.

The 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 Administrative Appeals Board which handles appeals against certain decision 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 Equal Opportunities Commission (EOC) are permitted under their respective legislation to disclose information in a number of situations associated with the proper discharge of the functions and the exercise of powers by them.)

Proposal No. 30 : Immunity for PCPD and his Prescribed Officers from being Personally Liable to Lawsuit

- **To protect the PCPD and his prescribed officers from being held personally liable for any act done or omission made in good faith in the exercise or purported exercise of PCPD's functions and powers under the PDPO.**

(Background: At present the PCPD and his prescribed officers are not immune from suit as a result of exercise of powers and functions under the PDPO. The proposal will provide the PCPD and his staff the necessary protection from such personal liability. Similar "immunity" provisions are found in the legislation governing other statutory bodies such as the Airport Authority, EOC, Mandatory Provident Fund Schemes Authority and The Ombudsman.)

Proposal No. 31 : Power to Impose Charges for Educational and Promotional Activities

- **To provide the PCPD with an express power to impose**

reasonable charges for undertaking educational or promotional activities or services.

(Background: At present, there is no express fee-charging provision under the PDPO. An express provision is necessary to provide a legal basis for the PCPD to charge fees for educational and promotional services it renders. There are examples that statutory bodies are provided with the power to charge fees. The EOC is empowered to impose reasonable charges for educational or research projects undertaken by it under Section 65 of the Sex Discrimination Ordinance. Section 9A of The Ombudsman Ordinance provides that the Ombudsman may charge such reasonable fee in respect of service approved by the Director of Administration.)

Proposal No. 32 : Power to Obtain Information to Verify a Data User Return

- **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.**

(Background: A data user is required under Section 14 to submit to the PCPD a data user return containing prescribed information, including 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. 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.)

(B) Introducing New Exemptions

Proposal No. 33 : Use of Personal Data Required or Authorized by Law or Related to Legal Proceedings

- **To create an exemption from DPP 3 for use of personal data required or authorized 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.**

(Background: A data user may be required or authorized by or under law, 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. Moreover, under the existing provisions, the exemption from application of DPP 3 does not cover the use of personal data required or authorized by or under law or court orders, or related to legal proceedings or for establishing, exercising or defending legal rights. It is reasonable and legitimate for data users to change the use of personal data in such circumstances. 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.)

Proposal No. 34 : Transfer of Records for Archival Purpose

- **To create an exemption from DPP 3 for the transfer of information containing personal data of historical, research, educational or cultural interests to the Government Records Service ("GRS") for archival purpose.**

(Background: 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 (use of personal data principle). Given the size and variety of personal data collected, 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. The 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.)

Proposal No. 35 : Refusal to Comply with a Data Access Request on Ground of Self-Incrimination

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

(Background: Under common law, an individual has the fundamental right and privilege against disclosure of any information that may

incriminate himself. 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 him. The proposal serves to uphold the common law principle of privilege against self-incrimination.)

(C) Clarifying the Application of the PDPO in Certain Circumstances

Proposal No. 36 : Definition of Crime under Section 58

- **To clarify the scope of application of the exemption provision under Section 58 by defining "crime" to mean a crime under Hong Kong law, or a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation.**

(Background: Section 58(2) exempts the use of personal data for the prevention or detection of crime, etc. from DPP 3 (use of personal data principle). The existing meaning of "crime" and "offenders" in Section 58 does not contain clear words of extraterritorial application. We consider that there is a need to clarify the scope of the application of Section 58 of the PDPO to cover:

(i) Hong Kong crime;
(ii) a crime and offence under the law of a place outside Hong Kong, which is the subject of legal or law enforcement cooperation.

With the proposed amendment, law enforcement agencies 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.)

Proposal No. 37 : Expand the Definition of "Relevant Person"

- **To expand the definition of "relevant person" under Section 2 to include the guardian of data subjects with mental incapacity, who are appointed under Sections 44A, 59O, 59Q of the Mental Health Ordinance (Cap. 136).**

(Background: 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 in the PDPO to mean a person who has parental responsibility for the minor, or the person who is appointed by a court to manage the affairs of the individual who is incapable of managing his own affairs, or a person authorized in writing by the individual to make a data access request, a data correction request, or both such requests, on behalf of the individual. 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. The proposal aims to expand the definition to accord sufficient protection to the mentally incapacitated with regard to their rights to complain and make data access and data correction requests.)

Proposal No. 38 : Exclude Social Services from the Definition of "Direct Marketing"

- **To amend Section 34 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.**

(Background: 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 exercises the "opt-out" right (i.e. a data user has to cease to use the personal data of a data subject for direct marketing purposes if the data subject has so requested), the social worker will be prohibited from using the personal data to make direct contact with that individual. This would seriously frustrate the delivery of service by social workers who, in the proper interest 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 for the benefit of the target recipients from the definition of "direct marketing" under Section 34. The proposal aims to effect this amendment.)

Proposal No. 39 : Exemption for Personal Data Held by the Court or Judicial Officer

- **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.

(Background: Personal data may be handled by the courts and the 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 PDPO. The proposal gives recognition to judicial independence and immunity.)

Proposal No. 40 : Extend Time Limit for Laying Information for Prosecution

- **To specify that the time limit for laying information for prosecution of an offence under the PDPO shall be two years from the date of commission of the offence.**

(Background: The statutory time limit for laying information to prosecute an offence under the PDPO is prescribed under Section 26 of the Magistrates Ordinances. 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 need to analyze the case, the Police need to carry out investigation into a suspected offence and the Department of Justice need 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.)

Proposal No. 41 : Duty to Prevent Loss of Personal Data

- **To amend DPP 4 in Schedule 1 to make it explicit that a data user is required to take all reasonably practicable steps to prevent the loss of personal data.**

(Background: DPP 4 (security of personal data principle) requires a data user to take all reasonably practicable steps to ensure that personal data held by him are protected against unauthorized or accidental access, processing, erasure or other use. Whereas the legislative intent is that similar security measures should be taken to prevent loss of personal data, this requirement has not been made explicit in the current provision. The proposal aims to clarify the provision to better reflect the legislative intent.)

(D) Clarifying Other Operational Matters

Proposal No. 42 : PCPD to Serve an Enforcement Notice together with the Results of Investigation

- **To amend Section 47 to allow the PCPD to serve an enforcement notice together with the results of investigation upon the relevant data user.**

(Background: Section 47(2)(d) and 47(3)(e) requires 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 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, it is proposed to amend Section 47(2)(d) and 47(3)(e) to allow the PCPD to "decide whether to serve an enforcement notice" at the time of notifying the complainant and the relevant data user of the result of investigation.)

Proposal No. 43 : Contact Information about the Individual Who Receives Data Access or Correction Requests

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

(Background: 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 alternate way of compliance by allowing the data user to give the post title of the responsible person instead.)