立法會
Legislative Council

LC Paper No. CB(2)2113/11-12

Ref : CB2/BC/8/10

Paper for the House Committee meeting on 25 May 2012

Report of the Bills Committee on Personal Data (Privacy) (Amendment) Bill 2011

Purpose

This paper reports on the deliberations of the Bills Committee on Personal Data (Privacy) (Amendment) Bill 2011.

Background

2. The Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") protects the privacy of individuals in relation to personal data. PDPO covers any data relating directly or indirectly to a living individual ("data subject"), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. PDPO applies to any person ("data user") who controls the collection, holding, processing or use of personal data. Data users must follow the fair information practices stipulated in the six data protection principles ("DPPs") in Schedule 1 to PDPO in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, availability of data information, and access to personal data.

3. In June 2006, the Office of the Privacy Commissioner for Personal Data ("PCPD") formed an internal Ordinance Review Working Group to assess the adequacy of PDPO in protecting personal data privacy of individuals. On 28 August 2009, the Administration, with the support of the Office of PCPD, issued the Consultation Document on Review of PDPO to invite public views on the proposals to amend PDPO. A major objective of the review of PDPO was to examine whether the existing provisions of PDPO still afforded adequate protection to personal data having regard to the rapid development of the society, in particular advancement in technology. The Administration published the Consultation Report in October 2010.

4. According to the Administration, the legislative proposals in the Consultation Report were drawn up in the light of the views received during the public consultation exercise as well as subsequent developments; and the coming to light of the transfer of massive customer personal data by some enterprises, most notably the Octopus Rewards Limited ("the Octopus incident"). In the Octopus incident, Octopus cardholders' personal data collected under the Octopus Rewards Programme were passed to third parties by Octopus Rewards Limited for direct marketing purposes. That has aroused wide public concerns over the provision of customers' personal data by some enterprises to others for direct marketing purposes without explicitly and specifically informing the customers of the purpose of the provision and the identity of the receivers, or seeking the customers' consent. There were also concerns about the inadequacies in the existing legislation for the protection of personal data. The Administration further discussed the legislative proposals with the public from October to December 2010 and published the Further Public Discussions Report in April 2011. The Personal Data (Privacy) (Amendment) Bill 2011 ("the Bill"), which seeks to implement the proposals in the Report, was subsequently introduced into the Legislative Council in July 2011.

The Bill

5. The Bill seeks, among other things, to impose additional requirements on a data user in the use of the personal data of data subjects, or provision of such data to other persons, for direct marketing or in the sale of such data. It proposes to require a data user to allow a data subject an informed choice if the data user intends to use or provide the relevant personal data to others for direct marketing or if the data user intends to sell such data.

6. The Bill also seeks to empower PCPD to provide legal assistance to aggrieved persons intending to institute legal proceedings to claim compensation for damage by reason of a contravention of PDPO; to make new provisions relating to the powers and liability of PCPD; to create a new offence for the disclosure of personal data obtained without the consent of the data user; to impose a heavier penalty for repeated contravention of enforcement notices; to create a new offence for repeated contravention of the requirements under PDPO for which enforcement notices have been served; to introduce new exemptions in respect of certain requirements under PDPO; and to make technical amendments to improve the operation and presentation of PDPO.

The Bills Committee

7. At the House Committee meeting on 7 October 2011, Members agreed to form a Bills Committee to study the Bill. Under the chairmanship of Dr Hon Philip WONG Yu-hong, the Bills Committee held 16 meetings with the Administration and received views from eight deputations at two of these meetings. The membership of the Bills Committee is in **Appendix I**. The list of deputations which have given views to the Bills Committee is in **Appendix II**.

Deliberations of the Bills Committee

Direct marketing (clause 21 - proposed new Part VIA)

8. Members noted that the Octopus incident had aroused public concerns about the inadequacies of the existing regulatory regime and the practices adopted by some data users engaging in direct marketing. The concerns included the lack of specific requirements in PDPO for clear notification from data users to data subjects about the intended use, provision or sale of personal data for direct marketing purposes; data users requiring data subjects to give "bundled consent" to the terms and conditions of goods/services contracts and the use of their data for direct marketing purposes; the poor legibility of the written notification provided by data users to data subjects in relation to the use, provision or sale of personal data; and contravention of DPPs under PDPO not being a criminal offence. In the light of these public concerns, members have expressed support for tighter regulation of the use of personal data by enterprises in order to afford more protection to the personal data privacy of data subjects. Members have, however, found it necessary to strike a balance between safeguarding personal data privacy and business efficacy.

9. According to the Administration, the proposed regulatory requirements for the use and provision of personal data for use in direct marketing are clearer and more stringent than the existing ones under PDPO. They would enhance the transparency of the whole regulatory regime and afford more personal data privacy protection to data subjects. The proposed regulatory requirements have also struck a balance between safeguarding personal data privacy and facilitating business operations while providing data subjects with an informed choice as to whether to allow the use of their personal data in direct marketing.

"Opt-in" and "opt-out" mechanisms and "taken not to object if no reply sent within 30 days arrangement"

10. The Bill provides that a data user who intends to use or provide the personal data of a data subject to others for use in direct marketing should inform the data subject in writing of certain prescribed information and provide the data subject with a response facility through which the data subject may indicate in writing whether he objects to the intended use or provision (i.e. the "opt-out" mechanism). Members have expressed diverse views on this proposed "opt-out" mechanism. Some members consider that the proposed "opt-out" mechanism falls short of the strong public expectation revealed in the Octopus incident and is in effect a retrograde step in tightening the control over the unauthorized sale of personal data by data users. They also consider the "opt-out" mechanism unfair to data subjects because it would be incumbent upon data subjects to make a specific opt-out request or else they would be deemed not to have opted-out. Moreover, as a data subject may have provided his personal data to various data users and if he wishes to exercise his opt-out right, it would be very difficult for him to identify which data user has used his personal data for direct marketing purposes. Since a data user may also sell the collected personal data to others unless the data subject has exercised his opt-out right, some members take the view that it is too burdensome for the data subject to identify each and every person to whom the data has been sold and make an opt-out request to each of them. In this regard, they have called for the adoption of an "opt-in" mechanism under which it is incumbent upon data users to obtain explicit consent from data subjects before the use or sale of their personal data. This "opt-in" mechanism would respect a data subject's right of choice on the use of his personal data and could reduce complaints about the intrusion into personal data privacy and the cost of handling such complaints.

11. Some members, however, have expressed support for adopting the "opt-out" mechanism on the grounds that the "opt-out" mechanism has been adopted by most overseas jurisdictions and the Administration has already proposed to introduce additional specific requirements to strengthen regulation over the collection, use and sale of personal data in direct marketing. In their view, the proposed "opt-out" mechanism has already struck a balance between the protection of personal data privacy and businesses efficacy, while at the same time providing benefits and choices to consumers. They have also pointed out that following the implementation of PCPD's recommendations in his 2010 investigation report on the Octopus incident, there have been improvements in the protection of personal data. As there is public demand for direct marketing, these members consider that the adoption of an "opt-in" mechanism would have a negative impact on the operation of the direct

marketing business. They have also queried whether it is necessary for Hong Kong to take a great leap forward to adopt an "opt-in" mechanism given that most overseas jurisdictions have adopted an "opt-out" mechanism.

12. Some members consider that the Administration could adopt an "opt-out" mechanism for the use of personal data in direct marketing and an "opt-in" mechanism for the provision of personal data to others for use in direct marketing. They share the view of PCPD that the provision of personal data for gain would not be reasonably contemplated by a data subject if he was not informed of this before or at the time of data collection.

13. The Bills Committee has noted the position of PCPD that while an "opt-in" mechanism is not widely applied to the use of personal data for direct marketing purposes in overseas jurisdictions, it should be adopted in Hong Kong as an ultimate goal to better protect personal data privacy and respect customers' rights of choice. As it would take time for consumers and the trade to adjust to an "opt-in" mechanism, PCPD has suggested that an improved "opt-out" mechanism with some interim measures, such as a central "Do-not-call" register for person to person telemarketing calls, should be put in place before the full roll-out of an "opt-in" mechanism. Some members have suggested that if an "opt-in" mechanism would be adopted in future, it should be implemented incrementally rather than in one go.

14. The Administration has explained that, coupled with the introduction of the additional requirements in relation to the provision and use of personal data in direct marketing, the "opt-out" mechanism proposed in the Bill would afford better and more protection of personal data than the existing regulatory requirements under PDPO. It would also strike a right balance between the protection of personal data privacy and allowing room for businesses to operate while providing data subjects with an informed choice as to whether to allow the use of their personal data in direct marketing. The arrangement is also in line with the approach adopted under the Unsolicited Electronic Messages Ordinance (Cap. 593).

15. The Bill also proposes that data users will have to provide certain information on the intended use or provision and a response facility to data subjects for them to exercise their opt-out right. If no reply indicating objection is sent within 30 days after the required information and response facility are provided, the data subject is taken not to object. This arrangement is intended to cater for situations where the data user did not intend to use or provide the data subject's personal data to others for use in direct marketing at the time of data collection but intends to do so afterwards.

16. Members have expressed strong opposition to the arrangement as "no reply" cannot be taken as "no objection". They have pointed out that the notification from the data user about the intended use or provision of personal data may not have reached the data subject as the data user's record of the data subject's address may not be up-to-date, or the data subject's reply to indicate objection may not reach the data user. In either event, the data subject will be taken not to have opted-out. In the view of PCPD, the arrangement will place an unnecessary burden on the data subject if he exercises his opt-out right after the 30-day response period, as he may also have to deal with the person(s) to whom his personal data have been provided and not only the data user himself. The data subject may have to make his opt-out request to each and every person to whom his data have been provided.

17. Having regard to members' views and concerns in paragraphs 10 to 13 and 16 above, the Administration has agreed to withdraw the "taken not to object if no reply sent within 30 days arrangement". The Administration has put forward for the Bills Committee's consideration a revised regulatory regime under which a data user can only use or provide a data subject's personal data to others for use in direct marketing if he has provided the required information and response facility and received a reply from the data subject indicating that the data subject does not object to the data user doing so. If the data user has not received such a reply from the data subject and uses, or provides the data to others for use in directing marketing, the data user will be liable, on conviction, to a fine of $500,000 and imprisonment for three years (or a fine of $1,000,000 and imprisonment for five years if the provision is for gain). Members generally consider the revised proposal to be in the right direction. As to the details, their in-depth deliberations are elaborated in the ensuing paragraphs.

Verbal communication between data user and data subject

18. Some industry bodies consider it not uncommon for personal data to be collected and transactions concluded over the phone. Most of these transactions will be recorded as well, and the recording will be an effective safeguard for data subjects. They urge the Administration to consider accepting verbal communication between data users and data subjects, as it would be more convenient for data subjects to indicate no objection during the telephone conversation with the data users, rather than in writing. Some members share these views. Some members have also suggested that to provide additional safeguard for personal data privacy, consideration should be given to making audio recording a statutory requirement if the required information on the intended use or provision and the data subject's consent are given orally. Data users should also be required to alert data subjects that the

telephone communication between them will be recorded. Standard scripts for that purpose should be prepared by PCPD to facilitate the adoption of the practice of recording the entire telephone communication.

19. While the Bills Committee does not object to accepting oral consent, some members have expressed grave concern that this oral consent should be restricted to the use of personal data by the data user for direct marketing purposes and should not be extended to the provision of personal data (whether for gain or not) by the data user to others for use in direct marketing. In their view, data subjects may not wish their personal data to be provided to third parties in particular for monetary gains. Also, PCPD considers that sale of personal data will fall outside the reasonable contemplation of data subjects if they were not informed of this before or at the time of data collection and therefore the explicit and express consent of data subjects should be obtained. He considers that an oral consent falls short of the standard of an explicit and express consent and the provision of personal data to others for use in direct marketing should be subject to written consent so as to meet that more stringent standard.

20. Having considered members' views and concern, the Administration has agreed to introduce Committee Stage amendments ("CSAs") to permit a data user who intends to use the data subject's personal data in direct marketing for his own purposes, to provide the data subject with the required information either orally or in writing, and the data subject to indicate his consent (including indication of no objection) to the data user either orally or in writing. As an additional safeguard, the Administration also proposes that if consent is given orally, the data user must, before using the personal data in direct marketing, confirm in writing to the data subject within 14 days from the date of receipt of the consent the permitted kind of personal data and the permitted class of marketing subjects.

21. In the light of members' grave concern on the acceptance of oral consent of data subjects in relation to the provision of personal data (whether for gain or not) to others for use in direct marketing, the Administration has agreed not to pursue this. In other words, the provision of personal data (whether for gain or not) to another data user will be subject to the requirement that the data user must provide to the data subject in writing the required information. Before proceeding to provide the data, the data user must receive a reply in writing from the data subject indicating that the data subject does not object to the data user doing so.

22. Noting that a data user would be allowed to use the personal data of data subjects in direct marketing for his own purposes once he has received the

oral consent of the data subjects and sent the written confirmation, some members have expressed concern that the revised proposal could not cater for the situation where the data subjects may not receive the written confirmation and hence may not have the opportunity to raise objection to the contents of the written confirmation. They have sought the view of the Administration on the PCPD's suggestion that the personal data of a data subject can be used by a data user in direct marketing only when the data user has not received any objection from the data subject on the details of the consent as set out in the written confirmation within 14 days after the written confirmation is sent to the data subject. The Administration has advised that data user should be allowed to use the personal data in direct marketing once he has received the oral consent of the data subject and sent the written information. The data subject may subsequently at any time require the data user to cease to use the personal data.

23. As regards making audio recording a statutory requirement, the Administration has advised that it would be in the interest of the data user to keep a record of the consent of the data subject, whether in written form or audio recording. Data subjects can also make data access requests to obtain copies of the relevant recordings under PDPO. Nevertheless, to address members' concern, best practices for recording verbal communication will be covered in the guidance notes to be prepared by PCPD with a view to enhancing compliance and understanding of the new requirements proposed in the Bill.

24. Members have also deliberated on the scope of and contents to be covered in PCPD's guidance notes. In addition to the inclusion of best practices for the use and provision for use of personal data in PCPD's guidance notes, members have suggested that standard scripts and standard forms for the purposes of obtaining data subjects' oral or written consent to the intended use of their personal data should be provided in the guidance notes. At the request of the Bills Committee, the Administration has undertaken to revert to the Panel on Constitutional Affairs of the Legislative Council on the preparation of the guidance notes and the related publicity and public education work.

Meaning of sale of personal data

25. Members have also discussed the expression "sale of personal data" in the Bill. According to the submission from the Hong Kong Direct Marketing Association, in direct marketing business, personal data may be licensed for temporary sharing, but they have not been sold and no transfer of ownership is involved. While the definition of "sale of personal data" in the Bill is drafted in such a way to cover such sharing, the Association has taken issue with the use of the word "sale", which is commonly taken to mean giving up of ownership or control. To provide clarity, the Administration will introduce a

CSA to replace the expression "sale" in the Bill with the expression "provision for gain".

Grandfathering

26. Some members take the view that a data user who has collected any personal data in compliance with the existing requirements under PDPO before the commencement of the new legislative provisions relating to direct marketing should be allowed to continue to use the data already collected for direct marketing purposes after the commencement. They have suggested that before the implementation of the proposed new requirements for the provision and use of personal data in direct marketing, a one-off exercise should be conducted to grandfather the personal data that have been collected and let data subjects opt out if they choose to.

27. The Administration has advised that a grandfathering arrangement for pre-existing personal data subject to certain conditions has already been provided in the Bill, i.e. proposed new section 35I(1) (to be renumbered as section 35D(1) in the CSAs to be introduced by the Administration). The proposed new section 35I(1) provides that, for personal data which a data user has, before the entry into force of the new requirements, used in direct marketing in compliance with the existing requirements under PDPO, and which the data user intends to use in relation to the same marketing subject, the new requirements will not apply. This grandfathering arrangement, however, will only be applicable to the personal data that have been used in direct marketing before the commencement of the provisions in the Bill relating to direct marketing. Having regard to the operational need of the direct marketing business that direct marketing activities may involve the use of different combinations of personal data, the Administration has agreed to introduce CSAs to provide for the application of the grandfathering arrangement to the use of any personal data of the data subject in relation to the same class of marketing subjects if any of the data subject's personal data have been so used before the commencement date.

Mechanism to provide information on transferee(s) to data subjects

28. Some members have expressed support for PCPD's suggestion of conferring on individuals a right to be informed of the source of their personal data by direct marketers. Alternatively, consideration could be given to devising a mechanism for data subjects to request data users to provide information on each and every person to whom their personal data have been provided so that data subjects can require these persons to cease to use their personal data in direct marketing.

29. The Administration has explained that a data user who intends to provide personal data of a data subject to a third party for use in direct marketing must, under the proposed new requirements, inform the data subject of certain required information relating to the provision, including the class of persons to whom the data are to be provided (i.e. the transferee(s)). A data subject may also subsequently require the data user to notify the transferee to cease to so use the personal data. The transferee who receives such a notification from the data user must cease to use the personal data of the data subject in direct marketing in accordance with the notification. Otherwise, the transferee will commit an offence and be liable on conviction to a fine of $500,000 and imprisonment for three years (or a fine of $1,000,000 and imprisonment for five years if the provisions is for gain). The Administration considers that the proposal will afford adequate protection to data subjects and there is no need to devise the suggested mechanism.

Commencement of operation of the new requirements (clauses 1 and 21)

30. The Bills Committee notes the Administration's proposal that provisions unrelated to direct marketing or the legal assistance scheme shall commence operation on 1 October 2012. A separate commencement date will be proposed for the commencement of provisions relating to direct marketing, taking into account the need to provide sufficient time for PCPD to prepare guidance notes in relation to the promotion of and compliance with the new requirements in the Bill and for data users to prepare for the necessary documentation and procedural changes after passage of the Bill. According to the Administration, PCPD may take around nine months after the passage of the Bill to prepare the guidance notes in consultation with the relevant parties and undertake other preparatory work.

31. As there will be an interim period between the passage of the Bill and the commencement of the new requirements relating to direct marketing, PCPD has proposed a cut-off date for the grandfathering arrangement under the proposed new section 35D(1), which should be a date as soon as possible after the passage of the Bill. In the view of PCPD, some data users may, during this interim period, carry out massive direct marketing activities for the purpose of avoiding compliance with the new requirements. In order to prevent such activities, some members have expressed support for PCPD's proposal that a cut-off date should be specified under the proposed new section 35D(1). If a data user has not used personal data of data subjects in direct marketing before that date, the data user cannot rely on the proposed new section 35D(1) for exemption under the grandfathering arrangement.

32. The Administration has explained that the grandfathering arrangement is to cater for personal data collected before the commencement of the new requirements relating to direct marketing, including the data collected during the period between the passage of the Bill and the commencement of the new requirements. In the Administration's view, setting an earlier cut-off date for the grandfathering arrangement will mean advancing the commencement date of the new requirements for those data users who intend to use the personal data collected during this interim period in direct marketing. However, during this interim period, PCPD's guidance notes and other publicity and public education work to assist data users in complying with the new requirement are not yet in place. This will create unnecessary confusion to both data users and data subjects.

33. The Administration has further explained that with the latest drafting of the proposed new section 35D(1), a data user cannot trigger the exemption by simply having used the personal data of a data subject in direct marketing before the commencement date. The data user's eligibility for the exemption is also subject to the conditions that the data user has not, in relation to the use of the personal data in direct marketing before the commencement date, contravened any existing requirements under PDPO, and that the data subject has not indicated objection. The Administration has informed members that a further condition under the proposed new section 35D(1) is that the data subject must have been explicitly informed of the use of his personal data in direct marketing in relation to the class of marketing subjects before the commencement date. Also, the grandfathering arrangement will not affect the right of the data subject to object to the use of his personal data in direct marketing at any time.

Mutual assistance relationship between PCPD and his counterparts outside Hong Kong (clause 4 - proposed amendment to section 8(1)(g))

34. The Bills Committee notes with concern the proposed amendment to section 8(1)(g) which stipulates that PCPD "shall" provide assistance to his counterparts in overseas jurisdictions. While agreeing that PCPD should have the power and the discretion to decide whether to provide assistance to his counterparts in jurisdictions outside Hong Kong, some members have questioned the appropriateness of using the word "shall", as it might imply that PCPD has a duty to provide assistance upon request from his counterparts outside Hong Kong and does not have the discretion to decide whether to accede to such requests. Moreover, the proposed amendment to section 8(1)(g) may not duly reflect the mutual assistance relationship between PCPD and his counterparts outside Hong Kong.

35. Taking into account members' views and on closer examination of the preamble of section 8(2) which empowers PCPD to do all such things as are necessary for, or incidental or conducive to, the better performance of his functions, the Administration has agreed to move a CSA to delete the proposed amendment to section 8(1)(g).

Charging for promotional and educational activities (clause 4 - proposed new section 8(2A))

36. Members note that PCPD has been providing a wide range of promotional and educational activities targeted at the general public, specific sectors or individual organizations with a view to raising awareness and understanding of the provisions of PDPO. For those promotional and educational activities targeted at specific sectors or customized to meet the needs of individual organizations, PCPD normally charges a fee based on the cost recovery principle. Consideration will also be given to the payer's affordability and the market rates for similar products and services when determining the actual fees charged.

37. PCPD has assured members that he would not arbitrarily impose charges for promotional and educational activities. The proposed new section 8(2A), modelled on a similar provision in the Sex Discrimination Ordinance (Cap. 480), provides that PCPD may only impose reasonable charges.

38. While members do not object to levying a charge on those tailor-made promotional and educational activities provided by PCPD to specific sectors or individual organizations to meet their needs, they are of the view that it should be PCPD's priority to devote resources to the general public rather than individual organizations, and those promotional and educational activities targeted at the general public should be provided free of charge.

Verification of data user returns (clause 8 - proposed new section 14A)

39. Members note with concern about the proposed new section 14A which empowers PCPD to require any person to provide any document etc. for the purpose of verifying the accuracy of data user returns submitted by data users and to require data users to correct inaccurate information in the returns. Members note that under the proposed new section 14A(3), a data user can refuse to provide any document, record, information or thing, or any response to any question as required by PCPD if he is entitled or obliged under any other Ordinance to do so. Some members have queried the justification for this provision and asked the Administration to specify expressly "any other

Ordinance".

40. The Administration has advised that a data user is required under section 14 of PDPO to submit to PCPD a return containing the prescribed information set out in Schedule 3 to PDPO. The proposed new section 14A provides an additional power for PCPD to require a person to provide any document, record, information, etc. in order to assist PCPD in verifying the accuracy of the information in a data user return. According to the Administration, the secrecy provisions in other ordinances do not put an absolute ban on disclosure of information but invariably allow disclosure under specified circumstances. For example, section 4 of the Inland Revenue Ordinance (Cap. 112) and section 120 of the Banking Ordinance (Cap. 155) impose stringent secrecy provisions on information obtained under the respective Ordinances but allow disclosure of the information to the person to whom the information relates. Section 15 of The Ombudsman Ordinance (Cap. 397) permits information obtained in the course of an investigation to be disclosed only for the purposes of, among others, proceedings under the Ordinance or reporting evidence of crimes to ensure, inter alia, that investigations would not be jeopardized. In the Administration's view, secrecy provisions reflect the outcome of a balancing exercise in respect of different policy considerations including personal data protection. These secrecy provisions have also been subject to careful legislative scrutiny before enactment. In this connection, the Administration considers it not appropriate for PCPD's additional power to obtain information under the proposed new section 14A to override the secrecy provisions in other ordinances.

41. The Administration has also explained that it would not be practicable to specify all ordinances under which a person is entitled or obliged to refuse to provide any document, record, information or thing or any response to any question as required by PCPD. It would be more appropriate to set out the general rule that PCPD's additional power under the proposed new section 14A should be subject to the secrecy provisions in other ordinances.

<u>Refusal to comply with data access requests (clause 13 - proposed amendment to section 20)</u>

42. The Bills Committee notes with concern the secrecy provisions in the proposed amendment to section 20(1)(c) and the proposed new section 20(3)(ea). They provide that a data user shall or may refuse to comply with a data access request if compliance with the request is prohibited under PDPO or any other Ordinance or if he is entitled under PDPO or any other Ordinance not to disclose the data. Some members have expressed concern that the Bill does not contain any provision that gives it an overriding effect over any other ordinances. They urge the Administration to specify all the ordinances under

which compliance with a data access request is prohibited or refusal to comply with a data access request is allowed.

43. The Administration has advised that when formulating secrecy provisions, all relevant factors including not only the need to preserve secrecy, but also the need to respect the data subject's right to access his own personal data would have been taken into account. For this reason, some ordinances such as the Inland Revenue Ordinance impose a duty of secrecy on the official concerned but allow the data subject to access his own personal data, whereas some other ordinances such as the Sex Discrimination Ordinance do not allow such access. The proposed amendments to section 20(1) and (3) are intended to resolve the conflict between the requirement to comply with a data access request under section 19 of PDPO and the requirement to comply with secrecy provisions in other ordinances. Without these amendments, a data user bound by a statutory duty to maintain secrecy will face a dilemma of either breaching the data access provision of PDPO or the relevant secrecy provisions in another ordinance. At the same time, PCPD's decision may be challenged if he accepts a data user's compliance with a statutory secrecy requirement or a statutory right to non-disclosure as a ground for refusing a data access request.

44. According to the Administration, public views have been invited on these amendment proposals during the two rounds of public consultation in 2009 and 2010. The majority of the submissions received have agreed with the proposed arrangement and consider that this proposal could save the data user from the dilemma of either contravening the provisions of PDPO on data access or the relevant secrecy provision in other ordinances. The Administration considers it impracticable to specify all ordinances under which compliance with a data access request is prohibited or refusal to comply with a data access request is allowed. It would be more appropriate to set out the general rule that the right for a data subject to access his own personal data should be subject to the non-disclosure or secrecy requirements in other ordinances.

Criminal penalty for the supply of false or misleading information in a data correction request (clause 15 - proposed new section 22(4))

45. The Bills Committee notes that a criminal penalty is imposed under the proposed new section 22(4) on the supply of false or misleading information in a material particular in a data correction request. Noting that the provision of false data or inaccurate personal data in the first instance is not an offence under the existing legislation and hence no penalty will be imposed on such act, some members have questioned the need to have the new section and consider it too harsh to impose across the board a criminal penalty for supplying inaccurate

personal data in a data correction request.

46. The Administration has advised that the offence in the proposed new section 22(4) is not a new offence, but a repositioning of the existing section 64(2). The existing section 64(2) provides that a person who, in a data correction request, supplies any information which is false or misleading in a material particular for the purpose of having the personal data corrected commits an offence. There are many reasons why an individual may choose not to provide accurate personal data, say, to conceal his identity for the purpose of privacy. It is not an offence currently and it will be going overboard to impose a criminal liability on data subjects for providing false personal data to data users generally. However, the supply of false or misleading information for making a correction request is a different matter. To make a data correction request, the data subject must have a specific purpose in mind to seek the correction. The data concerned may not be provided by the data subject in the first place but may be obtained by the data user from other sources. In this regard, the Administration considers that criminal penalty would become necessary if the data subject knowingly or recklessly supplies false or misleading information for the purpose of making the data user comply with the correction request.

47. The Administration has further advised that the elements of "knowingly" and "recklessly" will be retained in the proposed new section 22(4), such that the prosecution is required to prove that the defendant knows, or is reckless as to whether, the information supplied is false or misleading. As the threshold required for committing this offence is high, the Administration considers it appropriate to impose a criminal penalty if it can be proved that the data subject knows, or is reckless as to whether, the information supplied is false or misleading in a material particular in the data correction request.

<u>Disclosure by PCPD to authorities outside Hong Kong (clause 24 - proposed new sections 46(7) to (9))</u>

48. The Bills Committee has noted that PCPD is subject to a statutory duty under PDPO to maintain secrecy in respect of all matters that come to his actual knowledge in handling complaints, investigations and inspections. This secrecy duty restricts the ability of PCPD to cooperate with his counterparts in other jurisdictions. Under international and regional enforcement cooperation arrangements, authorities handling privacy matters may seek assistance from each other regarding privacy investigations and enforcement matters. Assistance may involve cooperating on enforcement actions, sharing information about an organization or a matter being investigated, and collecting evidence in relation to privacy investigations. Parallel or joint investigations

may also be required. If privacy enforcement authorities are unable to share information, that might increase the effort required to obtain the necessary information and evidence. In the view of PCPD, it is important for PCPD to be given the discretion to share information about potential or existing investigations or enforcement actions with other privacy enforcement authorities.

49. The Bills Committee has deliberated on the scope of cooperation between PCPD and his counterparts in other jurisdictions. Some members consider the drafting of the proposed new section 46(8) too broad under which PCPD may exchange or disclose personal data in response to a request of an authority in a jurisdiction outside Hong Kong if, in the opinion of PCPD, the authority is similar to PCPD in terms of functions. They urge the Administration to provide more safeguards for personal data exchanged during the cooperation between PCPD and authorities in jurisdictions outside Hong Kong.

50. To address members' concerns and to provide certainty, the Administration has agreed to introduce CSAs to amend the proposed new section 46(7) to the effect that PCPD may disclose matters to authorities outside Hong Kong to assist the authorities in performing their functions provided that legislation similar to, or serves the same purposes as, PDPO is in force in those jurisdictions. The Administration will also introduce CSAs to amend the proposed new section 46(8) to specify conditions under which PCPD is empowered to disclose matters to authorities outside Hong Kong if the purpose is for the proper performance of his functions or proper exercise of his powers under PDPO.

Repeated contravention of enforcement notices (clauses 27 and 28 - proposed amendment to section 50 and new section 50(A))

51. The Bills Committee has noted that under the existing PDPO, a data user who contravenes an enforcement notice commits an offence. If the data user intentionally commits the same act or makes the same omission again after having complied with the enforcement notice, he is not liable to criminal proceedings. PCPD can only issue another enforcement notice to the data user. The Administration has advised that the new section 50A(3) is proposed to plug this loophole by making such act or omission an offence. As this is akin to the first time contravention of an enforcement notice, a penalty that is the same as that for first conviction is proposed.

52. Some members agree that the penalty for a second and subsequent conviction relating to enforcement notices should be heavier than the first

conviction. The proposed new section 50A(1) should better define the scope of a second or subsequent conviction. Should a data user after having complied with the enforcement notice commit the same act or make the same omission again, it should be regarded as a second and subsequent conviction and the data user should be subject to a heavier penalty for the contravention. Members also take the view that an enforcement notice should have an indefinite binding effect for certain acts and there should not be a date specified in the enforcement notice for compliance to preclude repeated contraventions for such acts.

53. The Administration has explained that PCPD is empowered to direct the data user concerned to take corrective actions for non-compliance with the provisions of DPPs by issuing an enforcement notice. If a data user has complied with the enforcement notice but subsequently commits the same act or makes the same omission in contravention of the requirement under the enforcement notice intentionally, the proposed new section 50A(3) would apply. Without serving another enforcement notice, PCPD can take legal action against the data user concerned. The proposed new section 50A seeks to enhance the deterrent effect. If a data user fails to take corrective actions for his contravention by the date specified in an enforcement notice, under the proposed new section 50A(1)(a), he will be liable to a fine at level 5, currently at $50,000, and imprisonment for two years. If the offence continues, the data user will be liable to a daily penalty of $1,000. On a second or subsequent conviction, the maximum penalty, under the proposed new section 50A(1)(b), is a fine at level 6, currently at $100,000, which is two times the maximum penalty for the first conviction. Although the term of imprisonment for a second and subsequent conviction remains unchanged at two years, the Administration has taken the view that the proposed penalty has a sufficient deterrent effect.

<u>Exemption from the provisions of Data Protection Principles 3 and 6 (clauses 31 and 32 - proposed new sections 59(2) and 59A(1))</u>

54. The scope of exemption under the proposed new section 59(2) has been of concern to the Bills Committee. DPP 3, which governs the use of personal data, prohibits any improper use, disclosure or transfer of the personal data by the data user, whereas DPP 6 provides for an individual's data access rights and data correction rights. Under the proposed new section 59(2), personal data relating to the identity or location of a data subject is exempt from DPP 3 if the application of those provisions would likely cause serious harm to the physical or mental health of the data subject or any other individual. Some members consider the scope of the proposed exemption too wide as the seriousness of the harm to the physical or mental health of the data subject could be a subjective

judgement. They suggest to narrow the scope of exemption by specifying in the provision that the person disclosing such data should believe that the disclosure would be able to mitigate or prevent serious harm to the data subject or any other person.

55. The Administration has advised that the proposed exemption would apply if the application of DPP 3 would be likely to cause serious harm to the physical or mental health of the data subject or any other individual. Under PDPO, personal data relating to the physical or mental health of the data subject is already exempt from either or both DPP 3 and 6 if the application of those provisions would be likely to cause serious harm to the physical or mental health of the data subject or any other individual. The proposed new section 59(2) is to extend the exemption to personal data relating to the identity or location of a data subject. It aims to address situations which require the timely provision of identity and location data to facilitate immediate actions to be taken by the relevant parties to prevent serious harm to the physical or mental health of an individual. The proposed exemption is one of the proposals on which public views have been invited during the previous two rounds of public consultation in 2009 and 2010. Of the submissions received, the majority have expressed support for its implementation. There are also similar exemption in the legislation in Australia, New Zealand and Canada. In case of disputes over whether compliance with DPP 3 would likely cause serious harm to the data subject, PCPD would assess whether the disclosure in reliance on the exemption is appropriate.

56. Members note that the purpose of the proposed new section 59A(1) is to facilitate the exercise of proper parental care and guardianship. Under that proposed section, personal data in relation to a minor transferred or disclosed by the Hong Kong Police Force or Customs and Excise Department to a relevant person of a minor are exempt from DPP 3 if the purpose of the disclosure is to facilitate the exercise of proper parental care and guardianship of the minor. Some members have noted with concern about the scope of the proposed section and that the exemption may result in inadequate protection to the personal data of minors. They urge the Administration to provide training and guidelines to the Police and the Customs and Excise Department in respect of the application of the exemption in the proposed section.

57. The Administration has advised that since the existing PDPO does not provide for an exemption as proposed in new section 59A, there have been occasions where the Police and the Customs and Excise Department were uncertain whether the personal data of a minor could be transferred or disclosed even if the disclosure of such data would have been for the benefits of the minor. Given the prevalence and hidden nature of the problem of drug abuse in Hong

Kong, notifying the parents or guardians of such matters would boost preventive efforts, and facilitate early identification of hidden problems and intervention for treatment and rehabilitation to prevent the problems from further deteriorating. The exemption is proposed to be confined to the Hong Kong Police Force and the Customs and Excise Department, and can only be invoked by an officer at the rank of Station Sergeant (or equivalent or above) if he is satisfied that all three conditions set out in the proposed new section are met. Nevertheless, the Administration has agreed to take on board members' suggestions to provide more detailed guidelines and training as necessary.

58. Members have expressed concern on the proposed new section 59A(2) in which a defence is provided for persons if they have reasonable grounds for believing that failure to transfer or disclose the data would likely prejudice the exercise of parental care and guardianship of a minor. They consider that the defence may undermine compliance with DPPs and have questioned its rationale.

59. The Administration has advised that the proposed new section 59A(2) is intended to provide for a defence for persons who have acted out of good faith. In the light of members' views, the Administration will move a CSA to delete the proposed new section 59A(2). Similarly, the Administration will also move a CSA to delete the proposed new section 63C(2).

Transfer of records for archive purposes (clause 34 - proposed new section 63D)

60. The proposed new section 63D provides for an exemption from the provisions of DPP3 in respect of personal data contained in Government records which are transferred to the Government Records Service ("GRS") for archive purposes. According to the Administration, the exemption is considered necessary because massive records are held by various government departments and it would not be practicable to seek the prescribed consent of the data subjects to the transfer of their data to GRS where such consent is required under DPP3. The proposed new section 63D aims to permit government departments to transfer records to GRS for archive purposes, without the need to seek data subjects' prescribed consent even if personal data are contained therein. The proposed exemption will not change the policy in respect of access to government records.

61. Ms Cyd HO does not accept the Administration's explanation. She considers the Administration's interpretation of "records" too narrow. In her view, records of archival value should not be held solely for the purposes of preservation. Some personal data contained in those archival records may be significant for research purposes and hence should be made available for public

access. In her view, there are many organizations providing archival services similar to those of GRS such as the Legislative Council Archives. Records transferred to these archival organizations should enjoy the same exemption as provided in the proposed new section 63D. She has indicated that she may consider moving CSAs to the proposed new section 63D along the following lines:

(a) to extend the exemption from the provisions of DPP 3 to include the records of the public bodies such as the Judiciary, the Legislative Council and other statutory bodies; and

(b) to give due regard to the right of the public to access public records.

Legal assistance to data subjects (clauses 37 and 38 - proposed amendment to section 66 and proposed new sections 66A and 66B)

62. The Bills Committee notes that at present, a data subject who suffers damage by reason of any contravention of a requirement under PDPO by a data user in relation to his personal data is entitled under section 66 of PDPO to compensation from the data user for that damage. PDPO, however, does not empower PCPD to provide assistance to aggrieved data subjects in respect of legal proceedings under the section. Members generally take the view that if PCPD is empowered to offer legal assistance to an aggrieved data subject who suffers damage to seek redress under PDPO, the aggrieved party may not be inhibited to file a lawsuit due to cost considerations. This could also achieve greater deterrent effect on acts or practices which intrude into personal data privacy, and enhance the overall effectiveness of sanctions provided for under PDPO.

63. The Bills Committee has expressed support for empowering PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO, based on the model of the Equal Opportunities Commission. Some members have suggested that PCPD should seek to mediate such claims for compensation before resorting to legal action.

Long title

64. Some members have questioned the need and appropriateness of setting out in the long title of the Bill a detailed list of every aspect covered by the Bill. They have expressed concern that such details might have a narrowing effect on the scope of amendments which could be moved to the Bill. They have also

pointed out that in the course of scrutiny of bills, they have found many instances of inconsistencies in the drafting style of the long titles of bills. In this connection, the Bills Committee has requested the Research Division of the Legislative Council Secretariat to conduct a research on the long titles of bills introduced into the Council in recent years to analyze the length of long titles to see if there is any trend of the Government introducing bills with longer long titles in recent years.

65. The Secretariat research has found that while the long titles of some bills are couched in broad terms, there is an apparent trend for longer and more detailed long titles to be adopted in amendment bills as compared to those in new bills. The Administration has explained that the long title of a bill should be drafted in terms wide enough to embrace the whole of the contents of the bill. The length of, and the level of details to be provided in, the long title of a bill have to be decided by reference to the context of each case. Members in general are of the view that a consistent approach should be taken in drafting the long titles of bills in accordance with some general principles. The Bills Committee agrees that the issue of drafting warrants further study and should be referred to the Panel on Administration of Justice and Legal Services for follow up.

"Data" as a collective uncountable noun

66. The Bills Committee has noted with concern the word "data" whose usage in the Bill has been changed from the plural form to the collective uncountable form. Some members have enquired about the appropriateness of such change. The Administration has explained that although the word "data" is the plural form of *datum* in Latin and is still used as such in scientific fields, it is commonly treated as an uncountable noun taking a singular verb in modern and non-scientific use. According to the Administration, this usage is widely accepted as standard English. "Personal data" is also widely reported in the English language media and in corporate and government communications as an uncountable noun with a singular verb agreement. In the Administration's view, it is appropriate to change "data" in PDPO to the singular form in order to reflect the increasingly dominant contemporary use of "data" as an uncountable noun.

Committee Stage amendments

67. Apart from those set out in the above paragraphs, the Administration has also agreed to move some other CSAs taking on board certain suggestions of the legal adviser to the Bills Committee to improve clarity and consistency.

The Bills Committee agrees to the Administration's proposed CSAs which are set out in **Appendix III**. The Bills Committee has not proposed any CSA. Ms Cyd HO has indicated that she may move CSAs to the proposed new section 63D (paragraph 61 refers).

Follow-up actions

68. The Bills Committee has agreed to refer to the Panel on Constitutional Affairs for follow up on issues relating to the preparation of guidance notes and publicity and public education to be pursued by PCPD (paragraph 24 refers) and to the Panel on Administration of Justice and Legal Services for follow up on issues relating to the drafting of long titles of bills (paragraph 65 refers).

Resumption of the Second Reading debate

69. Subject to the moving of the CSAs by the Administration, the Bills Committee supports the resumption of the Second Reading debate on the Bill at the Council meeting of 6 June 2012.

Advice sought

70. Members are invited to note the deliberations of the Bills Committee.

Council Business Division 2
Legislative Council Secretariat
24 May 2012

Appendix I

Bills Committee on Personal Data (Privacy) (Amendment) Bill 2011

Membership List

Chairman	Dr Hon Philip WONG Yu-hong, GBS
Deputy Chairman	Hon Paul TSE Wai-chun, JP
Members	Hon James TO Kun-sun Hon Emily LAU Wai-hing, JP Hon TAM Yiu-chung, GBS, JP Hon Vincent FANG Kang, SBS, JP Hon WONG Kwok-hing, MH Hon WONG Ting-kwong, BBS, JP Hon Ronny TONG Ka-wah, SC Hon Cyd HO Sau-lan Hon CHAN Kin-por, JP Dr Hon Priscilla LEUNG Mei-fun, JP Hon IP Kwok-him, GBS, JP Dr Hon Samson TAM Wai-ho, JP Hon Alan LEONG Kah-kit, SC (Total : 15 Members)
Clerk	Ms Elyssa WONG
Legal adviser	Mr Arthur CHEUNG
Date	5 March 2012

Appendix II

Bills Committee on Personal Data (Privacy) (Amendment) Bill 2011
List of deputations which have given views to the Bills Committee

1. Asia Digital Marketing Association
2. Consumer Council
3. Hong Kong Association of Banks
4. Hong Kong Bar Association
5. Hong Kong Call Centre Association
6. Hong Kong Direct Marketing Association
7. Hong Kong Human Rights Monitor
8. Hong Kong Retail Management Association
9. Office of the Privacy Commissioner for Personal Data
10. The Hong Kong Federation of Insurers
11. The Law Society of Hong Kong
12. Mr CHAN Chung-yau (member of the public)
13. Member of the public

Personal Data (Privacy) (Amendment) Bill 2011

Committee Stage

Amendments to be moved by the Secretary for Constitutional and Mainland Affairs

Clause	Amendment Proposed
1	By deleting subclause (2) and substituting— "(2) Subject to subsection (3), this Ordinance comes into operation on 1 October 2012. (3) Sections 20, 21, 37(2), 38 and 42 come into operation on a day to be appointed by the Secretary for Constitutional and Mainland Affairs by notice published in the Gazette.".
3	By adding before subclause (1)— "(1A) Section 2(1)— **Repeal the definition of *data user return*** **Substitute** "***data user return*** (資料使用者申報表) means a return submitted to the Commissioner under section 14(4) and, if applicable, corrected under section 14A(5);".".
3	By adding— "(2A) Section 2(1), in the Chinese text, in the definition of ***Committee***— **Repeal** "會。" **Substitute** "會；".
3(3)	By adding—

"***change notice*** (變更通知) means a notice served on the Commissioner under section 14(8) and, if applicable, corrected under section 14A(5);".

4 By deleting subclause (2).

7 By deleting subclause (1) and substituting—

"(1) Section 14(4)—

Repeal

"data user return"

Substitute

"return".

(1A) Section 14(5)(b), in the English text—

Repeal

"be obtained by".

(1B) Section 14(7), in the English text—

Repeal

"be obtained by".

(1C) Section 14(9)(a), after the semicolon—

Add

"and".

(1D) Section 14(9)(b)—

Repeal

"; and"

Substitute a full stop.

(1E) Section 14(9)—

Repeal paragraph (c).".

7(3) In the proposed section 14(11), by deleting "submitted to, or notice served on, the Commissioner" and substituting "or change notice".

8 In the proposed section 14A(1), by deleting everything after "data user return" and substituting—

"or change notice, the Commissioner may, by written notice served on any of the persons specified in subsection (2), reasonably require the person—

(a) to provide any document, record, information or thing

specified in the written notice; and

(b) to respond in writing to any question specified in the written notice.".

8 In the proposed section 14A(2)(b), by adding "or change notice" after "data user return".

8 In the proposed section 14A(3), by deleting "this or".

8 In the proposed section 14A(4), by deleting everything after "subsection (1), the Commissioner" and substituting "has reasonable grounds to believe that any information in a data user return or change notice is inaccurate, the Commissioner may, by written notice, require the data user to correct the information in the data user return or change notice.".

8 In the proposed section 14A(5), by deleting "the period" and substituting "such reasonable period as is".

8 In the proposed section 14A, by adding—

"(5A) A person who contravenes subsection (5) commits an offence and is liable on conviction to a fine at level 3.".

8 In the proposed section 14A, by adding—

"(7) A data user who, in purported compliance with a notice under subsection (4), knowingly or recklessly in a data user return or change notice supplies any information which is false or misleading in a material particular, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.".

9 By adding—

"(1A) Section 15—

Repeal subsection (1)

Substitute

"(1) The Commissioner must keep and maintain a register

of data users who have submitted data user returns, using information in those returns and in any change notices.

(1B) Section 15(2)(b)—

Repeal

"under section 14(4), such particulars of the information supplied in that return"

Substitute

", such particulars of the information supplied in that return and any change notice".

(1C) Section 15(3)—

Repeal

"prescribed form"

Substitute

"specified form".".

11(2) In the proposed section 18(5)(a), in the English text, by deleting "informing" and substituting "inform".

11(2) In the proposed section 18(5)(b), in the English text, by deleting "supplying" and substituting "supply".

13(3) In the proposed section 20(3)(ea), by deleting "disclose the personal data which is the subject of" and substituting "comply with".

21 By deleting the proposed Part VIA and substituting—

"**Part VIA**

Use of Personal Data in Direct Marketing and Provision of Personal Data for Use in Direct Marketing

Division 1

Interpretation

35A. Interpretation of Part VIA

(1) In this Part—

consent（同意), in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision;

direct marketing（直接促銷）means—

(a) the offering, or advertising of the availability, of goods, facilities or services; or

(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

through direct marketing means;

direct marketing means (直接促銷方法) means—

(a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or

(b) making telephone calls to specific persons;

marketing subject (促銷標的), in relation to direct marketing, means—

(a) any goods, facility or service offered, or the availability of which is advertised; or

(b) any purpose for which donations or contributions are solicited;

permitted class of marketing subjects (許可類別促銷標的), in relation to a consent by a data subject to an intended use or provision of personal data, means a class of marketing subjects—

(a) that is specified in the information provided to the data subject under section 35C(2)(b)(ii) or 35J(2)(b)(iv); and

(b) in relation to which the consent is given;

permitted class of persons (許可類別人士), in relation to a consent by a data subject to an intended provision of personal data, means a class of persons—

(a) that is specified in the information provided to the data subject under section 35J(2)(b)(iii); and

(b) in relation to which the consent is given;

permitted kind of personal data (許可種類個人資料), in relation to a consent by a data subject to an intended use or provision of personal data, means a kind of personal data—

(a) that is specified in the information provided to the data subject under section 35C(2)(b)(i) or 35J(2)(b)(ii); and

(b) in relation to which the consent is given;

response channel (回應途徑) means a channel provided by a data user to a data subject under section 35C(2)(c) or 35J(2)(c).

(2) For the purposes of this Part, a person provides

personal data for gain if the person provides personal data in return for money or other property, irrespective of whether—

(a) the return is contingent on any condition; or

(b) the person retains any control over the use of the data.

Division 2

Use of Personal Data in Direct Marketing

35B. Application

This Division does not apply in relation to the offering, or advertising of the availability, of—

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

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

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

35C. Data user to take specified action before using personal data in direct marketing

(1) Subject to section 35D, a data user who intends to use a data subject's personal data in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject—

(i) that the data user intends to so use the personal data; and

(ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use;

(b) provide the data subject with the following information in relation to the intended use—

(i) the kinds of personal data to be used; and

(ii) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without

charge by the data user, communicate the data subject's consent to the intended use.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and, if in written form, easily readable.

(5) Subject to section 35D, a data user who uses a data subject's personal data in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(7) In any proceedings for an offence under subsection (5), the burden of proving that this section does not apply because of section 35D lies on the data user.

35D. Circumstances under which section 35C does not apply

(1) If, before the commencement date—

(a) a data subject had been explicitly informed by a data user in an easily understandable and, if informed in writing, easily readable manner of the intended use or use of the data subject's personal data in direct marketing in relation to a class of marketing subjects;

(b) the data user had so used any of the data;

(c) the data subject had not required the data user to cease to so use any of the data; and

(d) the data user had not, in relation to the use, contravened any provision of this Ordinance as in force as at the time of the use,

then section 35C does not apply in relation to the intended use or use, on or after the commencement date, of the data subject's relevant personal data, as updated from time to time, in direct marketing in relation to the class of marketing subjects.

(2) If—

(a) a data subject's personal data is provided to a data user by a person other than the data subject (***third person***); and

(b) the third person has by notice in writing to the data user—

(i) stated that sections 35J and 35K have

been complied with in relation to the provision of data; and

(ii) specified the class of marketing subjects in relation to which the data may be used in direct marketing by the data user, as consented to by the data subject,

then section 35C does not apply in relation to the intended use or use by the data user of the data in direct marketing in relation to that class of marketing subjects.

(3) In this section—

commencement date（本部生效日期）means the date on which this Part comes into operation;

relevant personal data（有關個人資料）, in relation to a data subject, means any personal data of the data subject over the use of which a data user had control immediately before the commencement date.

35E. Data user must not use personal data in direct marketing without data subject's consent

(1) A data user who has complied with section 35C must not use the data subject's personal data in direct marketing unless—

(a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively;

(b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming—

(i) the date of receipt of the consent;

(ii) the permitted kind of personal data; and

(iii) the permitted class of marketing subjects; and

(c) the use is consistent with the data subject's consent.

(2) For the purposes of subsection (1)(c), the use of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data; and

(b) the marketing subject in relation to which the data is used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a use of personal data either through a response channel or other means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35F. Data user must notify data subject when using personal data in direct marketing for first time

(1) A data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.

(2) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(3) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years.

(4) In any proceedings for an offence under subsection (3), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35G. Data subject may require data user to cease to use personal data in direct marketing

(1) A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject—

(a) has received from the data user the information required to be provided in relation to the use of personal data under section 35C(2); or

(b) has earlier given consent to the data user or a third person to the use.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) A data user who contravenes subsection (3) commits an offence and is liable on conviction to a fine of

$500,000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(6) This section does not affect the operation of section 26.

35H. Prescribed consent for using personal data in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for using any personal data of the data subject in direct marketing, the data user is to be taken to have obtained the consent if the data user has not contravened section 35C, 35E or 35G.

Division 3

Provision of Personal Data for Use in Direct Marketing

35I. Application

(1) This Division does not apply if a data user provides, otherwise than for gain, personal data of a data subject to another person for use by that other person in offering, or advertising the availability, of—

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

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

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

(2) This Division does not apply if a data user provides personal data of a data subject to an agent of the data user for use by the agent in carrying out direct marketing on the data user's behalf.

35J. Data user to take specified action before providing personal data

(1) A data user who intends to provide a data subject's personal data to another person for use by that other person in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject in writing—

(i) that the data user intends to so provide the personal data; and

(ii) that the data user may not so provide the data unless the data user has received the data subject's written consent to the intended provision;

(b) provide the data subject with the following written information in relation to the intended provision—

(i) if the data is to be provided for gain, that the data is to be so provided;

(ii) the kinds of personal data to be provided;

(iii) the classes of persons to which the data is to be provided; and

(iv) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended provision in writing.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and easily readable.

(5) A data user who provides personal data of a data subject to another person for use by that other person in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction—

(a) if the data is provided for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or

(b) if the data is provided otherwise than for gain, to a fine of $500,000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35K. Data user must not provide personal data for use in direct marketing without data subject's consent

(1) A data user who has complied with section 35J must not provide the data subject's personal data to another person for use by that other person in direct marketing unless—

(a) the data user has received the data subject's written consent to the intended provision of personal data, as described in the information provided by the data user under section 35J(2)(b), either generally or selectively;

(b) if the data is provided for gain, the intention to so provide was specified in the information under section 35J(2)(b)(i); and

(c) the provision is consistent with the data subject's consent.

(2) For the purposes of subsection (1)(c), the provision of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data;

(b) the person to whom the data is provided falls within a permitted class of persons; and

(c) the marketing subject in relation to which the data is to be used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a provision of personal data either through a response channel or other written means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction—

(a) if the data user provides the personal data for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or

(b) if the data user provides the personal data otherwise than for gain, to a fine of $500,000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35L. Data subject may require data user to cease to provide personal data for use in direct marketing

(1) A data subject who has been provided with information by a data user under section 35J(2)(b) may, at any time, require the data user—

(a) to cease to provide the data subject's personal data to any other person for use by that other person in direct marketing; and

(b) to notify any person to whom the data has been so provided to cease to use the data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject has earlier given consent to the provision of the personal data.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) If a data user is required to notify a person to cease to use a data subject's personal data in direct marketing under a requirement referred to in subsection (1)(b), the data user must so notify the person in writing.

(5) A person who receives a written notification from a data user under subsection (4) must cease to use the personal data in direct marketing in accordance with the notification.

(6) A data user who contravenes subsection (3) commits an offence and is liable on conviction—

(a) if the contravention involves a provision of personal data of a data subject for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or

(b) in any other case, to a fine of $500,000 and to imprisonment for 3 years.

(7) A person who contravenes subsection (5) commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years.

(8) In any proceedings for an offence under subsection (6) or (7), it is a defence for the data user or person charged to prove that the data user or person took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(9) This section does not affect the operation of section 26.

35M. Prescribed consent for providing personal data for use in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for providing any personal data of the data subject to another person for use in direct marketing, the data user is taken to have obtained the consent if the data user has not contravened section 35J, 35K or 35L.".

New By adding—

"**23A. Section 45 amended (Protection of witnesses, etc.)**

Section 45(1), after "but any"—

Add

"enactment or".".

24 By deleting subclause (1) and substituting—

"(1) Section 46(1)—

Repeal

"and (3)"

Substitute

", (3), (7) and (8)".".

24(3) In the proposed section 46(2)(a), by adding "subject to subsection (8)," before "disclosing".

24(7) By deleting the proposed section 46(7) and (8) and substituting—

"(7) The Commissioner may, for the purpose of enabling or assisting an authority of a place outside Hong Kong to perform a relevant function of that authority, disclose matters to that authority, if—

(a) that authority has undertaken to be bound by the secrecy requirements imposed by the Commissioner; and

(b) in the opinion of the Commissioner, there is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance.

(8) The Commissioner may, for the proper performance of the Commissioner's functions or the proper exercise of the Commissioner's powers under this Ordinance, disclose matters to an authority of a place outside Hong Kong that performs a relevant function, if—

(a) that authority has undertaken to be bound by the secrecy requirements imposed by the Commissioner; and

(b) any of the conditions specified in subsection (9) is satisfied.

(8A) In subsections (7) and (8)—

relevant function (有關職能), in relation to an authority of a place outside Hong Kong, means a function relating to investigation into a suspected contravention, and enforcement, of legal or regulatory requirements in that place concerning the protection of privacy of individuals in relation to personal data.".

24(7) In the proposed section 46(9)(e), in the Chinese text, by deleting "擁有" (whenever appearing) and substituting "持有".

27(1) In the proposed section 50(1), by adding “and, if appropriate, prevent any recurrence of ”after “to remedy”.

27(1) By deleting the proposed section 50(1A)(a), (b) and (c) and substituting—

“(a) state that the Commissioner is of the opinion referred to in subsection (1) and the reason for that opinion;

(b) specify—

(i) the requirement which, in the opinion of the Commissioner, is being or has been contravened; and

(ii) the act or omission that constitutes the contravention;

(c) specify the steps that the data user must take (including ceasing any act or practice) to remedy and, if appropriate, prevent any recurrence of the contravention;”.

27 By deleting subclauses (4) and (5) and substituting—

“(4) Section 50(3)—

Repeal the section

Substitute

“(3) The steps specified in an enforcement notice to remedy and, if appropriate, prevent any recurrence of any contravention to which the notice relates may be framed—

(a) to any extent by reference to any approved code of practice; and

(b) so as to afford the relevant data user a choice between different ways of remedying and, if appropriate, preventing any recurrence of the contravention.”.

28 In the proposed section 50B(1)(a), (b) and (c), by deleting “any other person” and substituting “a prescribed officer”.

28 In the proposed section 50B(1)(a) and (c)(i) and (ii), in the English text, by deleting “that other person” and substituting “the officer”.

32 In the proposed section 59A(1), in the English text, by deleting “of a minor” and substituting “of the minor”.

32 By deleting the proposed section 59A(2).

33 In the proposed section 60A(1) and (2), by adding "a request under" before "a provision of".

33 In the proposed section 60B(a), by adding ", by any rule of law" after "enactment".

34 In the proposed section 63B(3), by deleting "sale, transfer or disclosure" and substituting "transfer, disclosure or provision for gain".

34 In the proposed section 63B(6), by deleting the definition of ***sell***.

34 In the proposed section 63B(6), by adding—

"***provision for gain*** (為得益而提供), in relation to personal data, means provision of the data in return for money or other property, irrespective of whether—

(a) the return is contingent on any condition; or

(b) the person who provides the data retains any control over the use of the data.".

34 By deleting the proposed section 63C(2).

34 By deleting the proposed section 63D(1) and substituting—

"(1) Personal data contained in records that are transferred to the Government Records Service is exempt from the provisions of data protection principle 3, when the records are used for archive purposes.".

35 By deleting the clause and substituting—

"**35. Section 64 substituted**

Section 64—

Repeal the section

Substitute

"**64. Offences for disclosing personal data obtained without consent from data users**

(1) A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent—

(a) to obtain gain in money or other

property, whether for the benefit of the person or another person; or

(b) to cause loss in money or other property to the data subject.

(2) A person commits an offence if—

(a) the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent; and

(b) the disclosure causes psychological harm to the data subject.

(3) A person who commits an offence under subsection (1) or (2) is liable on conviction to a fine of $1,000,000 and to imprisonment for 5 years.

(4) In any proceedings for an offence under subsection (1) or (2), it is a defence for the person charged to prove that—

(a) the person reasonably believed that the disclosure was necessary for the purpose of preventing or detecting crime;

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

(c) the person reasonably believed that the data user had consented to the disclosure; or

(d) the person—

(i) disclosed the personal data for the purpose of a news activity as defined by section 61(3) or a directly related activity; and

(ii) had reasonable grounds to believe that the publishing or broadcasting of the personal data was in the public interest.".".

36 In the heading, by deleting "**Section 64A**" and substituting "**Sections 64A and 64B**".

36 By renumbering the proposed section 64A as section 64B.

36 By adding before the proposed section 64B—

"**64A. Miscellaneous offences**

(1) A data user who, without reasonable excuse, contravenes any requirement under this Ordinance commits an offence and is liable on conviction to a fine at level 3.

(2) Subsection (1) does not apply in relation to—

(a) a contravention of a data protection principle;

(b) a contravention that constitutes an offence under section 14(11), 14A(5A) or (6), 15(4A) or (7), 18(5), 22(4), 31(4), 32(5), 44(10), 46(10), 50A(1) or (3), 50B(1), 63B(4) or 64(1) or (2); or

(c) a contravention of any requirement under Part VIA.".

38 In the proposed section 66A(2)(b), in the Chinese text, by deleting "鑠" and substituting "爍".

39(19) In the proposed section 2(3), in the Chinese text, by deleting "手段或其他手段" and substituting "規範方法或其他方法".

39(26) In the proposed section 4(2), in the Chinese text, by deleting "手段或其他手段" and substituting "規範方法或其他方法".