

Room 525, 5/F., Prince's Building, Central, Hong Kong  
Telephone: 2521 1160, 2521 1169 Facsimile: 2868 5035  
Email: info@hkab.org.hk Web: www.hkab.org.hk

香港中環太子大廈5樓525室  
電話：2521 1160, 2521 1169 圖文傳真：2868 5035  
電郵：info@hkab.org.hk 網址：www.hkab.org.hk

21 October 2011

By Post and email: bc\_58\_10@legco.gov.hk

Bills Committee on Personal Data (Privacy) (Amendment) Bill 2011  
Legislative Council  
Legislative Council Complex  
1 Legislative Council Road  
Central  
Hong Kong

Dear Sirs

**Personal Data (Privacy) (Amendment) Bill 2011**

1. Introduction

We refer to the Personal Data (Privacy) (Amendment) Bill 2011 which was gazetted on 8 July 2011 and introduced to the Legislative Council on 13 July 2011 (the "**Amendment Bill**"). As banks are one of the largest groups of personal data users, the Hong Kong Association of Banks ("**HKAB**") would like to submit to the Bills Committee our members' views on the Amendment Bill, in particular, the wording of those provisions which affect our members.

We believe that the Amendment Bill largely reflects the spirit of the consultation conclusions published by the Constitutional and Mainland Affairs Bureau. Nevertheless, having regard to the far-reaching implications of some of the proposed changes on the banking and business community and the society as a whole, it is of critical importance that the statutory provisions are clear and not unduly broad to facilitate efficient compliance and implementation in practice.

2. Comments on the Amendment Bill

**New Section 11A – Immunity**

**Response:**

The immunity applies in favour of the Privacy Commissioner or a prescribed officer where he performs any function or exercises any power in good faith. In order to put this beyond doubt, please revise new Section 11A(1) as marked in the following: "..... anything done or omitted to be done by the person or officer in good faith in the performance or purported performance of any function, or in

the exercise or purported exercise of any power, imposed or conferred on the Commissioner or officer under this Ordinance".

***New Section 14A - Verification of data user returns***

**Response:**

1. It remains our view that it is appropriate to maintain status quo and rely on the existing Section 64(1) of the Personal Data (Privacy) Ordinance ("PDPO") which makes it an offence for a data user knowingly or recklessly to supply false or misleading information to the Privacy Commissioner. A similar mechanism applies under the Banking Ordinance and the Securities and Futures Ordinance.
2. In any event, new Section 14A should expressly provide for the power to be exercised by the Privacy Commissioner in a reasonable manner. The power conferred on the Hong Kong Monetary Authority and the Securities and Futures Commission to require production of documents or information by relevant persons for the purposes of performing their regulatory functions (including conducting investigations) is subject to similar reasonableness requirement. We consider that the Privacy Commissioner should be subject to the same reasonableness requirement as the financial regulators. We also note that a reasonableness requirement is incorporated in respect of the Privacy Commissioner's power under Section 15(3) of the PDPO.

Further, the exemption from compliance specified in new Section 14A(3) is too narrow.

3. Accordingly, we propose to revise new Section 14A as marked below:
  - (1) For the purpose of verifying the accuracy of information in a data user return submitted under section 14, the Commissioner may, by written notice, require any of the persons specified in subsection (2) -
    - (a) to provide any document, record, information or thing reasonably specified in the notice; and
    - (b) to respond in writing to any question reasonably specified in the notice, which the Commissioner has reasonable grounds to believe to be relevant for the purpose of verifying the accuracy of information in a data user return submitted under section 14.

- (2) The persons are -
- (a) the data user; and
  - (b) any other person whom the Commissioner has reasonable grounds to believe may be able to assist in verifying any information in the data user return.
- (3) A person on whom a notice is served under subsection (1) may refuse to provide any document, record, information or thing, or any response to any question, specified in the notice, if the person is permitted, entitled or obliged under this or any other Ordinance, any legal or regulatory requirement or any direction or order of any regulatory authority or court to which that person is subject to do so.
- (4) If, having regard to any document, record, information or thing, or any response to any question, provided under subsection (1), the Commissioner reasonably considers that any information in a data user return is inaccurate, the Commissioner may, by written notice, require the data user to correct the information in the data user return.
- (5) Subject to subsection (3), a person on whom a notice is served under subsection (1) or (4) must comply with the requirement within the period reasonably specified in the notice.
- (6) A person who, in purported compliance with a notice under subsection (1), knowingly or recklessly provides any document, record, information or thing, or any response to any question, 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."

***New Section 20(3)(ea) - Circumstances where a data user may refuse to comply with a data access request***

**Response:**

We propose to revise new Section 20(3)(ea) as marked below:

"(ea) the data user is permitted, entitled or obliged under this or any other Ordinance, any legal or regulatory requirement or any direction or order of any regulatory authority or court to which the data user is subject not to disclose the personal data which is the subject of the request; or".

***New Section 20(5) - Specified body to determine whether a data user shall or may refuse to comply with a data access request***

Response:

Please revise new Section 20(5)(a) as marked in the following: "..... whether a data user is permitted, required or entitled to refuse to comply with a data access request .....".

***New Section 32(5) - Offence for breaching any condition subject to which the Privacy Commissioner consents to a matching procedure request***

Response:

We note that this point is new and was not covered in the consultation. The proposed new Section 32(5) should be considered carefully as it provides that a data user commits an offence if it contravenes any condition subject to which the Privacy Commissioner consents to its matching procedure request.

The usual consequence for breaching a condition subject to which a consent or approval is given is the suspension or revocation of the relevant consent or approval. That may, in turn, result in the commission of an offence if the person to whom the consent or approval was given continued to act without valid consent or approval.

In our view, it is appropriate to adopt the usual consequence in this case and we would suggest revising Section 32(5) as marked below:

"(5) The Commissioner may suspend or revoke any consent given in a notice under subsection (1)(b)(i) if aA requestor who carries out a matching procedure in contravention of any conditions specified in that notice under subsection (1)(b)(i) commits an offence and is liable on conviction to a fine at level 3."

Even if our suggestion is not accepted, the new Section 32(5) should be revised for the sake of clarity as marked below:

"(5) A requestor who carries out a matching procedure in contravention of ~~contravenes~~ any conditions specified in a notice under subsection (1)(b)(i) commits an offence and is liable on conviction to a fine at level 3."

***New Sections 35B to 35F - Sale of personal data***

Response:

We propose the changes marked below for clarity and practicability:

1. Section 35B(3)  
"(3) The data user must take all practicable steps to provide the data subject with .....";
2. Section 35B(3)(b)  
"(b) a response facility through which the data subject may ..... objects to the intended sale.";
3. Section 35B(5)  
"(5) The information and response facility provided under subsection (3) must be presented in a manner that is easily readable and easily understandable by the standards of a reasonable, average person.";
4. Section 35B(7)  
"(7) In any proceedings for an offence under subsection (6), it is a defence for the data user charged to prove that the data user took all practicable steps reasonable precautions and exercised all due diligence to avoid the commission of the offence.";
5. Section 35C(3)  
"(3) A data subject may indicate whether the data subject objects to a sale of personal data through the response facility or other means as the data user may reasonably specify.";
6. Section 35D(1)  
"(1) ..... the data subject may subsequently object to such sale by sending a written notification to the data user through the response facility or other means as the data user may reasonably specify.";
7. Section 35D(3)  
"(3) A data user must, without charge to a data subject, comply with the requirement specified in a notification from the data subject under subsection (1). For the avoidance of doubt, a data user is deemed to have complied with this subsection (3) if the data user does more than the data subject specified in the notification."; and
8. Sections 35C(5) and 35D(7)  
The wording describing the defence in the above sections should be revised in the same manner as set out in paragraph 4 above.

We would also take this opportunity to re-iterate our strong support for an opt-out approach over an opt-in approach having regard to the major shortcomings of an opt-in approach as set out below:

- (i) data subjects must actively engage in an opt-in approach. This approach may

not work for data subjects who prefer a hassle-free approach. Other data subjects may fail to respond for other reasons including that they may not understand the opt-in approach and confirmation process;

- (ii) an opt-in approach which provides for data subjects to opt-in on a case-by-case basis or a complicated opt-in approach does not serve the interest of data subjects. If the model is not user-friendly, data subjects may not react to it and there is a further risk of desensitising data subjects if they are bombarded with opt-in requests thereby rendering the initiative ineffective;
- (iii) requiring data subjects to opt-in on a case-by-case basis will be overly burdensome on data users and impossible to administer and upkeep in practice; and
- (iv) the brunt of the opt-in requirement will be borne by data users especially if the requirement applies with retrospective effect to personal data already collected from data subjects. This will create an unbearable burden on costs and resources on data users.

Further, giving data subjects the right to opt-out any time should afford sufficient and appropriate protection to data subject.

***New Sections 35G to 35Q - Use of personal data in direct marketing***

Response:

We propose to make corresponding changes to Sections 35H, 35J, 35K, 35L(4), 35N, 35O and 35P as set out above in relation to Sections 35B to 35F.

We repeat our views above regarding the opt-out approach. We would also like to add that in the case of HKAB member banks, in conducting direct marketing for the first time, they will remind customers of their rights to opt-out and provide convenient channels (such as visiting branches, by e-mail or phone) for the customers to perform the opt-out request.

***New Section 35R - Disclosure of personal data obtained without consent***

Response:

We propose to revise new Section 35R(4)(b) as marked below:

- "(b) the disclosure was permitted, required or authorized by or under any enactment, by any rule of law or by any legal or regulatory requirement or any direction or an order of a regulatory authority or court to which the person is subject;"

***New Section 50B - Offences relating to failure to comply with requirements of Privacy Commissioner, etc.***

Response:

We propose to revise new Section 50B as marked below:

"(1) A person commits an offence if the person-

- (a) without lawful authority or reasonable excuse, obstructs, hinders or resists the Commissioner .....
- (b) without lawful authority or reasonable excuse, fails to comply with any lawful requirement of the Commissioner ....., or
- (c) in the course of the performance or exercise by the Commissioner .....
  - (i) makes to the Commissioner ..... a statement which the person knows to be false or does not believe to be true; or
  - (ii) otherwise knowingly misleads the Commissioner or that other person in a material particular".

***New Section 58(6) - Crime, etc.***

Response:

We are concerned that the new definition of "crime" in Section 58(6) significantly limits the scope of the exemption under Section 58. The current wording of paragraph (b) of the definition renders it applicable to law enforcement agencies only (and not data users in general). That would significantly reduce the ability of a data user such as an international financial institution in implementing global anti-money laundering and anti-terrorist financing measures. Such approach is inconsistent with the recommendation of the Financial Action Task Force (the "FATF") (please see paragraphs 14 to 16 of its Consultation Paper on "The Review of the Standards - Preparation for the 4th Round of Mutual Evaluation" published in June 2011, copy attached for ease of reference).

The Review of  
Standards - Preparatio

Having regard to the FATF recommendation, we are of the view the new definition is not necessary. If it is decided to introduce that definition, we propose to revise it as marked below:

"crime means an offence under the laws of Hong Kong or any other jurisdiction;".

- ~~— (a) —~~ an offence under the laws of Hong Kong; or
- ~~— (b) —~~ if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place;"

#### ***New Section 63B - Due diligence exercise***

##### Response:

We propose to revise the new Section 63B(4) for clarity and practicability as marked below:

- "(4) If a data user transfers or discloses personal data to a person for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction described in subsection (1), the person -
- (a) must only use the data for that purpose; and
  - (b) must, as soon as practicable after the completion of the due diligence exercise and provided that the data is no longer necessary for the purpose of the business transaction -
    - (i) return the ~~personal~~ data to the data user without keeping any record of the data; or and
    - (ii) destroy any record of the ~~personal~~ data that is kept by the person."

#### ***Section 64 - repealing existing Section 64 on offences***

##### Response:

We propose to revise Section 64(2) for clarity as marked below:

- "(2) Subsection (1) does not apply in relation to -
- (a) a contravention that does not constitute an offence including a contravention of a data protection principle or a contravention of any requirement under section 35B(1), 35H(1) or 35N(1); or
  - (b) a contravention that constitutes an offence under .....; ~~or~~
  - ~~(c) — a contravention of any requirement under section 35B(1), 35H(1) or 35N(1)."~~



***New DPP2(3) and DPP4(2) in Schedule 1 - Data user's duty to monitor its data processors***

Response:

We propose to revise the new DPP2(3) for clarity and practicability as marked below:

"[DPP2(3)] Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt such contractual or other means as are practicable to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data."

***New DPP3(2) and DPP3(3) in Schedule 1 - Relevant person giving prescribed consent to use personal data for a new purpose on behalf of minor, mentally incapacitated person, etc.***

Response:

As regards the data subjects in question, the relevant person in relation to the data subject in a particular case will be best placed to decide whether to give prescribed consent on behalf of the data subject having regard to the relevant circumstances including whether the use of data for a new purpose is clearly in the interest of the data subject. It remains our view that it is reasonable and appropriate to allow a data user to follow the judgment of the relevant person given that the data user is unlikely to be in a position in practice to form a view on this point.

In view of the above, the new DPP3(3) is unduly onerous on a data user. We propose the changes as marked below to make it more practicable for a data user to comply:

"(3) A data user ~~may~~must not use the personal data of a data subject for a new purpose ~~even~~ if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly not in the interest of the data subject."

***Amendments to DPP4 in Schedule 1 - prevention of loss of personal data***

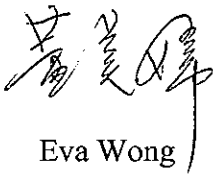
Response:

As regards loss of data or any device holding the data, it remains our view that the critical question is whether the "loss" results in unauthorized access or use of data causing damage to the data subjects. Accordingly, we propose to revise DPP4(1) and new DPP4(2) as marked below:

- "(1) All practicable steps shall be taken to ensure that personal data ..... held by a data user is protected against unauthorized or accidental access, processing, erasure, ~~loss~~ or use, or loss actually resulting in unauthorized or accidental access, processing, erasure or use of data having particular regard to .....".
- (2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt such contractual or other means as are practicable to prevent unauthorized or accidental access, processing, erasure, ~~loss~~ or use of the data transferred to the data processor for processing, or loss of the data actually resulting in unauthorized or accidental access, processing, erasure or use of the data.".

If you have any further questions, please contact our Manager Ms. Ivy Wong at 2521 1169.

Yours faithfully



Eva Wong  
Secretary

Enc.