PCPD's Submissions in response to the

Public Consultation on Automatic Exchange of Financial Account Information in Tax Matters in Hong Kong

This submission is made by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") in response to the Public Consultation carried out by the Financial Services and Treasury Bureau ("**FSTB**") on Automatic Exchange of Financial Account Information in Tax Matters ("**AEOI**") in Hong Kong in April 2015 ("**Consultation Paper**"). The Administration proposed to introduce into Hong Kong by local legislation the AEOI standard promulgated by the Organisation for Economic Cooperation and Development ("**OECD**"). Public views are sought on seven questions concerning the proposed legislative framework. As the regulator to protect individuals' privacy in relation to personal data under the Personal Data (Privacy) Ordinance, Cap. 486 ("**PDPO**"), the PCPD would like to raise concerns on the proposal from the perspective of personal data privacy protection.

Overall comments

2. It is noted that the proposed AEOI framework will be operated in two tiers. First, the financial institutions (as defined in the Consultation Paper) ("**FIs**") will be made subject to statutory requirements to collect account information from their customers who are non-Hong Kong tax residents, identify reportable accounts and report such information to the Inland Revenue Department ("**IRD**"). Secondly, the IRD will be empowered by the proposed legislation to provide the information to overseas tax authorities on an ***automatic*** (*i.e.* annual) basis for tax purposes.

3. Currently, Hong Kong has only opted for the arrangement for exchange of information on a bilateral basis upon request by overseas tax authorities based

on suspicion of tax evasion as opposed to an automatic exchange. The shift to a regime of automatic exchange is a draconian move but the Consultation Paper has not indicated that the existing regime is deficient. It is therefore incumbent upon the Administration to explain how the public interest of annual exchange of the financial account information overrides the privacy interest of the overseas tax residents concerned. The need to comply with an international obligation as indicated in the Consultation Paper is relevant but the underlying reasons for the international community to enhance the global information exchange is not readily apparent. Further, we need to bear in mind that one of the cardinal principles in the exchange of information is that the information exchanged should be foreseeably relevant (*i.e.* there will be no fishing expeditions[1]).

Specific comments on the Consultation Paper

(a) Reporting Requirements

The Proposal involves personal data as defined under the PDPO

4. Generally, FIs collect and hold vast amount of information of their customers in the course of their business in providing banking and financial services. Paragraph 2.19 of the Consultation Paper sets out the scope of reportable account information which includes the name, address, jurisdiction(s) of residence, Tax Identification Number ("**TIN**"), date of birth of each reportable person, the account number, the account balance or value, and other relevant financial information of the account, etc. All these data satisfies the definition of "*personal data*"[2] and hence is protected under the PDPO. It is therefore necessary to ensure that the future legislative framework for the purpose of the AEOI shall be consistent with the legal requirements under the PDPO.

[1] Paragraphs 2.28 and 2.34 of the Consultation Paper.

[2] Under section 2(1) of the PDPO, "*personal data"* means any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

Function and activity of FIs and the IRD

5. As provided under Data Protection Principle ("**DPP**") 1(1)(a) in Schedule 1 of the PDPO, personal data shall be collected for a lawful purpose directly related to a function or activity of the data user. Unless authorised by law, there may be doubt as to whether the IRD and FIs should collect all of the reportable account information for their own functions or activities. However, we note that the Administration will enact legislation to specify the procedures for FIs to identify reportable accounts held by non-Hong Kong tax residents account holders, and to collect and disclose the required reportable account information to the IRD. Likewise, the future legislative framework will explicitly empower the IRD to collect and disclose information for the purpose of AEOI. The legal basis for IRD and FIs' participation in AEOI is thus secured.

Only adequate but not excessive personal data shall be collected

6. Furthermore, DPP1(1)(b) and (c) of the PDPO requires that data user shall only collect personal data which is necessary for a lawful purpose directly related to its function or activity, and the personal data so collected shall be adequate but not excessive for such purpose. Hence, the IRD shall only collect and the FIs shall only be required to provide adequate but not excessive account information necessary for AEOI purpose.

7. We note that the scope of reportable account information as proposed in the Consultation Paper tallies with that as provided under the Common Reporting Standard of the OECD ("**CRS**")[3]. Also, the scope of the FIs to be covered in the proposed legislation[4] is the same as that provided in the CRS[5]. As the

[3] See paragraph 2 of section 2 of the model Competent Authority Agreement provided by the OECD (Annex A of the Consultation Paper).
[4] See pparagraph 2.12 of the Consultation Paper.
[5] As provided in Section VIII under "*A. Reporting Financial Institution*" of the Common Reporting Standard (Annex B of the Consultation Paper). However, the PCPD is not in the capacity to give specific comments on the definitions and the scope of FIs.

scope of information required to be reported by the proposed category of FIs is premised on compliance with the international standard for AEOI purpose, we see no objection.

Disclosure of reportable account information

8. In addition, DPP 3 of the PDPO requires that personal data shall not be used for a new purpose[6] unless the data subject's prescribed consent[7] has been obtained or an exemption provision under Part 8 of the PDPO applies. As disclosure of reportable account information of non-Hong Kong tax resident for AEOI arrangement serves the ultimate purpose of the assessment or collection of overseas tax, it is unlikely that such disclosure would be considered as directly related to the original purpose of collecting the same by the FIs in their dealings with customers. In such circumstances, prescribed consent of the customers must be obtained for the subsequent disclosure of information to the IRD for the purpose of AEOI. Alternatively, if the reporting obligation by FIs is to be prescribed by legislation as proposed, the Administration has to take into account how the exemption provisions under section 58(2) (for the purpose under section 58(1)(c)[8]) and section 60B(a)[9] of the PDPO may be invoked. Specifically, in proposing the amendment bill to the Inland Revenue Ordinance, Cap.112 ("**IRO**"), the Administration should explain how the *prejudice* requirement under section 58(2) of the PDPO will be satisfied under the proposed AEOI regime.

---

[6] A new purpose means any purpose other than (a) the purpose for which the data was to be used at the time of collection of the data; or (b) a purpose directly related to the purpose referred to (a).

[7] *"Prescribed consent"* means express consent of the person given voluntarily but not withdrawn by notice in writing (section 2(3) of the PDPO).

[8] Under section 58(2) of the PDPO, personal data is exempted from DPP3 if the data is used for a purpose referred to in section 58(1) (which includes the assessment or collection of any tax or duty) and non-disclosure of the data *would be likely to prejudice* such purpose. The meaning of *"tax"* is further defined under section 58(1A).

[9] Under section 60B(a) of the PDPO, personal data is exempted from DPP3 if the disclosure is "*required or authorised by or under any enactment, ... in Hong Kong.*"

(b) Requirements for FIs to identify and keep information of accounts concerning reportable jurisdictions

9. Paragraph 2.20 of the Consultation Paper stated that the FIs will perform the due diligence procedures (to be set out in a Schedule to the IRO) during which the FIs may choose to identify and keep relevant information from *all* their non-Hong Kong tax resident-account holders (including those with residence not falling within IRD's specific reportable jurisdictions at the material time). We note that the Administration would have an open mind (but subject to compliance with privacy regime in Hong Kong) if FIs opt to identify and keep information of *all* non-Hong Kong tax-resident account holders, over and above the proposed legal requirements for specific reportable jurisdictions[10].

10. As far as collection of personal data is concerned, the FIs should be mindful that the purpose of collecting personal data for the discharge of their reporting obligation concerning the individuals with residence falling under the reportable jurisdictions may be different from the purpose of collecting personal data to fulfil their due diligence obligation to identify reporting accounts. To serve these two separate purposes, the types of personal data to be collected are different. There is a risk of excessive collection of personal data if the FIs do not differentiate between these two purposes and, for expediency sake, collect *all* types of data from customers in one go as if their residence all falls within the reportable jurisdictions.

11. As regards retention of personal data, all reasonably practicable steps shall be taken by data users to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used (section 26(1) and DPP2(2) of the PDPO refer). Prima facie, FIs' keeping of personal data of *all* non-Hong Kong

[10] See paragraph 2.21 of the Consultation Paper.

tax-resident account holders, collected in fulfilment of their due diligence obligation, for a period which makes no distinction between reportable and non-reportable accounts will be inconsistent with the requirements under section 26(1) and DPP2(2) of the PDPO. This is however, subject to other applicable retention requirements, such as the due diligence requirements under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap.615.

12. Further, with regard to the retention of reportable account information of the reportable jurisdiction, it is advisable for the future legislation to specify the retention period for the purpose of satisfying the reporting obligation.

13. On a separate matter, FIs are required to take all reasonably practicable steps to ensure that their customers are explicitly or implicitly informed on or before collection of their personal data the purpose of use of the data and the classes of transferee(s) of the data (under DPP1(3) of the PDPO). FIs should as part of the AEOI implementation review and (as necessary) amend their Personal Information Collection Statement to ensure that customers are duly informed of the purpose of use of the personal data for the AEOI arrangement and the classes of transferees.

14. In particular, paragraph 2.19(a) of the Consultation Paper further stated that for the pre-existing accounts (i.e. accounts created before the commencement of the proposed legislation), FIs are not required at present to report TINs or dates of birth provided that such information is not in the possession of FIs and there is not otherwise a requirement for such information to be collected under domestic legislation. However, after the AEOI arrangement comes into play, the FIs are required to use "*reasonable efforts*" to obtain the TINs or dates of birth in respect of the pre-existing account holders by the end of the second calendar year after such accounts were identified as reportable

accounts. Although there will be domestic legislation put in place to legitimise the automatic exchange of information in future, we would advise that FIs should, as a matter of good corporate governance, duly inform their pre-existing account holders in advance about such arrangement.

(c) Information Technology System

Security of the reportable account information

15. We note that a secure platform (i.e. AEOI Portal) will be provided by the IRD for the FIs to submit notifications and file AEOI returns electronically. Digital certification issued by the Hong Kong Post Certification Authority will be adopted for online authentication and transaction[11]. Further, paragraph 3.10 of the Consultation Paper outlined the various steps which will be taken by the IRD to protect the confidentiality of all data received (such as encryption, audit trail and system log). In view of the inherently sensitive nature of the information to be submitted via the AEOI Portal, the Administration is reminded of the importance to take all reasonably practicable steps for ensuring the security of the personal data uploaded, transmitted and stored in the AEOI Portal in accordance with DPP 4 of the PDPO.

16. Further, we note that security risks assessments will be conducted by the IRD regularly[12]. It is important to conduct the assessments on the control, security and access measures on all data received via the AEOI Portal. Besides, given the vast amount of sensitive information that will be submitted via the AEOI Portal, we would stress that Privacy Impact Assessments[13] should be carried out on the AEOI data flow and its entire lifecycle. These privacy impact

[11] Paragraph 3.6 of the Consultation Paper.
[12] Paragraph 3.10 of the Consultation Paper.
[13] See the Information Leaflet on "*Privacy Impact Assessment*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/files/PIAleaflet_e.pdf)

and security risks assessments should be conducted prior to the initial development of the system for AEOI as well as regularly during their operations; and be equally applied to any self-developed systems by FIs. In this connection, we would like to emphasis the following aspects (not meant to be exhaustive):-

(i) multiple technical measures should be adopted to ensure that only authorised personnel of the FIs and IRD shall be given access to the AEOI Portal on a *need-to-know* basis and the transmission is secured;

(ii) the security measures should cover the full data cycle (both local and international data flow);

(iii) the security measures must be developed for central (IRD) system and distributed (FIs) system;

(iv) both the IRD and FIs must put in place and implement effectively clear and robust policies to safeguard the personal data; and

(v) both the IRD and FIs should undertake periodic audit including Privacy Compliance Assessment on their respective internal compliance with the privacy policies and practices.

(d) Other related comments

(i) Riding on the bilateral CDTA and TIEA signed under section 49(1A) of IRO as the legal basis for implementing AEOI and providing data privacy and confidentiality safeguards

17. It is noted that AEOI will be implemented under the existing framework consisting of the Comprehensive Avoidance of Double Taxation Agreements

("**CDTA**") and Tax Information Exchange Agreement ("**TIEA**") on a bilateral basis which are already made plausible by virtue of sections 49(1A) and 49(1B) of the IRO[14]. The PCPD would raise concerns in the ensuing paragraphs as to the actual safeguards offered to personal data privacy.

Inland Revenue (Disclosure of Information) Rules

18. For the AEOI arrangement, it is noted that the IRD will not adopt the existing approach to *notify the individual in writing* about the disclosure to overseas tax authorities as provided under section 5(1) of the Inland Revenue (Disclosure of Information) Rules (Cap.112BI)[15]. In that case, the relevant individual will no longer be entitled to invoke the current mechanism of request for amendment of the information (as provided under sections 5 to 7 of the said Rules).

19. On the face of it, it may be argued that the reportable account information is factual in nature and hence the existing notification requirement is not necessary. However, we are of the view that the *accuracy* of the information (e.g. the jurisdiction of residence) and account holder's right of *correction* must be addressed. The data users' obligation to ensure data accuracy and the data subjects' right of correction are cornerstones of data protection and they are explicitly outlined in DPP 2(1), DPP 6 and sections 22 to 25 of the PDPO. Inaccurate information can lead to serious consequence to the account holders. The explanations that the AEOI shall operate under a different mode and the IRD may experience administrative difficulties in following the said Rules are not sufficient justifications to deny account holders of their rights.

[14] Paragraphs 2.27 to 2.35 of the Consultation Paper.
[15] Paragraph 2.32 of the Consultation Paper.

Actual safeguards provided under CAA and privacy protection in overseas jurisdiction

20. On the other hand, we note that a new Competent Authority Agreement ("**CAA**") will be signed with the bilateral partners who have in place appropriate laws and rules to safeguard data privacy and confidentiality. Given the safeguards provided in paragraphs 2.28 and 2.29 of the Consultation Paper merely reiterates the provisions under the CDTA/ TIEA in *broad* terms (*e.g.* to ensure the "*necessary*" level of protection of personal data[16]), we would remind that it is incumbent upon the IRD to ensure the bilateral partners shall have in force laws and systems that offer adequate protection to personal data privacy and, in particular, to the transferred reportable account information. The IRD should have an on-going monitoring system to verify that actual safeguards are implemented by its overseas partners to give the fullest protection to the personal data transferred under the AEOI arrangement.

Transfer of personal data overseas

21. As it is a pre-condition that the bilateral partners will have in place appropriate laws and rules to safeguard data privacy and confidentiality, we would remind that the Administration should make reference to the level of protection under the PDPO in assessing whether the pre-condition is satisfied. Section 33 (not yet operative) of the PDPO is relevant as it prohibits the transfer of personal data outside Hong Kong unless one of the specific exceptions provided under section 33(2) applies.

22. Section 33(2)(a) of the PDPO provides for the personal data to be transferred to jurisdictions on the PCPD's White List (*i.e.* those jurisdictions which have in force "*any law which is substantially similar to, or serves the same*

[16] See article 5 "Confidentiality and Data Safeguards" of the model Competent Authority Agreement provided by the OECD (Annex A of the Consultation Paper).

purpose as" the PDPO). The PCPD is empowered under section 33(3) to publish by way of Gazette the said White List[17]. As explained in the "*Guidance on Personal Data Protection in Cross-border Data Transfer*" issued by the PCPD[18], in assessing a jurisdiction's data protection regime for the purpose of inclusion in the White List, the PCPD considers that generally a proper assessment should cover various aspects including the scope of application of the data privacy regime, the existence of equivalent provisions of the DPPs under the PDPO, the data subject's rights and redress, the level of compliance and the data transfer restrictions[19]. The Administration may make reference to the methodology adopted by the PCPD in compiling the White List.

23. In addition, cross-border data transfer will be permissible under section 33(2)(e) if any of the exemptions from DPP3 (governing "*use*" which meaning shall include "*transfer*" or "*disclosure*") under Part 8 of the PDPO is applicable. For instance, the exemptions of section 58(1)(c) (for assessment or collection of tax) and/or section 60B(a) ("*if required or authorised by or under any enactment*")) mentioned above may be relevant if the AEOI arrangement will be put into effect by way of legislation.

(ii) Use of the exchanged information for non-tax related purposes

24. To facilitate the bilateral exchange of tax-related information with the competent overseas authorities upon request, section 58(1A) was introduced to the PDPO in 2010 to expand the definition of "tax" to cover the tax of an

---

[17] The PCPD had completed a survey of 50 jurisdictions in 2013 and came up with a White List of places, which has in force data protection law which is substantially similar to, or serves the same purposes as the Ordinance. A copy of the said white list report (which is now kept confidential) has been forwarded to the Government for information.

[18] See the "*Guidance on Personal Data Protection in Cross-border Data Transfer*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf).

[19] See paragraph 6 at page 4 of the *Guidance on Personal Data Protection in Cross-border Data Transfer*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf).

overseas territory which the Administration has already made an arrangement under section 49(1A) of the IRO. It is important to note that under section 58(2) of the PDPO, the exemption will be applicable only if the non-disclosure *would be likely to prejudice* the assessment or collection of tax as provided under section 58(1)(c).

25. It is however stated in paragraph 2.28(f) of the Consultation Paper that the information originally exchanged for tax purpose may be subsequently used for other purposes[20] provided that such use is allowed under the laws of both contracting parties and the competent authority of the supplying party authorises such use. In this regard, the PCPD reiterates its previous concern expressed for the CDTA/ TIEA framework in respect of exchange of information for investigation and detection of overseas crime[21]. In that case, it must be noted that the exemption under section 58(1)(a) of the PDPO is subject to the restriction imposed on overseas crimes under the conditions as stated in section 58(6) of the PDPO[22].

26. We would also reiterate the prior submissions to the Bills Committee on Inland Revenue (Amendment) Bill 2013 on 6 June 2013[23]. The concern remains that the terms *"other purposes"* or *"non-tax related purposes"* are too vague. In this regard, the Administration has explained in its paper to the Bills Committee that the scope of *"non-tax related purposes"* is limited and that "*for clarity sake, [the Administration] will specify the limited non-tax related*

---

[20] According to paragraph 2.28(f) of the Consultation Paper, the sharing of the information exchanged is meant for "higher priority matters" such as to combat money laundering, corruption and terrorism financing.

[21] See LC Paper No. CB(1)1260/12-13(01).

[22] *"Crime"* is defined under section 58(6) of the PDPO to mean: "*(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*." Hence, in so far as overseas offence is concerned, the transfer or disclosure of personal data is permissible under the PDPO only if it is in connection with legal or law enforcement cooperation between Hong Kong and that overseas jurisdiction.

[23] See LC Paper No. CB(1)1260/12-13(01).

purposes in the texts of future CDTA (including their protocols), which will then be enacted as subsidiary legislation domestically"[24]. At this juncture, the Administration should explain the steps taken so far to restrict the scope of application of the *"non-tax related purpose"* to ease our concern.

(iii) Embrace personal data privacy protection

27. To manage privacy and data protection responsibly and to demonstrate the data users' commitment to good corporate governance, it is recommended that the IRD and FIs adopt a proactive strategy by formulating and implementing a comprehensive privacy management programme ("**PMP**") for AEOI. Many organisations including the Government and insurance industry have pledged support to implementing PMP on a voluntary basis.

28. PMP serves as a strategic framework to assist an organisation in building a robust privacy infrastructure supported by on-going review and monitoring process to facilitate compliance with the requirements under the PDPO. It involves top management commitment and ensures that privacy is built by design into all initiatives, programmes and services. For more information, please refer to the "*Privacy Management Programme: A Best Practice Guide*" issued by the PCPD[25].

The Office of the Privacy Commissioner for Personal Data

30 June 2015

[24] Paragraph 22 of LC Paper No. CB(1)1285/12-13(02).

[25] See the "*Privacy Management Programme: A Best Practice Guide*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/files/PMP_guide_e.pdf).