PCPD's Submissions

on

Proposed New Legislation on the Customer Due Diligence and Record-Keeping Requirements for Financial Institutions and the Regulation of Remittance Agents and Money Changers – Detailed Proposals

The Consultation Document released on 7 December 2009 sets out the detailed legislative proposals on the customer due diligence and record-keeping requirements for financial institutions and the regulation of remittance agents and money changers. The aim is to enhance the anti-money laundering regulatory regime in respect of the financial sectors.

2. In discharge of its function under section 8(1)(d) of the Personal Data (Privacy) Ordinance ("the Ordinance"), the Privacy Commissioner for Personal Data (PCPD) has to examine any proposed legislation that may affect the personal data privacy of individuals, and to inform the authority proposing the legislation matters that may attract personal data privacy concerns. The ensuing comments are provided by the PCPD from the perspective of a privacy regulator.

Collection of Personal Data

3. It is noted that the identities of customers and beneficial owners of corporate customers will have to be ascertained and verified under various proposals as set out in Annex A of the Consultation Document. Identification documents and information relating to individuals will be collected in carrying out customer due diligence ("CDD") under proposal 4 (verify identity of customer before establishing business relationship), proposal 5 (CDD measures to be carried out), proposal 6 (on-going due diligence), proposal 8 (simplified due diligence), proposal 9 (enhanced due diligence), proposal 10 (third party to conduct CDD), proposal 13 (verification on originator for wire-transfer equals to or above $8,000) and proposal 14 (verification on customer for wire-transfer equals to or above $8,000).

4. With regard to the collection of personal data, Data Protection Principle ("DPP") 1 in the Schedule 1 to the Ordinance sets out the legal

requirement to be observed by data user, i.e. any person who controls the collection, holding, processing or use of personal data.

5. DPP1(1) provides in essence that personal data should only be collected for a lawful purpose directly related to the function or activity of the data user and that the personal data collected should be necessary, adequate but not excessive in relation to that purpose. In the verification processes as set out in the aforesaid proposals, it is noted that only proposals 13 and 14 list out specifically the kind of personal data to be collected from individuals, including identity card number (or certificate of identity, document of identity or travel document number with place of issue), telephone number, address and place of birth. Specific attention should be given to clearly define and delimit, as far as practicable, the kind of personal data to be collected. The financial institutions ("FIs") and the relevant authorities (as defined in the proposed legislation) collecting the data should be mindful of the requirements under DPP1(1).

6. DPP1(3) provides that on or before collection of personal data directly from the data subject, the data user should inform the data subject of the purpose for which the data are to be used, the classes of persons to whom the data may be transferred, whether it is obligatory or voluntary for him to supply the data, and, where it is obligatory for the individual to supply the data, the consequences for him if he fails to supply the data. Furthermore, on or before the first use of the data for the purpose for which the personal data were collected, the data subject should be explicitly informed of his rights to request access to and correction of personal data, and the name and address of person to whom any such request may be made. In order to comply with the requirements, FIs should take all reasonably practicable steps to notify individuals of the prescribed information under DPP1(3).

7. The PCPD has recently handled a complaint against the collection of identification document for CDD when opening an account with certain bank. The major cause of the complaint was that the bank had failed to explain to the customer the collection was based on the Supplement to the Guideline on Prevention of Money Laundering issued by the Hong Kong Monetary Authority. The lesson leant from this complaint is that the FIs should ensure customers will be explicitly informed of the basis and purpose of collection of identification documents.

Proposal 4(a) and (b)

8. Proposal 4(a) and (b) in Annex A specifies two exceptional situations where an FI may verify a customer's identity after establishing a business relationship.

9. Following the Financial Action Task Force ("FSTK") 40 Recommendations ("40 Recommendations"), the conduct of the CDD measures should operate on a risk-sensitive or risk-based approach depending on the type of customers, business relationship or transactions and associate risks.

10. Proposal 4(a) provides for a situation where the CDD verification process *may* be completed after establishment of a business relationship when there is *"little risk of money laundering or terrorist financing"*. While the word "may" gives flexibility to the time of making the verification, regard should be given, in view of the risk-based approach, whether it is indeed necessary to conduct the verification process where *"little risk"* is involved.

11. Likewise, the word "may" in Proposal 4(b) should be reviewed in light of the risk-based approach. Both the 40 Recommendations and the Guidance Paper on Anti-money Laundering and Combating the Financing of Terrorism issued by the International Association of Insurance Supervisors in October 2004 do not mandate the general collection of identification documents of beneficial owners when the relationships are entered into with life insurance customers. Given the beneficiary named under a life insurance policy may be changed at any time before the death of the insured, there is no risk of money-laundering before any money is paid out to the latest beneficiary. By using the word "may" in Proposal 4(b), an FI is not restricted to collect identification documents of beneficial owners at an early stage when there is no risk of money laundering or financing terrorist activities. Consideration should be given by the Administration to revise Proposal 4(b) accordingly.

Proposal 5(b)

12. It is proposed that the CDD measures to be carried out will include identifying and verifying the identity of the *"beneficial owner"*. According to the definition of "*beneficial owner*" in the List of Proposed Definition (at page 17 of the Consultation Document), it includes a person *"who owns or controls, directly or indirectly, including through trusts or bearer share holdings for any legal entity 10% or more of the shares or voting rights of the entity or*

otherwise exercise control over the management of the entity".

13. It is noted that recommendation 4(c) of the 40 Recommendations requires *"identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement".* There is no specific percentage imposed for determining the *"controlling interest".*

14. While PCPD acknowledges the benefit of clarity in specifying a percentage, justification is required for the proposed legislation to prescribe the proposed threshold of 10%. Especially, many shareholders with 10% voting rights will be subject to CDD even though they may not hold enough shares to constitute a majority shareholding or exercise control over the management of the entity.

Proposals 5 and 9(c)

15. This proposal will require FIs to put in place a system to determine whether a customer is a politically exposed person ("PEP") which is defined in the List of Proposed Definition (at page 18 of the Consultation Document) as a person *"who is an individual who is or has been entrusted with a prominent public functions in a place outside the PRC".* There will also be special CDD requirements for the PEP. In the absence of further information in the Consultation Document, there does not appear to be any absolute linkage between a PEP and the risk for money laundering or financing terrorist activities. The Administration has to give further justification for the proposal.

Proposal 7

16. It is stated that on-going due diligence must be conducted upon the occurrence of certain triggering events for existing business relationship entered into before the commencement of the proposed legislation. The proposal then goes on to state that notwithstanding the non-occurrence of the triggering events, the FIs are required to conduct CDD to all existing accounts within 2 years upon the commencement of the proposed legislation. The proposal seems to depart from the risk-based approach when CDD will be applied to the existing accounts no matter whether there is any triggering event happened.

17. The triggering events mentioned in Proposal 7 include *"substantial*

changes to customer documentation standards" and *"FI becomes aware that it lacks sufficient information about an existing customer"*. It is advisable for Administration to be specific about the meanings of "*customer documentation standards"* and *"sufficient information"*.

Proposal 8

18. This proposal specifies certain situations where an FI may choose to conduct *simplified due diligence*. The use of the word "may" gives flexibility to an FI to choose to carry out either CCD or *simplified due diligence*. The PCPD considers that CDD should only be conducted when there is sufficient justification to do so. Hence, where the situation justifies the carrying out of a *simplified due diligence,* no CCD should be conducted.

Proposals 13 and 14

19. Different personal data will be collected under proposals 13 and 14 respectively for transfer of money outside Hong Kong for a sum equals to or above $8,000 by means of wire transfer and remittance other than wire transfer. It should be noted that the personal data collected under the circumstances should be necessary, adequate but not excessive taking into account of the different nature of the transactions and the risk involved.

Proposal 13(c)

20. The FIs are required to collect the originator's address or, in the absence of address, the identity card number or "date and place of birth" when undertaking wire transfers equal to or above $8,000. It is difficult to understand how "date and place of birth" could serve as an alternative to address data. The Administration has to ensure that the alternative information should be necessary for the original collection purpose and are proper replacement of address data.

Use of Personal Data

21. DPP3 stipulates that personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than the purpose for which the data were to be used at the time of collection or for a directly related purpose. The term "use" is defined under section 2(1) of the Ordinance to include the *transfer* or *disclosure* of personal data.

Proposal 10

22. Pursuant to this proposal, FIs will be permitted to rely on a third party (such as lawyer, auditor, etc.) to conduct the CDD. It must be borne in mind that where personal data (including identification or such documents from which the identity of an individual can be ascertained) are transferred to the FIs, the requirement of DPP3 should be observed. To give legislative basis for the transfer or disclosure of personal data to the FIs by such third party, the proposed legislation should specify *the purpose(s) for, the circumstances and conditions* under which the personal data of an individual who is subject to the CDD would be transferred to the FIs. In the event the transfer (or disclosure) is not expressly provided for under the proposed legislation, the transferor is required to ensure that the purpose of transfer (or disclosure) is the same as or directly related to the collection purpose, otherwise the data subject's prescribed consent to the transfer (or disclosure) must be obtained.

Proposals 20 and 21

23. The proposal will empower the "relevant authority" to *"inspect and make copies or record details of records"* from the FIs and to require any person to *"produce any record or document relevant to the investigation"*. In such circumstances, where personal data will be collected by or disclosed to the "relevant authority", the requirements under DPP1(1), DPP1(3) and DPP3 should be observed.

Security of Personal Data

24. DPP4 requires that all practicable steps should be taken to ensure that personal data are protected against unauthorized or accidental access, processing, erasure or other use.

Proposal 13(d)

25. Under this proposal, FIs are required to include the originator's account number or a unique identifier in a message or payment form for wire transfers. The PCPD considers that security safeguards should be put in place to protect the personal data contained therein against misuse or unauthorized access or disclosure in accordance with DPP4.

Proposals 20 and 21

26. Under these proposals, the "relevant authority" will be empowered to collect personal data that are sensitive in nature. It is imperative that specific safeguards be provided to ensure data security and to protect the personal data against unauthorized or accidental access, processing, erasure or other use.

Retention of Personal Data

27. DPP2(2) stipulates that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the date are or are to be used. Also, section 26(1) of the Ordinance requires a data user to erase personal data that are no longer required for the purpose.

Proposal 15

28. The FIs are required to maintain records of identification data and transaction records for 6 years following termination of an account or business relationship. In paragraph 3.21 (page 10) of the Consultation Document, it is explained that the proposed period ties in with the relevant period under section 9 of the Organized Serious Crimes Ordinance, Cap.455 and the statutory limitation period under the Limitation Ordinance, Cap.347. The proposal goes on to mention that the "relevant authority" may require the FIs to keep records beyond the specified period if the records relate to on-going investigations or transactions which have been the subject of disclosure, or any other purposes as specified by the "relevant authority".

29. In deciding on the retention period of the personal data, the Administration should give due regard to the requirements of DPP2(2) and section 26 and FIs should ensure timely erasure of the personal data when the purpose of use is fulfilled.

Sharing of personal data with overseas regulators

Proposal 30

30. It is proposed that the "relevant authority" may share information

obtained under the proposed legislation with overseas regulators which exercise similar functions if it is in the *"public interest"*. The meaning of the term *"public interest"* is broad. Consideration may be given to particularize in the proposed legislation as far as practicable the situations where information may be shared. In addition, regard may be given to *by whom* and *how* "public interest" is to be determined and to confine "*public interest*" to anti-money laundering and counter financing terrorism only.

31. The proposal further provides that onward disclosure of information is subject to the *consent* of the "relevant authority". The proposed legislation should spell out clearly and limit the circumstances relating directly to anti-money laundering and counter financing terrorism that the "relevant authority" may give such consent.

32. The advantages of these measures are individuals may ascertain how their personal data can be used and proper safeguards are provided against possible request for sharing of information under the pretext of *"public interest"* which may not be for the purpose of anti-money laundering and counter financing terrorism.

33. It then remains yet another question on how the "relevant authority" is going to verify a request to share information. Specific safeguards should be built in against acceding to improper request.

34. Furthermore, the proposal only requires overseas regulators to adopt adequate secrecy provisions. To enhance privacy protection, it would be appropriate to require overseas regulators to adopt adequate security measures to guard against data security breach.

35. It should also be noted that any transfer of personal data from Hong Kong to overseas will be governed by section 33 of the Ordinance when it comes into operation. Section 33 of the Ordinance prohibits the transfer of personal data to places outside Hong Kong except in specified circumstances. With a view to the eventual operation of the provision, regard should be given to the existence of any data protection legislation in the recipient jurisdiction similar to that in Hong Kong and measures be taken to ensure that the data so transferred received sufficient data privacy protection.

Regulations on Remittance Agents and Money Changers

Proposal 38

36. With regard to the proposed regulation on Remittance Agents and Money Changers ("RAMC"), the Commissioner for Customs and Excise will be the licensing authority to administer and supervise the licensed RAMCs' compliance with the CDD and record-keeping obligations. The PCPD's aforesaid comments in relation to the collection, retention, use (including disclosure and transfer) and security of personal data are also applicable.

Proposal 39

37. Under this proposal, the Commissioner for Customs and Excise will maintain a register of licensed RAMCs for public inspection. The Consultation Document does not specify the information to be included in the public register. If personal data are involved, the public register should be given legislative basis and the purpose of setting up the register should be clearly stipulated in the proposed legislation. To accord with the requirements of DPP1(1), the register should only include the type of personal data the disclosure of which is necessary to fulfill the purpose as specified in the proposed legislation.

38. The applicants to be registered as licensed RAMCs should be given a Personal Information Collection Statement ("PICS") pursuant to DPP1(3). The PICS should, among other things, inform that the personal data collected will be disclosed in the register and give a clear indication of the specific purpose of the register.

39. Steps should be taken to ensure that all persons accessing or requesting access to the register are aware of the specific purpose and the need to confine the subsequent use of the data to such purpose as laid down in the proposed legislation.

40. Given the personal data in the register will be easily available to the public, it is appropriate for the proposed legislation to impose sanctions against improper use of the personal data contained in the register so as to provide sufficient protection and safeguards for personal data privacy.

Proposal 52

41. This proposal will empower the licensing authority to enter and search any premises other than domestic premises and to seize documents, records, items, etc. found on the premises. Insofar as the documents to be seized may contain personal data, it is advisable that the Administration considers requiring the authorized officers of the RAMCs' licensing authority to obtain warrant from court before exercising such power. It is generally considered a prudent measure to ensure proper exercise of the proposed power and that the intrusion to one's privacy is justified in the circumstances.

PCPD to be further consulted

42. It is noted that the legislative proposals in Annex A are brief descriptions only. To ensure that individual's personal data privacy is adequately protected, the PCPD wishes to be further consulted at the drafting stage of the relevant legislation.

Office of the Privacy Commissioner for Personal Data
5 February 2010