Public Consultation on the PDPA – Regulations and Advisory Guidelines

ABS Feedback / Comments

The ABS is grateful for the opportunity to respond to the various documents set out by the Personal Data Protection Commission ("**PDPC**") for public consultation, as set out below.

Referenced documents:

(a) Personal Data Protection Act ("**PDPA**")

(b) Proposed Regulations on Personal Data Protection in Singapore ("**Proposed Regulations**")

(c) Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act ("**Proposed Concept Guidelines**")

(d) Proposed Advisory Guidelines on Selected Topics in the Personal Data Protection Act ("**Proposed Topical Guidelines**")

Before commenting on the specific documents, the ABS would like to make certain general observations.

A. The ABS understands that the PDPA is generic in nature, and not confined to the financial industry. However, as a highly regulated industry, both in Singapore and in other jurisdictions, there are sectoral laws and regulations which overlap with the PDPA. In this respect, the ABS proposes to develop guidelines for financial institutions to ensure that there is a smooth transition when the Do Not Call ("DNC") registry and the main data protection rules come into force. The ABS would welcome the PDPC's input in the development of these guidelines.

B. The ABS would also like to suggest that clear transitional provisions be included in the Proposed Regulations, especially in the context of potential conflicts of the PDPA and the primary legislation of that particular sector. It should also consider the issue of the overlap of jurisdiction between the PDPC and the primary regulator, and in particular, the potential prosecution of the entity concerned for offences under the PDPA and the principal statute flowing from the same set of circumstances.

C. The ABS would also like the PDPC to consider a less prescriptive approach when the collection, use and disclosure of personal data is in the "legitimate interests" of the collecting organization. This term is used under the UK Data Protection Act, and is explained by the Information Commissioner's Office in their Guide to Data Protection. In the publication, they state that the "*Data Protection Act recognises that you may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.*"

D. Financial institutions require an expanded definition of "evaluative purpose" in the PDPA to take into account various regulatory and risk management requirements, such as for credit, operational, technology, regulatory and legal areas. Specific relief should be granted where sectoral requirements are already in place.

E. The ABS understands that the PDPC will also issue sectoral guidelines, including those for the financial industry. We trust that the public consultation will precede the issuance of such guidelines.

1. Definition of "personal data": Anonymisation

Reference: Paragraph 5 of Proposed Concept Guidelines, Paragraph 4 of the Proposed Topical Guidelines

Banks have the practice of codifying customer data, or masking off parts of its records, prior to transmission (either intra-group, or to third parties), usually for data processing. ABS would like PDPC to confirm that the anonymised data, when received by the party outside Singapore in such form, would not be considered personal data even if the sending party continues to be able to identify the individual. The use of the word ñorganizationò in Paragraph 4 of the Proposed Topical Guidelines is broad enough to encompass all group companies. In addition, many banks have branches globally, although they operate legally as a single legal entity. However, as an example, a branch in Singapore may mask data, which is processed by its Hong Kong Branch which may not be able to identify the individuals. The ABS requests that the PDPC clarify the definition of ñorganizationsò, taking into account group companies and/or branch networks in differing jurisdictions.

2. Definition of "personal data": CCTV Recordings

Reference: Paragraph 5 of Proposed Concept Guidelines

2.1 The ABS suggests that in the context of CCTV recordings, limitations be imposed on access and correction in the context of CCTVs, and in particular, making a distinction between such devices covering public and private areas.

2.2 The ABS would also like to propose that CCTV images at public areas (e.g. ATMs and banking halls) should not constitute personal data that fall under the purview of the PDPA.

3. Persons subject to the PDPA

Reference: Paragraph 6.3 of Proposed Concept Guidelines

Clarity is sought from the PDPC in the context of how the PDPA would be applied in the context of the ñbookingò model adopted by most financial institutions. For example, the Singapore branch may collect, use and disclose information of customers who are resident in jurisdictions outside Singapore. Conversely, Singapore resident customers may request that their transactions be booked in other jurisdictions for tax efficiency or other purposes. In the latter situation, ABS suggests that the PDPA should not apply to the branches/entities in these foreign jurisdictions where booking takes place.

4. Concept of "consent" and "deemed consent" under the PDPA

Reference: Paragraph 11 of Proposed Concept Guidelines

4.1 The ABS is extremely concerned in relation to the concepts of consent and deemed consent; in particular, the expressed inability to use the ñopt-outò method. Financial institutions consistently update their terms and conditions to take into account the dynamic changes that occur in the industry. A customerôs consent is typically obtained at account opening stage and the bank does not subsequently seek a customerôs consent as the terms and conditions agreed to at account opening provide that the bank may amend the terms and conditions at any time by notification to the customer. Factors such as a large customer base, and the inability to contact some customers or get customers to provide a response preclude obtaining consent for each change in the relevant terms and conditions.

4.2 In addition, banks may be required to collect, use or disclose customer information for a new purpose not envisaged or notified to a customer at the time consent was obtained (e.g. to provide a new product/service/benefit to customers). The ABS would like the PDPC to understand the significant difficulties that financial institutions would face if they were required to request for every customer to indicate his/her consent for the collection, use or disclosure (as the case may be) of his/her personal data for such new purposes. It is proposed that a notification to customers of the new purpose would be more practical and customers' consent should be deemed to have been

provided. The financial institution could put in place a process where a customer who does not agree to the new purpose can then withdraw his/her consent.

4.3 The ABS also proposes that in the case of consumer banking customers, where consent has been obtained prior to the appointed day (as defined in section 19 of the PDPA), the permitted use of the personal data should be extended to cover all related consumer banking activities that are required to meet a consumer's financial needs without requiring further consent from the customer for every consumer banking product. In particular and given how closely related these consumer banking products and services are, it is proposed that the consent that bank may have obtained prior to the PDPA coming into force should continue to be valid in relation to consumer banking products and services. For example, customers may use their credit cards to pay for insurance premiums (potential disclosure of personal data by the bank to an insurance company), or set up a deposit account for GIRO payments of housing loans (potential disclosure of personal data by the bank to mortgagees) or to receive funds from equities trading (potential disclosure of personal data by the bank to trading counterparties) etc.

5. Definition of "reasonable effort" and "reasonableness"

Reference: Paragraph 3.7(a) of Proposed Regulations

In situations throughout the PDPA where references were made to the use of "reasonable effort" and "reasonableness", ABS proposes to issue its own industry-specific interpretation and practices in this regard. This is to enable standardization across all banks. The ABS would welcome the PDPCôs input in the development of these guidelines.

6. Interaction between the requirements of PDPA and MAS Sectoral Requirements

Reference: Paragraph 7 of Proposed Regulations; Paragraph 15 of Proposed Concept Guidelines

6.1 In view of the overlap between MAS' sectoral requirements imposed on banks, and the PDPA requirements, ABS proposes that banks' compliance with the sectoral requirements should suffice for the purposes of the PDPA.

6.2 One instance of such overlap would be in the situation of outsourcing - ABS is of the view that banks' adherence and compliance with the MAS Guidelines on Outsourcing should suffice for similar compliance with the PDPA.

6.3 Another significant area of overlap arises in the Technology Risk Management (ñTRMò) and Business Continuity Management (ñBCMò) spaces. For example, banks with global or regional footprints may consolidate their technology support in specific countries. Under such circumstances, there could be datacentres operating outside Singapore which support the banksô Singapore businesses. Such activities are regulated by a combination of the TRM, BCM and Outsourcing Guidelines. The ABS submits that such core functions of a bank be exempted from the PDPA in the context of collection, use or disclosure [failing which financial institutions may have to seek consent in relation to every system or computer server which supports the Singapore businesses containing personal data].

6.4 ABS also notes the requirement that when using data intermediaries, banks should undertake an "appropriate level of due diligence" to assure itself that the data intermediary is capable of complying with the PDPA. In view of the due diligence already prescribed under the MAS Guidelines on Outsourcing, ABS would like to reiterate its suggestion that compliance with the MAS Guidelines on Outsourcing should suffice for banks seeking to transfer personal data.

6.5 Another instance of such overlap would be the obligation imposed on organisations to verify accuracy of personal data collected. ABS is of the view that banks' adherence and compliance with the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism should suffice for the verification obligations under the PDPA.

6.6 Such overlap is also evident in the PDPA requirements on banks to put in place reasonable security arrangements to protect personal data. ABS is of the view that compliance and adherence to the Risk Management Guidelines issued by the MAS should suffice in this regard.

6.7 As a matter of prudence, ABS would like to suggest a dialogue session to be held between the PDPC, MAS and ABS so as to better determine the concurrent application of the PDPA and MAS' sectoral guidelines on banks.

7. Data access/correction requests

Reference: Paragraphs 3.7, 5.1, 6.3 and 6.4 of Proposed Regulations

7.1 ABS proposes that the timeframe for responding to data access/correction requests be extended from 30 days to 40 days. This would be in line with the current position in Hong Kong and the United Kingdom.

7.2 Due to banks' practice to archive its records and in view of the voluminous amounts of records, physical retrieval of such archived records is typically a time-consuming process.

7.3 In addition, ABS also proposes to implement, by way of industry guidelines, the fees banks will be charging in relation to each data access/correction request. The guidelines will provide a cap on the maximum amount of fees banks will charge for such request.

8. Data retrieval/retention

Reference: Paragraph 17 of the Proposed Concept Guidelines

The ABS also would like the PDPC to consider issues relating to physical impossibilities of retrieving personal data. For example, financial institutions could delete all data relating to an individual in the transactional records, but any information contained in email relating to a specific individual may be impossible to trace. There would also be difficulties in deleting data where it is stored in micro-film (together with other data), or in archived boxes that are difficult to retrieve/trace. The ABS proposes that if such information is kept secure and as long as security measures are in place to prevent unauthorised access to the personal data, it would comply with the PDPA in circumstances where it is practically impossible to access and delete such data.

9. Transfer of personal data to foreign jurisdiction

Reference: Paragraph 7 of Proposed Regulations

The ABS requests that the PDPC clarify that organizations may be permitted to transfer personal data to jurisdictions where there are comparable standards for data privacy in place either via (a) statutes or regulations; (b) binding agreements/binding corporate rules that are enforceable in the relevant jurisdiction; or (c) compliance with inter-group policies. Such requirements should be independent of each other.

10. Minimum age to exercise rights and powers under the PDPA

Reference: Paragraphs 9.2 to 9.5 of Proposed Regulations

10.1 The ABS suggests that instead of prescribing such prescriptive rules, the position should be consistent with general law, such as the Civil Law Act.

10.2 In particular, the ABS proposes that minors 14 years old and above opening basic savings banking accounts shall be deemed to be able to give consent for use of their personal data for purposes of providing such services.

11. Personal and domestic issues in the PDPA: definition of "home or family"

Reference: Paragraphs 6.8 – 6.10 of Proposed Concept Guidelines

11.1 ABS would like PDPC to provide further clarity on the definition of "home or family".

11.2 In addition ABS would also like PDPC to provide guidance on the application of the exclusions of "individuals acting in a personal or domestic capacity". This is especially relevant in trusts situations, where the trusts are typically set up for succession planning. Banks typically request, from the settlers of trust, the personal data of the trust's beneficiary. It is not banks' practice to concurrently request for the beneficiary's consent in this regard. PDPC to consider adopting the position of the EU, i.e. processing of individual data for a purely legal purpose that does not unfairly prejudice the individual would not require the individual's consent.

12. Law enforcement agencies

Reference: Paragraph 3.5 of Proposed Regulations; Paragraph 11.43 of Proposed Concept Guidelines

For financial institutions with a global presence, it is critical to specifically include foreign regulatory and fiscal authorities under the definition of õprescribed law enforcement agencyö to allow such financial institutions to make reports to the relevant regulatory or authority.

13. Priority of nearest relatives to an individual

Reference: Paragraphs 9.6 to 9.12 of the Proposed Regulations

In view of existing laws under the Intestate Succession Act and general intestacy law, ABS proposes that the priority of nearest relatives to an individual upon such individual's death should be identical to the abovementioned intestacy laws.

14. Data intermediaries: definition of "processing"

Reference: Paragraph 6.19 of the Proposed Concept Guidelines

The ABS proposes that the definition õprocessingö should be clarified to cover situations where personal data has been transferred to an intra-group company which will undertake to perform know-your-client checks, credit checks, or such other analysis on the personal data on behalf of the Singapore bank.

15. The 3 separate registers of the do-not-call ("DNC") registry

Reference: Paragraph 2.4 of the Proposed Concept Guidelines

15.1 It is noted that the DNC registry is envisaged to comprise of 3 separate registers, covering telephone calls, text messages and faxes.

15.2 ABS would like to propose that flexibility should be granted to organisations such that it would suffice to obtain a single consent from the same customer, which would cover all 3 modes of communication.

15.3 Registration on each of the 3 separate registers should also be disjunctive, i.e. registration on the registry covering telephone calls does not mean that the individual stops receiving marketing materials via fax.

16. Periodic purging of numbers on the DNC registry

Reference: Paragraph 24 of Proposed Concept Guidelines

ABS proposes the periodic (e.g. 3 years) purging of numbers listed on the DNC registry. Individual may then re-register their numbers if they so wish. This would be an opportunity for individuals to re-consider the original decision.

17. Requirements on display of organization information

Reference: Paragraph 2.5 of the Proposed Concept Guidelines

ABS proposes the issuance of industry-specific guidelines on what is the requisite amount of information to be displayed in marketing messages made by banks.

18. Data Protection Officer ("DPO")

Reference: Section 11(3) of the PDPA

ABS would like the PDPC to provide guidance and a better scope of the roles and responsibilities of the DPO. In particular, ABS would like the PDPC to clarify whether the DPO would, as a result of his office, be subject to personal liability under the PDPA in the event of any wrong doing by the corporate or another employee of the corporate.

19. Transitional provisions under the PDPA

Reference: Section 68 of the PDPA

19.1 In view of the large amounts of personal data that banks already have in their position, some of which may not have met the requirements under the PDPA, ABS would propose for a "grandfathering" of the PDPA requirements on all past personal data collected, and for the PDPA requirements to be imposed on a "forward looking" basis.

19.2 This "grandfathering" provisions would be especially relevant in the context of consent of collection, use and disclosure of personal data in the past. The use and disclosure requirements under the PDPA should only apply to personal data collected after the sunrise period of the PDPA, and not apply retrospectively to personal data collected after the sunrise period of the PDPA.

19.3 The ABS also suggests that such "grandfathering" provisions be applied to the data destruction requirements for personal data that are collected prior to the PDPA coming into force. As mentioned above, such personal data could be stored in manners that may make complete retrieval impossible.