# VIEWS AND COMMENTS

## PUBLIC CONSULTATION ISSUED BY MICA

## PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

Organisation: The Royal Bank of Scotland Group Singapore
Contact Person: NG Hock Chuan
Issue Date: 24 October 2011

## Questions in relation to objectives and principles of proposed DP framework:

**Question 1: Do you have any specific views/comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?**

**Question 2: With reference to paragraph 3.8, do you have any views/comments on the concurrent application of the DP law with existing sectoral regulations?**

RBS fully supports self-accountability and a complaints-based approach rather than a more stringent audit-based approach. (Section 3.5)

We note that the purpose of the new regime is to make Singapore a trusted hub for global data management and processing industries, such as **cloud computing**. Given the current legal concerns around the use of cloud computing services particularly in relation to data security, we would suggest that the new law should specifically address those concerns by including particular provisions on a cloud provider's ability to isolate and clearly identify customer data. The inclusion of such mandatory local law provisions would significantly increase the confidence of customers (particularly corporate customers in the banking and financial industry) in cloud computing services in Singapore.

We are of the view that financial services firms should not face the potential threat of double jeopardy as a result of dual regulation by the MAS and by the proposed data protection law. We note that sectoral regulators may apply to the DPC to exempt their licensees from specific requirements under the general law where necessary. Since the existing provisions on banking secrecy in the Banking Law are known to provide an equivalent, if not higher, standard of data protection, the preference would be to have specific exemptions written into the DP law to account for this instead of having to rely on a separate application to the DPC by MAS. (Section 3.8)

## Questions in relation to the definition of "personal data":

**Question 3: Do you have any views/comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?**

**Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views/comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views/comments on the proposed approach to the protection of personal data of the deceased?**

We agree that the DP law cannot prescribe a fixed list of personal data that should be protected as this may depend on the context in which the data is used. However, further guidance would be helpful on certain classes of data (such as computer IP addresses or other device indicators and anonymous data) where the legal status of such data in other jurisdictions is somewhat unclear. (Section 3.12)

We also agree that higher standards for the protection of "sensitive" personal data should be addressed at sector-specific level. Likewise, in relation to the personal data of deceased individuals, our general view is that the DP law should not cover such data (due to the practical difficulties involved in identifying who is able to act on behalf of the deceased for the purposes of obtaining consent or access to and correction of personal data), but MICA could consider including a limited number of specific provisions regarding the personal data of deceased individuals where such data is particularly sensitive in nature. (Section 3.15-3.16)

## Questions in relation to the organizations and activities covered by the DP law:

**Question 5: Do you have any views/comments on the proposed organizations covered by the DP law?**

**Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views/comments as to whether the DP law should extend to organizations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organizations?**

We recognize the practical difficulties in implementing an extra-territorial regime and for that reason on balance support the DP law only being applicable to organizations in Singapore. This will of course lead to concerns about cross-border transfers of data over the internet. To address this, perhaps MICA could consider sector-specific provisions within the law (to cover, for example, those engaged in online marketing or cloud computing) whereby the law would cover organizations outside Singapore in order to increase consumer confidence in such sectors. In terms of enforcement of the extra-territorial provisions, MICA could take guidance from the success of enforcement of extra-territorial provisions elsewhere in the world (e.g. the US Foreign Corrupt Practices Act and the UK Bribery Act). There would be practical difficulties, but the law is at least likely to have some sort of deterrent effect. (Section 3.20-3.22)

If any extra-territorial provisions are introduced, there should be an exemption for **intra-group transfers** within multinational companies subject to the same internal corporate rules and policies. The removal of the consent requirement in relation to intra-group transfers would facilitate anti-money laundering activities and since intra-group transfers are relatively low risk, it should be sufficient if the Singapore entity/branch is covered by the scope of the law.

## Questions in relation to the general exclusions from the DP law:

**Question 7: Do you have any views/comments on the proposed general exclusions from the DP law?**

**Question 8: With reference to paragraph 3.26, do you have any views/comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?**

We have no views on whether there should be exclusions for artistic and literary purposes. Other specific exclusions are discussed below. (Section 3.26)

We would appreciate further guidance from MICA on how the processing of personal data through **social media** will be treated under the law. For example, where social networking sites are used to obtain information about a potential job candidate, would this “processing” be subject to the DP law?

## Questions in relation to the general exclusions from the DP law:

**Question 10: Do you have any views/comments on the proposed general rules under the DP law?**

**Question 11: With reference to paragraph 3.35, do you have any views/comments as to whether individuals should be deemed to have given consent for organizations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?**

We support the proposition that there will be no distinction between the concepts of "data controller" and "data processor" and that outsourcing providers/cloud computing providers will still be subject to the DP law on the basis that they are data controllers themselves. That said, MICA should consider whether to impose a specific liability for **subcontractors** in the DP law, given that they often invoke their subcontractor status as exempting them from any liability. (Section 3.28)

In relation to the issue of consent, it is submitted that an obligation to obtain informed consent is not always entirely appropriate and there may be circumstances (e.g. intra-group transfers, transfers of employee data etc) where a mere notification obligation is more appropriate. (Section 3.35)

We appreciate the difficulties in prescribing in detail the manner in which consent may be given in the DP Act. However, some further guidance as to what is likely to constitute consent in particular scenarios (e.g. in an employment relationship) would be helpful for businesses in Singapore and in particular, how specific the organization needs to be in describing the purposes for which collection is made. We would also ask MICA to clarify whether it proposes to include "consent' as a defined term within the new law and if so, what that definition will be. (Section 3.31-3.36)

Within the financial services industry, it is common for customers to sign-on to a set of terms and conditions during account opening. Financial institution would normally be able to amend such terms and conditions via prior notification and customers would be deemed to have accepted the new terms and conditions if no objection were received within a specific period. For practical reasons, we are of the view that an individual should be deemed to have given consent for the disclosure of personal data if the organization has given prior notification in a reasonable manner (e.g. a letter directed to the individual) for the use or disclosure data and the individual is given a reasonable timeframe to object to the usage or disclosure of information.

## Questions in relation to the proposed rules on collection, use and disclosure of personal data:

**Question 12: Do you have any views/comments on the proposed rules on collection, use and disclosure of personal data?**

**Question 13: Do you have any views/comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organizations to collect, use and disclose and individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organization? Are there any other exceptions that should be provided?**

**Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined in paragraphs 3.60 to 3.61?**

We support the proposition that there should only be a notification obligation in relation to employee personal data as opposed to an obligation to obtain consent. Likewise, our view is that organizations should not have to obtain consent for the collection of their members' personal data for identification purposes or for internal circulation although we would appreciate some clarification as to how this exclusion is intended to interplay with the exclusion in relation to employees. (Section 3.44-3.45)

We strongly support the exclusion in relation to the outsourcing of the collection/processing of personal data provided the outsourcing provider only collects and processes such data for the same purposes. (Section 3.48)

Our views on the specific exceptions in respect of disclosure of personal data are that the exceptions are generally satisfactory. However, we would ask MICA to consider whether the exception relating to investigations into an offence should be slightly wider in scope to allow organizations to disclose data (if necessary) in connection with an **internal investigation** into criminal activity or fraud.

We support the exclusion relating to the sharing and transfer of personal data when organizations are involved in a merger or acquisition. (Section 3.57)

With regard to the proposed approach to the transfer of personal data outside Singapore, we support a risk-based approach where the onus is on the organization to ensure implementation of appropriate security measures where data is transferred outside Singapore. An EU-type approach involving binding corporate rules or standard contractual clauses would be too prescriptive and is likely to lead to difficulties in practice. (Section 3.60-3.61)

## Questions in relation to the proposed rules on accuracy, protection and retention of personal data:

**Question 14: Do you have any views/comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?**

**Question 15: With reference to paragraph 3.67, do you have any views/comments as to whether organizations should be required to specify the retention period when collecting personal data?**

We generally support the proposals with respect to the accuracy, protection and retention of personal data. However, further guidance from MICA would be helpful in determining what is meant by "**reasonable effort**' with regard to the obligation to ensure data is accurate and complete. Does a "reasonable effort" require an organization to incur additional expense in relation to such activity? (Section 3.63)

Our view is that organizations should not be required to specify the retention period at the point of collecting the personal data as it is not always possible or practical to determine the appropriate retention period in advance. (Section 3.67)

Financial services firms are subject to statutory record retention requirements in Singapore as well as from head office and/or head office regulators (in the case of foreign financial institutions). The DP law should not preclude organizations from complying with sectoral regulatory requirements (in Singapore or in home jurisdiction).

## Questions in relation to the proposed rules on access to and correction of personal data:

**Question 16: Do you have any views/comments on the proposed rules on access to and correction of personal data?**

We would appreciate clarification from MICA as to whether information provided in response to a data access request has to be provided in permanent form and whether there is any **time limit for providing** such information. We would also like clarification as to how to deal with requests from employees for information contained in **confidential reports/performance reviews** and so on.

In relation to the costs of providing access, we do not support a fixed fee and agree that a more flexible approach is appropriate. We would, however, ask MICA to address the issue of potential disputes over fees. Can an organization legitimately refuse an access request if the data subject refuses to pay the quoted fee?

The consultation paper states that an organization shall not be obliged to comply with an access request where personal data is collected or disclosed without consent "for the purposes of an investigation". We would ask MICA to clarify whether this exception is intended to cover internal investigations in relation to criminal activity/fraud, or only investigations carried out by law enforcement agencies in Singapore.

We would also appreciate further clarify on how the provisions of the DP law are intended to relate to anti-money laundering (AML) obligations. For example, would an exemption to an access request automatically apply to any Suspicious Transaction Report made under existing Singaporean legislation? What should an organization do if it is in doubt over whether disclosure of personal data would prejudice an investigation?

## Questions in relation to the proposed penalty and enforcement regime:

**Question 17: Do you have any views/comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?**

**Question 18: Do you have any views/comments on the proposed penalties for contravention of the DP law outlined in paragraphs 4.4 to 4.5? Do you have any views/comments on the criteria for breaches that would warrant financial penalties?**

We support the proposed tiered penalty regime and agree that a maximum fine of $1 million would represent an effective deterrent. However, we would only support custodial sentences in the most extreme of cases e.g in the case of fraud.

We repeat our view that financial services firms should not face the potential threat of double jeopardy as a result of dual enforcement by the MAS and by the proposed data protection law. We note MICA's proposal that the DPC can refer an incident to another regulatory agency if necessary, and support this proposal but would prefer this to be a mandatory obligation (as opposed to at the discretion of the DPC) in cases where an incident constitutes a breach in both regimes.

## Questions in relation to transitional arrangements:

**Question 19: Do you have any suggestions on specific guidelines that the DPC should provide to help organizations achieve compliance with the DP law?**

**Question 20: With reference to paragraphs 4.11 to 4.14, do you have any views/comments as to whether a one to two year "sunrise" period would be appropriate?**

**Question 21: With reference to paragraphs 4.15 to 4.19, do you have any views/comments on the proposed treatment of existing personal data?**

**Question 22: Are there any certain organizations that may require different transitional arrangements?**

We are of the view that a "sunrise" period of 2 years would give organizations sufficient time to modify their existing practices and procedures to ensure compliance with the law. (Section 4.14)

We have made a number of specific suggestions above as to where we would like MICA to issue further guidance or clarification to help organizations achieve compliance with the DP law.