STATE STREET.

State Street Bank and Trust Company

Singapore Branch
168 Robinson Road
#33-01 Capital Tower
Singapore 068912

main +65 6826 7100
facsimile +65 6826 7377

www.statestreet.com

Oct 20 2011

Ministry of Information, Communication and the Arts
140 Hill Street, #02-02
MICA Building
Singapore 179369

Dear Sir/Mdm,

Public Consultation of the Proposed Consumer Data Protection Regime for Singapore

Thank you for the opportunity to comment on the proposed Singapore consumer data protection ("DP") regime. State Street is a leading financial services provider serving some of the world's most sophisticated institutions. We offer a flexible suite of services that spans the investment spectrum, including investment management, research and trading, and investment servicing. State Street's singular focus on serving the needs of institutional investors is one of its key competitive differentiators. With US$22.8 trillion in assets under custody and administration, and US$2.1 trillion under management as of Jun 30 2011, State Street is an industry leader and innovator — setting standards with new products and services, and expanding the depth and breadth of client relationships.

State Street supports the over-arching objective of the DP regime which is to protect consumers' personal data through the regulation of the collection, use, disclosure, transfer and security of personal data. Moreover, we support the pragmatism of the proposed DP laws which seek to create a balance between the need to protect the individuals' personal data with the need for organizations to use the data for legitimate and reasonable purposes. We welcome the stated goal of achieving consistency between the DP regime and international standards. We also agree that getting the DP regime right will be key to developing Singapore as a data management and data processing hub.

We are broadly in agreement with the proposals on transitional arrangements, retention periods, collection, use, disclosure and consent of the DP laws. We do, however, recommend bank customer information be excluded from the DP laws given the risk of partial overlap and confusion in implementing the existing banking secrecy regime. In addition, we do not see the need for mandatory notification or the "opt-out" approach

where the purpose of data collection is legitimate, reasonable or obvious. Also, an organization that is outsourcing the collection and/or processing of personal data should be responsible for obtaining customer consent rather than the organization processing the information on an outsourced basis. Finally, we recommend a flexible approach to retention limits.

Detailed comments follow below:

1 Impact of the Proposed DP laws on the Banking Sector and Reasonable Exclusions

1.1 In response to question 2 of the paper, on the concurrent application of the DP law with regulations in specific sectors, we disagree that the DP regime should operate concurrently with the banking secrecy regime. The DP regime should exclude bank customer information, on the bases that:

- bank customer information is already protected by the banking secrecy regime;
- the banking secrecy regime currently provides for appropriate exclusions, for example customer information sharing for the purposes of audit and risk management, among others;
- analyzing and implementing the differences between the DP regime and the banking secrecy regime would be difficult and open to different interpretations which risks partial overlap and confusion in implementation; and
- while both Hong Kong and New Zealand have general DP laws that co-exist with specific sectoral regulations (as referenced in footnote 13 of the paper), they do not have a banking secrecy regime.

1.2 As for question 7, if the MICA were to decide to apply the DP laws concurrently with the banking secrecy laws, the general exclusions should reference the banking secrecy regime for consistent and appropriate exclusions, for example personal data collected for legitimate and reasonable purposes of audit and risk management (which includes satisfying anti-money laundering requirements).

1.3 If a general exclusion is not possible then arrangements should be made with the bank supervisor, the Monetary Authority of Singapore (MAS), to exempt banks from specific requirements under the general DP law – a mechanism proposed in paragraph 3.8 of the consultation paper for sectoral regulators.

1.4 We agree to MICA's practical exclusion of an individual's business contact information from the DP laws as proposed in paragraph 3.25 of the consultation paper.

2 Extra-Territoriality of the DP Laws

2.1 In response to question 6 of the paper, we agree that Singapore's DP laws should only cover organizations in Singapore due to the practical difficulties of applying the laws to foreign organizations during complaint investigation or proceeding with enforcement action.

3 Consent

3.1 In response to question 10, we agree to the general flexibility on the type of consent, whether explicit or implied, proposed by the MICA. An example where consent is deemed to be given and the purpose is obvious to a reasonable person is where personal data, such as qualifications, work experience and contact details, is provided to organizations by job applicants.

3.2 In addition, personal data, such as family details, are often provided to companies for the purpose of technology application authentication. The purpose of data collection in this instance is for the legitimate purpose of data protection and the purpose is generally understood by those providing the information. We are of the view that such personal data should be excluded from the need to obtain prior consent or notification.

3.3 Where the purpose of collection of data is legitimate, reasonable and obvious, for example under the circumstances highlighted in paragraphs 3.1 and 3.2 above, prior consent or notification should not be mandatory. The "opt-out" approach canvassed in question 11 would therefore not be necessary.

3.4 In response to paragraph 3.29 of the consultation paper, while we agree to the principle that an organization which has control over personal data should be responsible for the personal data, a service provider to whom the collection of data has been outsourced usually does not have a direct relationship with the individuals from whom data has been collected. Under such circumstances, the responsibility to obtain prior consent should rest on the organization that is outsourcing the collection and/or processing of personal data.

4 Rules on the Collection, Use and Disclosure of Personal Data

4.1 In response to questions 12 and 13 on the collection of personal data, we agree that the DP laws should allow for the collection of employee personal data for the purposes of establishing, managing or terminating an employment relationship and for internal circulation of data, for example photographs for organizational news letters and identification passes, without the need for consent. Mandatory consent would be onerous relative to the benefits of protection as the data is intended for internal circulation. However, it is reasonable to notify the individual the purpose of collection of the personal data.

4.2 On question 14 pertaining to the transfer of personal data outside Singapore, we agree to the proposed "principle-based" approach where the onus will be on the organization to ensure that appropriate measures are taken to protect personal data where such data is transferred outside Singapore, as the organization is considered to have control over the data.

5 Retention Period

5.1 In response question 15, it might be impracticable to specify the retention period at the point of collecting the personal data. Different types of information may need to be retained for different periods by different institutions. There might be instances where information needs to be kept for many years. For example, where an employee has been with the organization for 15 years or more or a customer has a long term relationship with an organization. We agree with the approach proposed in paragraph 3.66 of the consultation that information should be retained for a sufficient period of time so that the individual has a reasonable opportunity to have access to it, and that the information be disposed of appropriately when retention is no longer necessary. The DP regulations should give companies the flexibility to determine what constitutes reasonable access times and when retention is no longer necessary.

6 Transitional Arrangements

6.1 On question 21, we agree to the non-retrospective application of DP laws to the existing personal data due to the practical difficulties and costs of doing so. In addition, where such existing personal data, for example address or transaction information, change but the purpose of personal data collection has not changed, the DP laws should similarly not apply.

In conclusion, while we are supportive of the majority of the proposals in the consultation paper we recommend a review of the approach to the protection of bank customer information under the DP given the banking secrecy laws. Responsibility for obtaining consent should clearly rest with organizations outsourcing information rather than service providers. A flexible approach to time limits on the retention of information would be a sensible approach. In some circumstances, set out above and in the consultation paper, mandatory consent for the transfer of information would be unwarranted.

If you have any questions, please call June JA Lau, Head of Compliance, State Street Bank and Trust Company Singapore, at (65) 68267119 or email her at juneja.lau@statestreet.com.

Yours faithfully,

Nick Wright
Senior Vice President
Singapore Branch Manager