KPMG LLP
16 Raffles Quay #22-00
Hong Leong Building
Singapore 048581

Telephone +65 6213 3388
Fax +65 6225 0984
Internet kpmg.com.sg

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

Our ref CL/JJ/rm120430

Contact Caroline Lee
DID +65 6213 2620

30 April 2012

Dear Sirs

Response to public consultation on the proposed Personal Data Protection Bill and Do Not Call Registry

KPMG LLP (KPMG) is pleased to provide its feedback as part of MICA's public consultation on the proposed Personal Data Protection Bill and Do Not Call Registry.

In general, we agree with the need for a baseline standard for data protection, and accordingly a data protection law that cuts across all sectors. We believe the proposals on the data protection regime and do-not-call registry balance the needs of individuals with the needs of businesses. One concern we have is that foreign businesses may still hold the view that the proposed legislation does not offer sufficient protection, and may have reservations about transferring personal data into Singapore or storing them in Singapore. Whilst we recognize that this legislation is a step in the right direction, other regulators may not view it as equivalent to the data protection legislation in their jurisdiction.

One area where we believe the legislation needs greater clarity is around certain key terms. These terms, such as 'located', 'disclose', 'use' and 'data intermediary' do not appear to be defined within the proposed legislation. This may lead to different interpretations as to when the legislation applies. Further, clarity is required on which party bears the obligation to notify under Section 22(2) of the proposed Personal Data Protection Act.

We would be happy to discuss any of these matters in greater detail. Please feel free to contact me at the above telephone number or email carolinelee@kpmg.com.sg

Yours faithfully

Caroline Lee
Partner, Risk Management Department

Introduction

KPMG is committed to respecting the privacy of its people, clients and others in the community. KPMG agrees with the need for a minimum data protection base-line across all sectors of industry.

We note that personal data laws are rarely absolute; they should be balanced against the legitimate needs of other individuals, organizations and the public interest.

KPMG adopted and implemented personal data protection policies and practices in 2007. While we support MICA's intention to safeguard individuals' personal data against misuse, based we believe there's a need for greater clarity on the application of the Personal Data Protection Act (PDPA), and certain key provisions within it.

Examples

We have created four scenarios which will be referred to throughout this paper for illustration purposes.

Scenario One: A multi-national network of professional services firms uses common IT systems that include personal data from both Singapore and overseas jurisdictions (local and global data). This system can be accessed by employees in Singapore, and the personal data of Singaporean employees are also entered into the system.

Scenario Two: A telecommunications firm is required to undergo an audit. To enable the audit to be performed, it must allow the auditors access to all of its systems and documents. The auditor will use this information (including personal data) for the purposes of performing the audit. The information may also be accessed by staff from the audit firm (or its affiliates) for the purposes of performing internal reviews.

Scenario Three: A multi-national logistics company uses a third party IT service provider for its HR evaluation processes. Employees must enter their personal data into the system, prior to their manager's review also being entered. Each country hosts its own data in-country and access is restricted to employees within the same country, but all of the servers are mirrored to the third party service provider in Canada. The third party host can access the data files to perform maintenance on the servers, but does not have the encryption keys to make the data readable.

Scenario Four: A real estate firm is about to send out a brochure of a new development to all everyone on their mailing list who has previously put their name down in their visitors book. They provide all of the names and addresses to the printing firm in order for them to print personalized brochures.

Definitions

In order for the PDPA to be effective, the key terms within the Act need to be clearly defined and understandable. In the present draft, it is noted that the following terms are used repeatedly but are not defined, or not sufficiently defined, to provide a clear demarcation on where the PDPA will apply:

- "collect" or "collected";
- "located";
- "disclose" or "disclosure";
- "use"; and
- "data intermediary".

Collect / Collected

"Collect" and "Collected" are used throughout the PDPA. As this term is essential to interpreting the scope and requirements under the Ac, it therefore requires a very clear definition. To illustrate, we have come up with the following questions in relation to scenarios which we believe would regularly occur in Singapore:

- In Scenario One, have the Singaporean employees "collected" the personal data (Singaporean and Global) when they access the system? Similarly, have the other entities which use the system overseas "collected" the personal data of Singaporeans when they access the system?
- In Scenario Two, has the professional services firm "collected" the personal data of its client when it collects documents to perform an audit?
- In Scenario Three, has the third party service provider "collected" the personal data by providing hosting services?

As these are situations which KPMG regularly encounters for both its own personal data and that of clients, it is very important that it will be simple to ascertain when the PDPA will apply.

We would suggest a definition which includes "gathering, assembling or receiving personal data". This would mean that the personal data in Scenarios One and Two would be deemed to have been "collected", but the data in Scenario Three would not (as the third party host does not have the encryption key to make the data readable).

Located

This term is used in Section 5 of the PDPA. We are unclear as to what circumstances this would cover, other than obvious situation where physical documents are located in Singapore. For example, in Scenario One, is the global data "located" in Singapore if it can be accessed by an individual in Singapore?

We would suggest that Section 5(2)(a)(ii) is either re-worded, or guidance is provided to clarify what will be considered as "located" in respect of electronic information. We would even suggest that where such data is "located" in Singapore but not accessible by an individual in Singapore, such date is not defined to be subject to the PDPA.

Disclose / Disclosure

These terms are also used extensively throughout the PDPA and, as per "collection" are essential for determine the scope and application of the PDPA. For example:

- In Scenario One, have the entities "disclosed" the data by inputting the information into the system, which can be accessed other entities in other jurisdictions?
- In Scenario Three, has the logistics company "disclosed" data to the third party hosting service if the third party hosting service holds an encryption key? If so, would it still have "disclosed" the data, if the third party hosting service is unable to access the data in a readable form?

We would suggest a definition which includes "providing or transferring personal data in a readable format". This would mean that the personal data in Scenarios One, Two, Three and Four would be deemed to have been "disclosed", but the data in Scenario Three would not be deemed to be disclosed to the third party host.

Use

In general, we believe that "use" should be replaced with the term "process / processing" which has been defined. Further, we believe guidance may be necessary to address the following queries:

- In Scenario One, have the users of the system "processed" or "used" the personal data merely by accessing it, or having the ability to access it?
- In Scenario Three, has the third party hosting service "processed" or "used" the personal data?

Data Intermediary

We understand that "data intermediaries" are only required to safeguard personal data, without being subjected to the other sections of the PDPA. As data intermediaries will have substantially lower compliance requirements, it is important to clearly demarcate "data intermediaries" from "data controllers". Given the current definition, we believe the following situations would require further guidance:

- In Scenario One, are each of the receiving entities "data intermediaries" of the personal data of the other firms (and "data controllers" of the information which they input into the system), or are they "data intermediaries", or does this depend on the purpose for which they access the information?
- In Scenario Two, is the professional services firm a data intermediary?
- In Scenario Three, is the third party hosting service a data intermediary?
- In Scenario Four, is the printing firm a data intermediary?

We appreciate any thought MICA provides to the abovementioned scenarios and hope that either further definitions can be included in the PDPA, or that further guidance will be provided.

Jurisdictional approach

We believe that a balance MICA has taken the correct approach in proposing that the PDPA will cover all organizations that are engaged in data collection, processing or disclosure within Singapore, even if the organizations may not be physically be located in Singapore. Failure to do so would lead to overseas firms having an unfair advantage of lower compliance requirements while operating in Singapore, as well as failing to provide protection for individuals whose data is processed by non-Singaporean entities.

We also support MICA's decision to remove the requirement for organizations to take "appropriate measures" where "such data is transferred outside Singapore". Given the important of maintaining information flows among economies, we believe that a specific requirement for certain measures to be taken only when transferring data outside of Singapore would have unnecessarily restricted this flow, or placed burdens on it which would have had adverse implications for Singapore as a global business hub and created a significant implementation burdens on Singaporean organizations that belonged to global networks and/or had servers overseas.

Further, as advised by APEC, we would suggest the DPC to consider developing co-operative arrangements and procedures to facilitate cross-border co-operative arrangements so as to allow

for the enforcement of data protection laws in other jurisdictions. We would also appreciate guidance from MICA as to whether it will accept Inter-Firm Agreements and/or Binding Corporate Rules as an acceptable means for providing reasonable protection for personal data when transferred between different legal entities across multiple jurisdictions.

Consent, Purpose and Use

In regard to the "Purpose" provisions, we agree with the general principle that consent should be obtained where personal data is being used for a different purpose other than the purpose for which it was collected. However, we would like confirmation that the original use will not be narrowly defined.

For example, as a tax, audit and advisory firm, KPMG is often required to access personal data of our clients (their employees and our client's clients) in order to perform the services required (as illustrated in Scenario Two). If it was necessary for our clients to gain fresh consent from all of their employees and clients for KPMG to access the data to perform the business related services, this would cause a substantial administrative burden on the organization. As such, we believe that the original request for consent could indicate that third parties / service providers might obtain access for personal data for legitimate business purposes, and that this disclosure would be sufficient to obtain an informed consent as required under the PDPA.

In the alternative, we would request that MICA consider an additional exemption under Schedules 3 – 6 to allow for "where personal data is processed in aggregate for a legitimate business purpose, where the processing is not intended to affect the individuals to whom the personal data relates". We believe that this exemption would facilitate the processing of personal data by professional service firms where the personal data is only processed incidentally as part of the provision of a service to a business. Such an exemption could still be subject to compliance with Sections 20 and 26 of the PDPA.

Notification of Purpose

With regard to Section 22(2) of the PDPA, there is currently uncertainty as to whether the obligation will belong on the disclosing party to provide the receiving party with the information regarding the purpose of the collection, or whether the receiving party will have the burden of ensuring it has received the information regarding purpose prior to collecting the personal data.

Due to the frequency with which information is transferred between entities, it is important to determine which party would be liable in the event that the personal data is transferred without the purpose being disclosed to the receiving party.

We thank MICA again for the opportunity to provide our comments on the PDPA and would be happy to discuss further if so requested.