GE
Global Growth & Operations

Stuart L Dean
CEO, ASEAN

Level 6, 1 Sentral
Jalan Travers
Kuala Lumpur Sentral
50470 Kuala Lumpur
Malaysia

T +603 2273 9788
F +603 2273 7988
stuart.dean@ge.com
www.ge.com/asean

October 25, 2011

Honorable Dr Yaacob Ibrahim
Minister
The Ministry of Information, Communications & The Arts
140 Hill Street
#02-02 MICA Building
Singapore 179369

Dear Minister Dr Yaacob Ibrahim,

In light of the request for public consultation launched by your Ministry in respect of the Proposed Data Protection Law, we are pleased to set forth our views as follows:

Jurisdiction
In relation to Questions 5 & 6, we are of the view that the law should not be applied to data originating outside of Singapore. Singapore is a regional hub and many multi-national companies have chosen to site and operate their regional and sometime global data centers and BPO centers in Singapore. It would be extremely inexpedient, if not cumbersome, to business and operational efficiencies to obtain consent from foreigners to comply with a Singaporean law. This is likely to have a negative impact on Singapore and may prove to be a deterrent against using Singapore as a regional or even global hub for such a purpose. Hence, an application of this law to a wider scope would be contrary to the government's economic strategy in promoting Singapore as a business hub for such information collection and processing activities.

Scope
We are in favour of the intent behind Para 3.14 which seems to scope out business contact information. In addition, we would like to suggest that a threshold be set for personal information items as many small and medium enterprises in Singapore may have a hard time meeting the legal requirements to assign a privacy officer and implementing controls if they handle very few of such records. It may be worthwhile taking guidance from the recent experience in Japan where there was no threshold set initially when the Personal Information and Protection Act was first introduced in 2004 but METI had to introduce a threshold thereafter in response to widespread complaints.

Consent
We note that the issue of consent is raised in a number of places. (See : Paras 3.44, 3.48, 3.55, 3.56. 3.57. and 3.61). Our view is that the preferred approach is to opt for implied consent rather than express consent. There is no universal way of obtaining express consent that may be regarded as unequivocal and very often, the process of obtaining such consent slows downs business progress and puts a heavy cost and burden on operations.

Guidelines & Sunrise provision
We note that the sunrise period defined in Para 4.14 seems to start from the law being published rather than the guidelines being published. Our suggestion is that while the sunrise period could apply to the law, there should also be a similar sunrise period applicable to the guidelines as and when they are promulgated and implemented in order to allow sufficient time for companies to comply with them in line with MICA's goals.

Cross-border data transfer
In relation to Question 14 and Para 3.61, we are in favour of an approach where no sign-offs or consents are required. We believe a provision requesting security controls to be put in place before cross-border data transfers take place would be fair as long as the requirement for such security controls are reasonable and not a specific control that is not industry standard internationally.

Retention
In Question 14 and Para 3.67, we feel that it may not be practically feasible to specify to the customer a retention period on origination of the personal data. The better and more flexible approach would be simply to allow for a retention period that would be for as long as may be necessary for that relevant business needs/operations and as required by law.

Access
In relation to Para 3.68 which states:

"*Generally, upon the request of an individual, the organisation should take steps to assist the individual in obtaining access to his personal data, provide the individual with information about the ways in which the personal data has been and is being used by the organisation, and provide the individual with the names of the individuals and organisations to whom the personal data has been disclosed*"

We would suggest changing "individuals and organizations" in the last line to just "organizations". Providing the names of the individuals who handled a customer's data is difficult to do in operations and call centers that make heavy use of contractors and dispatch workers. Also it is dangerous to do in industries such as personal finance where a customer may feel the desire to harass staff. Revealing those names of individuals would compromise the privacy of those staff and may even pose physical danger to the security of these people.

Others
Lastly, we also seek clarification if there would be reporting requirements under the new law on security incidents like data leaks and would be interested to review such provisions, if any.

We look forward to continue working with you and your senior officials on these key issues and remain at your disposal to discuss any of this in further detail.

Yours sincerely,

Stuart L Dean
CEO, GE ASEAN