MARCH 20, 2013

Public Consultation on Proposed Regulations and Guidelines on Data Protection in Singapore

Submission by the Global Privacy Alliance

Miriam H. Wugmeister
Morrison & Foerster LLP
1290 Avenue of the Americas
New York, New York 10104
(212) 506-7213
mwugmeister@mofo.com

Public Consultation on Proposed Regulations and Guidelines on Data Protection in Singapore

Submission by the Global Privacy Alliance

Morrison & Foerster LLP on behalf of the Global Privacy Alliance is pleased to offer the attached submission in response to the consultation papers issued by the Personal Data Protection Commission of Singapore on its proposed regulations ("Regulations") and guidelines ("Guidelines") under the Personal Data Protection Act 2012.

The Global Privacy Alliance ("GPA") is comprised of a cross section of global businesses from the financial services, automobile, aerospace, consumer products, computer hardware and computer software, communications, and electronic commerce sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

SUMMARY RECOMMENDATIONS

Cross-Border Transfers

- In addition to permitting the use of legally binding instruments, the Regulations should provide for additional cross-border mechanisms such as the use of consent. Flexibility is needed because there are certain situations in which it is neither possible nor appropriate to have in place a legally binding instrument.
- The Regulations should make clear that legally binding instruments do not require Commission approval.
- The Regulations should clarify that transfers within the same legal entity are not subject to cross-border requirements.

Consent

- The Guidelines should clarify that when processing is necessary for the purposes of the legitimate interests of the company or the third party to whom the data are disclosed, consent is not required or, alternatively, deemed consent would be sufficient. In particular, consideration should be given to clarifying the scope of the consent exceptions and possibly the definition of deemed consent to make clear that there are additional legal grounds available to cover processing for routine and legitimate business activities.

Jurisdiction

- We encourage the Commission to issue a clarification or legal guidance that confirms that foreign organizations that outsource their foreign data processing to service providers located in Singapore or otherwise use Singapore data intermediaries would not be subject to the Act's provisions with respect to the processing of their data in Singapore.

I. Introduction

The Global Privacy Alliance commends the government of Singapore for its efforts to develop a robust data privacy law based on well-established, globally recognized privacy principles. The Personal Data Protection Act 2012 ("PDPA") contains the elements essential for an effective data privacy law. At the same time, the PDPA avoids burdensome regulatory requirements such as registration procedures and protections for business contact information that do little to further privacy protection. The exclusion of business contact information is a welcome exclusion that is consistent with practices in other countries that recognize the value of protecting information that individuals truly expect to keep private. We are also encouraged by the reasonable 18-month phase-in period that will facilitate the ability of global companies to comply with the law. The law's business friendly approach will enhance Singapore's ability to serve as an important IT hub in the region.

We appreciate the opportunity to submit these comments on the proposed Regulations and Guidelines. The Regulations and Guidelines will play an important role in establishing and clarifying the rules that companies must follow to implement the law's provisions. These rules need to be sufficiently flexible to protect and, at the same time, facilitate cross-border data transfers and commerce.

II. Cross-Border Transfers (Regulations)

In the Regulations, the Personal Data Protection Commission ("Commission") emphasizes the importance of maintaining a flexible approach to cross-border transfers but proposes that all cross-border transfers must be executed on the basis of a legally binding instrument that implements key obligations under the Act. In particular, it proposes the use of legally binding contracts for inter-corporate cross-border transfers and binding corporate rules (BCRs) for intra-corporate transfers. We agree with the Commission that organizations should be given some flexibility to determine the means to transfer personal data out of Singapore and that contracts and BCRs provide a useful way to accomplish this. In many situations, it is appropriate and desirable for organizations to have legally binding instruments in place. However, there are situations in which consent should be permitted as an alternative mechanism for cross-border transfers.

For example, an employee of a Singapore affiliate would like to be granted stock options under the U.S.-based parent company's stock option plan. The employee in Singapore and the employer in Singapore typically provide personal information directly to the parent company in the US which in turn may have to share the information with US securities regulators. In order to be granted US stock options, the information must be in the US. Requiring an agreement between the Singapore affiliate and the US parent would be unnecessary. Rather, if the employee wishes to be granted the stock options, then he/she will need to agree to allow his/her information to be shared with the US parent company and with US regulators.

Another example is when an employee requests that the company forward his/her compensation information to a foreign-based accountant or to a foreign-based financial

institution that is considering giving the employee a loan or mortgage for a home. The employer should not be expected to put into place transfer agreements with every possible accountant and/or financial institution, particularly those with whom the company has no ongoing relationship. In such cases, obtaining the individual's consent to the disclosure of the personal information should provide a sufficient legal basis on which to execute the cross-border transfer to the financial institution or accountant, provided it is given in accordance with the Act's consent requirements for third party disclosures.

Another possible situation where the use of consent should be permissible for cross-border transfers is when the company must comply with different national legal obligations. Under the US Fair and Accurate Credit Transactions Act of 2003 (FACTA), if a Singapore customer (who is a US taxpayer) wishes to transact business in the United States, he/she would have to agree to have his/her personal data transferred to the US Internal Revenue Service (IRS). Neither the Singapore affiliate nor the US parent would be able enter into an agreement with the IRS with respect to handling of that personal information and thus would not be able to obtain a legally binding arrangement with the recipient of the data in the US.

While organizations should endeavor to transfer wherever possible on the basis of a legally binding instrument, some additional flexibility is necessary. The majority of jurisdictions in the region (Philippines, Japan, Hong Kong, New Zealand, Taiwan and Australia) have adopted flexible cross-border approaches that do not mandate legally binding instruments for each and every cross-border transfer.

In addition, the Commission does not indicate in the draft Regulations whether an organization's legally binding instruments would need to be individually approved by the Commission before transfers may take place. We recommend that the Regulations set forth the basic requirements or principles that must be reflected in contracts or BCRs and then leave the execution to organizations concerned, without the need for DPA approval.

Lastly, there is one additional clarification that we think would be useful for the Commission to make. Where a transfer is within the same legal entity (not between affiliates) but crosses the national border, we suggest that the cross-border rules would not apply. For example, consider the case where Company XYZ's branch office in Singapore transfers personal data to Company XYZ branch in the US (the transfer is within the same legal entity). The legal entity (Company XYZ) remains responsible for protecting the data in accordance with the Singapore law within that legal entity. Although the information moves cross-border it would be protected by the same legal entity. We believe that this should not constitute a cross-border transfer. We would appreciate clarification to that effect.

There is a growing consensus that strict rules that limit cross-border transfers do not reflect the reality of global information flows and are not the best method of ensuring that personal information will be protected when it is shared across the borders. We urge the Commission to consider these refinements which we think are necessary to protect and facilitate cross-border transfers.

III. Consent (Guidelines)

Organizations need to collect, use and disclose personal data for many purposes, some of which are for routine and legitimate business operations. In such cases, obtaining the individual's consent would be burdensome or inappropriate. It would be helpful if the Commission clarifies in the Guidelines that when processing is necessary for the purposes of the legitimate interests of the company or the third party to whom the data are disclosed, either consent is not required or deemed consent would be sufficient.

Examples of activities where consent should not be required include:

- *Data Loss Prevention.* Companies seek to protect the personal information that has been entrusted to them by corporate customers, individuals, and business partners. One tool that is becoming more widely used is Data Loss Prevention software which allows a company to ensure that sensitive personal information is not inadvertently disclosed by employees. Absent clarity being provided, companies may be reluctant to utilized such tools in Singapore if they believe that consent is required in order to implement such tools. Companies should be encouraged to protect tools that protect personal information and thus consent should not be required in these situations as it will undercut the effectiveness of the tools and discourage organizations from utilizing them.
- *Sharing with Affiliates.* More and more organizations are seeking to centralize their systems and process personal information relating to employees or customers on a global basis. These companies wish to run their IT intrasructure more efficiently, provide 24/7 customer service centers using a "Follow The Sun" model, perform workforce analytics or ensure equal opportunities to employees. Without clarification from Singapore regulators, it is unclear if consent would be needed from each individual whose personal information might be collected, used or shared among affiliates for these expected and legitimate purposes. Requiring consent in this situation would create bureaucratic obligations without adding privacy protection for individuals.
- *Sharing in order to comply with foreign regulatory or legal obligations.* Multinational organizations are often caught between competing regulatory or statutory obligations and it is imperative that, as new privacy regulations are interpreted, organizations are not forced to choose with which law to comply. For example, a company that is headquartered in the US but has operations in Singapore could receive a request from the US Department of Justice that would require the US company to collect information from individuals in Singapore in response to the request. If consent were required and if the individual in Singapore refused to consent, the US entity would then be in a very difficult position because in order to comply with Singapore law it would be required to violate its obligation to the US Department of Justice. Organizations should not be required to obtain consent if the information is needed to comply with a legal obligation in another country or to respond to a valid legal process or a request from a public or government authority.

While there is no a legitimate interests exception under the PDPA, there are various consent exceptions that might cover such activities.[1] Perhaps these exceptions could be interpreted to fully cover these types of routine and legitimate processing of personal data? It would be helpful, therefore, for the Guidelines to clarify the scope of existing consent exceptions and possibly the definition of "deemed consent" to make clear that there are additional legal grounds available to cover these types of activities. Jurisdictions in Asia, such as the Philippines, Korea and Macao, and many in Europe permit the processing of personal data without consent for the legitimate interests of the company or the third party to whom the data are disclosed. Therefore, Singapore should consider addressing this issue in its Guidelines in order to assure companies that they will be able to carry out legitimate processing activities without having to rely on consent as the only justification for such activities.

IV. Jurisdiction Rules (not addressed in either the Regulations or the Guidelines)

Consistent with its objective to promote Singapore as an IT hub in the region, the Act makes clear that data intermediaries are exempt from all but the data security and retention requirements. However, the Act broadly defines an "organization" which could be interpreted to include companies that rely on Singapore-based IT service providers to process their foreign personal data. Since foreign personal data processed in Singapore are already subject to foreign data privacy laws, imposing an additional layer of regulation on such processing would discourage the use of Singapore-based service providers. We do not believe this interpretation is consistent with Singapore's intent.

Countries such as India and the Philippines that also seek to promote their IT industries have made clear that processing of foreign data in their respective countries is not subject to their laws. For example, in response to India's outsourcing industry concerns about the overly broad application of India's Privacy Rules issued in 2011, the Ministry of Communication & Technology issued a clarification[2] to make clear how the Rules apply to different types of organizations in India. In particular, if an organization in India receives information as a result of a contractual obligation with a legal entity (either inside or outside India), *e.g.,* it is acting as a service provider, the substantive obligations of notice, choice, data retention, purpose limitation, access and correction do not apply but the security obligations and the obligations relating to the transfer of information do apply. However, if an organization in India receives information as a result of a direct contractual relationship with an individual, all of the obligations under the Privacy Rules would apply.

Partly in response to the experience in India, Philippine government and industry officials worked closely together on the Philippine Data Privacy Act of 2012 to ensure that the Act would not put the Philippine outsourcing industry at a competitive disadvantage. As a result, the scope provisions make explicit that organizations that outsource their foreign data processing to service providers located in the Philippines and their Philippine-based service providers are not subject

---

[1] See Sections 1(a), (e), (f), and (o) of the Second Schedule; Sections 1(a), (e), (f)of the Third Schedule; and Sections 1(a), (f), and (h) of the Fourth Schedule.

[2] See Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000, available at http://www.mit.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf.

to the Philippine Act's provisions with respect to the processing of that data. In this way, Philippine outsourcing service providers and their clients are reassured that the Act will not disrupt their outsourcing activities by adding another and possibly conflicting layer of regulation.[3]

We think this issue can be easily addressed by issuing a clarification or legal guidance that confirms that foreign organizations that outsource their foreign data processing to service providers located in Singapore or otherwise use Singapore data intermediaries would not be subject to the Act's provisions with respect to the processing of their data in Singapore. Such clarification would provide welcome reassurance to companies and would thus encourage the growth of the outsourcing and IT sector in Singapore.

[3] See Section 4 of the Data Privacy Act of 2012, available at http://www.gov.ph/2012/08/15/republic-act-no-10173. In particular, Section 4 states: " This Act does not apply to …(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines."