American Express
Public Consultation of the Proposed Consumer Data Protection Regime for Singapore

Date : 30th April 2012

American Express International Inc.
Mapletree Business City
#08-00 Block C20 (West)
Pasir Panjang Road
Singapore 117439

Joanne Tay, Senior Manager, Compliance & Ethics
☎ 65-6317-6206 | ✉ joanne.p.tay@aexp.coms

Table of Contents

1. Introduction

We refer to the public consultation paper on the proposed Consumer Data Protection Regime for Singapore and thank you for the opportunity to share our feedback.

American Express International, Inc. ("Amex") conducts various businesses in Singapore such as consumer and corporate cards issuance, merchants acquisition and servicing, distribution of insurance products, sale of traveler cheques, provision of money-changing, remittance and other travel-related services. With our range of product and service offering, Amex has multiple touch points with individual consumers and corporate customers.

Being a reputable global company, Amex respects and upholds the privacy of our customers in our day-to-day business dealing and we welcome the proposal by the Ministry of Information, Communications and the Arts ("MICA") for a new Consumer Data Protection Regime in Singapore. Below is a summary of our feedback on the proposed regulatory requirements with details of each feedback in the document enclosed.

2. Feedback to MICA

2.1 Consent

(a) Consent provided to a specific business unit in an organization

- We would like to seek clarification in respect of consent obtained by a data user who is an organization with several business units providing different types of services.
- For example, if a customer or potential customer gives explicit consent to one business unit in an organization to use his personal data, can a different business unit in the same organization rely on that consent?

(b) Type of consent which must be obtained

- We would like to seek clarification on the specific forms of consent which the data user is required to obtain.
- Are any or all forms of consent set out below acceptable to comply with the PDPA?
  i) verbal,
  ii) in writing,
  iii) in writing and signed by the individual or authorized representative of an organization, as applicable, or
  iv) by conduct – for example, the provision of a name card during a promotional event by Amex.

2.2 Business Contact Information

- We support the view of excluding business contacts, but we would like to seek clarification on the meaning of "business purpose".
- Does contacting a person via his business contact to promote a retail product for the business constitute a business purpose?
- We assume that, contacting a person via his business contact to promote a consumer product i.e consumer credit card (versus a corporate product i.e corporate card) would not constitute a business purpose and hence would require specific consent from the customer.

2.3 Personal Data from a Third Party

- We would like to seek clarification in respect of two things:-

(a) Where the data user obtains personal data from a third party, can the data user rely on a contractual undertaking from the third party that (i) consent was obtained, and (ii) data was obtained for a purpose agreed to by the data subject?

(b) How far does the receiving organization need to go in ensuring that the third party has complied with the PDPA when obtaining the personal data?

- It would be very onerous for the data user if required to take additional steps to verify and ensure that the third party who is providing the data has previously complied with the PDPA. We would like to seek guidance on the expectation to comply, and the steps which a data user is required to undertake in order to comply with the following sections:-

(a) "The organisation possessing the data would have to ensure that the collecting organisation's purposes are in accordance with what the individual consented to. Similarly, the collecting organisation would have to ensure that the organisation from which it collects the personal data is permitted to disclose it under the PDPA. The PDPA will permit individuals to check with the organisation possessing the data to determine which organisations the data has been disclosed to, and approach the latter to withdraw consent if he wishes. (CP 2.83) "

(b) "On or before collecting personal data about an individual from another organisation without the consent of the individual, an organisation shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (Bill, 22(2))"

2.4 Do-Not-Call ("DNC") Register

- We would like to seek clarification on the "30 day prior to" period specified to check the DNC register.
- For example, if a telemarketer calls customer on the T+30 day (T being the date the data user runs a check on the DNC) and the customer requests for the telemarketer to call the customer back on T+35 day. For the follow up call, does the data user still require to check the list again before calling? Or does the customer's request for follow up call from the data user constitute consent and the data user does not then again require to check the DNC register?
- Hence, we would like to propose the validity of the screened list to be 60 days instead of 30 days.

2.5 Consequences of Withdrawal of Consent

- We would like to seek clarification on the communication to an individual of the consequences for withdrawal of consent by the same individual.
- Would it be sufficient for an organization to set the consequences out clearly in the Terms and Conditions of the service which will be provided to the individual? This will mean that the individual concerned will be notified of the consequences of withdrawal **prior to** withdrawal. Does the data user have to communicate the consequences again at the point of withdrawal?

2.6 Failure to Opt-out Is Not Deemed As Consent

- We would like to seek clarification around whether this section mandates that a data user must obtain positive affirmation from the individual whether he wishes to opt out or not.
- For example, if a form sets out a check-box for the individual to select, should he wish to opt-out of a specified data use (eg. marketing) and he fails to select the option, does this mean the data user cannot deem that the individual has consented to use of his data for marketing?

3. Summary of Major Points

With our range of product and service offering and the multiple touch points that Amex has with individual consumers and corporate customers; we would like to seek clarifications on the use of and type of consent, the context of consent in business contact information, our responsibilities with regards to third party, proposal of extension of validity period of screened list from the DNC register, clarification on informing individuals of their consequences of withdrawal of consent and clarity of failure to opt-out is not deemed as consent.

4. Conclusion

We appreciate your consideration and look forward to your advice and clarification. If you need any additional information, please contact us at the following email addresses.

Joanne Tay
Senior Manager, Compliance & Ethics
☎ 65-6317-6206 | ✉ joanne.p.tay@aexp.com

Annabell Koh
Senior Analyst, Compliance & Ethics
☎ 65-6317-6035 | ✉ annabell.koh@aexp.com

Aik-Hwee Ooi
Compliance Analyst, Compliance & Ethics
☎65-6317-6336 | ✉ Aik-Hwee.Ooi@aexp.com