cepts
apore

Contact person:

Vivianne JABBOUR

vivianne.gordon-pullar@sap.com

Azmeen MOIZ

Azmeen.moiz@sap.com

Beautrice WONG

beautrice.wong@sap.com

The Best-Run Businesses Run SAP®

SAP Asia Pte Ltd, based in Singapore, operates in 12 countries and has a presence in 20 countries across Asia Pacific Japan. With a 24-year history, SAP Asia provides its 23,000 customers and 1,100 partners with the most advanced business software and software-related services including applications, analytics, mobile, database and technology, SAP HANA, and cloud solutions. In 2012, SAP Asia delivered exceptional 22% YOY growth and €2.24-billion revenue in software and software-related service. The company currently employs more than 13,000 people in the region.

SAP Mobile Services, a division of SAP, is a global leader in mobile interconnection and mobile consumer engagement services. It provides mobile operators with unparalleled capabilities in global messaging interconnect, data roaming and an array of IPX-based services and enables enterprises to engage with their consumers through innovative mobile marketing and communication solutions.

SAP Mobile Services helps businesses process 1.8 billion messages per day, reaching more than 980 operators and 5.8 billion subscribers across 210 countries.

1: Summary of Major Points

SAP Asia Pte Ltd and SAP Mobile Services (collectively "SAP") wholeheartedly support the introduction of a formal system of data protection in Singapore and thank the PDPC for the opportunity to provide comments in relation to the Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act in Singapore. We are encouraged by the PDPC's approach to implementation of the PDPA and have found the Consultation Sessions helpful in clarifying our understanding of the intentions of the PDPA and the PDPC. We have only some comments to make in relation to the draft Advisory Guidelines that have been issued by the PDPC and these are set out in this document.

SAP takes its data protection obligations towards its employees, customers, clients and third parties with whom it deals extremely seriously and has many internal mechanisms and systems already in place which are actively promoted within our organisation in order to achieve as high a standard of data protection and awareness as possible.

We also operate within an extremely fast moving and technologically advanced space which constantly challenges norms and presumptions and requires regular reassessment of our own practices and policies. It is important to weigh the practical commercial needs of a multi-national technology based company with the important requirement to deliver high standards of data protection.

We thank the PDPC for the opportunity to provide comments in relation to the Advisory Guidelines on Key Concepts in the Personal Data Protection Act (PDPA).

In our Mobile Services business, we act as a conduit for our customers, passing SMS messages between sender and recipient and while we are given access to mobile phone numbers so that we can deliver the messages, we are consciously given no access to any other identifying information with that message.

As a blind conduit for messages, we believe that the mobile phone numbers we hold are not capable of classification as "personal data" and that we both qualify as "telecommunications service providers" for the purposes of the Do Not Call Registry and "network service providers" for the purposes of the Electronic Transactions Act.

Of course, we accept that, as regards our own internal personal data concerning employees, we are fully bound by the PDPA.

2. Comments

2.1 The Definition of Personal Data

a. We note that paragraph 5.10 refers to "mobile telephone number" as personal data.

b. We note that data may be considered personal data if it is possible to identify an individual by combining certain data with other data to which the organisation has or is likely to have access.

c. SMS messaging service providers (who provide the conduit through which messages are sent but have no control over the content or initiation of the sending of the message), neither have, nor have access to, the information required to match an anonymous mobile phone number to an individual.

d. The data required to match names to phone numbers and hence create personal data, are held by the originator of the message who is effectively the data controller.

e. While the mobile phone number will constitute personal data while held by the data controller, we submit that it ceases to be so when sent, in an already anonymised state, to the SMS messaging service provider.

f. Furthermore, the data required to combine names and mobile phone numbers and render them personal data are not only created, collated and managed by the originator, the data controller, but are also generally seen to be its proprietary and confidential information. Access to this confidential information is carefully guarded by the originator of the SMS.

g. In order to protect the integrity of the technology and network as well as to meet their contractual obligations, the security surrounding our SMS messaging networks is sufficiently robust as to repel a "motivated intruder". Anyone breaking through this security to access numbers would be more than a "motivated intruder".

We propose that the definition in the Advisory Guidelines of a mobile phone number as personal data be expanded upon in order to clarify that in the circumstances described above, where an SMS messaging service provider transmits an SMS, a mobile phone number alone, incapable of being matched to any other lists of data from the originator, is not personal data for the purposes of the PDPA.

2.2 Network Service Providers

a. We note that the PDPA amended the Electronic Transactions Act (Cap 88) ("ETA") to provide that network service providers are exempt from the provisions of the PDPA insofar as a network service provider permits transmission of "third party material in the form of electronic records to which he merely provides access".

b. The term "network service provider" is not defined in either the Electronic Transactions Act or the PDPA although the Intellectual Property Office of Singapore defines it as an organisation that "provides internet access services and facilities for communication across networks".

c. We submit that an SMS messaging service provider whose business is to transmit messages between parties through the networks run and managed by the SMS messaging service provider as a blind conduit, qualifies as a "network service provider" for the purposes of the ETA and therefore is exempt from the scope of the PDPA in respect of those areas of its business that fall within that definition.

We seek clarification on the definition of "network service provider" and whether an SMS messaging service provider would, for the reasons set out above, fall within that definition.

2.3 The Do Not Call Register

a. We note that the "sender" of a message is responsible for complying with the DNC Provisions.

b. We reiterate our comments made in previous consultation exercises held by the IDA and the PDPC that SMS messaging service providers are mere conduits in that:

i. SMS messaging service providers do not initiate messages[1]. It is the originators of the message who decide to which mobile phone numbers the message should be sent and who ultimately make the decision to initiate the sending of the message. The fact that an SMS messaging service provider automatically initiates a transmission at the request of a third party does not mean that that SMS messaging service provider has initiated the transmission.

ii. SMS messaging service providers do not select the receiver of the message[2]. SMS messaging service providers do not create, collate, or manage the mobile phone number lists. These lists are created, collated and managed by the originator of the message. In fact, the originator of the list usually regards such lists as its proprietary and confidential information.

iii. SMS messaging service providers do not select or modify the information contained in the message[3]. SMS messaging service providers do not create the messages themselves nor do they determine what the content of the messages should be – they merely send on messages received from their clients, the originators.

c. We welcome statements made by the IDA and the PDPC at the Industry Briefing on 22 February 2013 that to be a "sender" of a message for the purposes of the PDPA there must be some pro-active participation in the sending of a message and that an SMS messaging service provider who merely acts as an intermediary, neither initiating the sending of the message, nor controlling who the recipient of the message is, nor the content of the message, will not be classified as a "Sender" for the purposes of the PDPA. We note the clarification in paragraph 30.1 of the Guidance.

d. We welcome the declaration made by the IDA and the PDPC at the Industry Briefing on 22 February 2013 that holders of an SBO licence would be classified as a telecommunications service provider for the purposes of Paragraph 30.1(a) of the Guidelines.

e. An SMS messaging service provider, while an SBO licence holder and therefore a telecommunications services provider for the purposes of Clause 36(2), does not necessarily have details of terminated Singapore numbers and therefore compliance with Clause 42 of the PDPA is unlikely to be possible.

[1] See also EU Council Directive 2000/31, 2000 O.J. (L178)3, at article 12(1)(a)
[2] See also EU Council Directive 2000/31, 2000 O.J. (L178)3, at article 12(1)(b)
[3] See also EU Council Directive 2000/31, 2000 O.J. (L178)3, at article 12(1)(c)

We propose that the fact that an SMS messaging service provider is not, for the purposes of the PDPA, a "sender" of messages and is therefore not subject to the provisions of the Do Not Call Registry should be reproduced in the Guidelines so as to introduce certainty on this point.

3. Conclusion

In conclusion, SAP is keen to support the current data protection initiatives and to make the new statutory system of data protection as practically functional as possible, balancing the realities of certain technology-based business models with the needs of the public whose data requires protection. The singularities of our business, and the technology it utilizes, raise certain very particular concerns and considerations which we have elaborated upon above.

SAP Asia Pte Ltd. (Regional SAP Headquarter)
30 Pasir Panjang Road
#03-32, Mapletree Business City
Singapore 117440

www.sap.com