SYBASE 365
MOBILE SERVICES

PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

25 OCTOBER 2011

RESPONSE TO CONSULTATION PAPER ISSUED BY MINISTRY OF INFORMATION AND THE ARTS

Contact Persons

DEREK HO
derek.ho@sybase.com

BEAUTRICE WONG
beautrice.wong@sybase.com

Part I: Introduction - Sybase

Sybase, an SAP® company, is an industry leader in delivering enterprise and mobile software to manage, analyze and mobilize information. We are recognized globally as a performance leader, proven in the most data-intensive industries and across all major systems, networks and devices. Our information management, analytics and enterprise mobility solutions have powered the world's most mission-critical systems in financial services, telecommunications, manufacturing and government. For more information: http://www.sybase.com (http://www.sybase.com/) . Read Sybase blogs: blogs.sybase.com (http://blogs.sybase.com) . Follow us on Twitter at @Sybase (http://www.twitter.com/sybase\t_blank) and @MobileWork (http://www.twitter.com/mobilework\t_blank) .

Sybase, through its Sybase 365 division, is the global leader in enabling mobile information services for mobile operators, financial institutions and enterprises. We provide our customers with the widest offering in SMS, MMS, GRX, IPX interoperability, end-to-end mobile commerce solutions, innovative mCRM, mobile marketing and content delivery services. Sybase 365 processes more than 1.5 billion messages per day, reaching 900 operators and 4.5 billion subscribers around the world. For more information, visit:www.sybase.com/365. Read our blogs: http://blogs.sybase.com

Part II: Summary of Major Points

The following is a summary of the major points raised by Sybase:

a) The definition of "personal data" should be clarified to discuss whether expressions of opinion would be covered.

b) Personal data of the deceased should not be covered by the proposed DP law.

c) The proposed DP law should make a distinction between data controller and data processor.

d) We have suggested some additional exceptions which should be included in the proposed DP law in relation to the rules on collection, use, disclosure, and data subject rights.

e) The proposed DP law should not legislate a specific time period with regards to the retention of data.

f) When an appeal is made to the Appeals Board, any orders made by the DPC should be stayed until the determination or withdrawal of the appeal.

g) The financial penalty of $1 million is too high and should be reduced. The power to impose financial penalties should only be exercised if the breach of the proposed DP law was deliberate or where the breach was likely to cause substantial damage or distress.

h) A two year “sunrise” period would be appropriate.

i) We are of the view that a Do-Not-Call registry would not be necessary given the combined operation of the proposed DP law and the existing Spam Control Act.

Part III: Specific Comments

Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?

We note that the definition of personal data does not expressly refer to expressions of opinion about an individual (unlike the UK Data Protection Act). Although it could be argued that the words "information about" in the proposed definition of personal data covers such expressions of opinion, we are of the view that for clarity and certainty, it should be clarified whether such expressions of opinion would be covered under the ambit of personal data. For example, these may include internal company discussions about prospective job applicants, or internal disciplinary findings.

The potential breadth of the definition of personal data could also extend to information which does not relate directly to the individual but which describes activities which the individual engages in. For example, traffic data which is linked to the phone number could arguably fall within the ambit of the definition, and thus be subject to the obligations of retention and processing. However, telecommunications licensees would need to process, store and exchange such traffic data for settlement of transit and interconnection charges, or for handling end user disputes. We suggest a similar concept as that contained in section 7(2) and 8(3) of the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 be considered in the context of drafting the proposed DP law.

Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?

We are of the view that personal data of the deceased should not be covered by the proposed DP law. It is not clear what interests the proposed DP law would be trying to protect in relation to a deceased person's personal data. Information which is related to a deceased person is already protected under specific legislation (e.g. medical records are protected under the Private Hospitals & Medical Clinics Act).

Further, a number of countries in their implementation of data protection laws (e.g. Hong Kong, Australia, the United Kingdom) only protect the personal data of living individuals. We note that even the voluntary Model Data Protection Code for the Private Sector that was introduced in Singapore only covers personal data of living individuals.

We note also that the National Internet Advisory Committee Legal Subcommittee in its Report on a Model Data Protection Code for the Private Sector was of the view that "the data subject must be a *living* individual, as it would be too complex to extend regulation to the estates of deceased persons."[1]

[1] See Report on a Model Data Protection Code for the Private Sector, page 30 at http://www.agc.gov.sg/publications/docs/Model_Data_Protection_Code_Feb_2002.pdf

Question 10: Do you have any views / comments on the proposed general rules under the DP law?

We note that the proposed DP law will not make a distinction between data controllers and data processors. We believe that this approach will not reflect the practical and commercial reality which some outsourcing service providers operate in. We suggest that the proposed DP law include a distinction between data controller and data processor.

The distinction between data controller and data processor is important as it reflects that the data processor is processing data *on behalf* of the data controller. It also accurately allocates responsibility to the entity that *factually* has control over the data, and how data subjects will be able to exercise their rights in practice.

We note that paragraph 3.29 of the Consultation Document suggests that an entity that processes personal data on an outsourced basis is likely to be deemed to have control over the personal data. We are of the view that it would not be accurate to make such an assumption. In respect of the data processor, the "control" which the data processor supposedly exercises is in large part determined by the data controller (that is, the relationship between the data controller and the individual, and the manner in which the personal data is collected by and provided by the data controller to the data processor). The purpose for which the personal data is collected and processed may also be determined and controlled by the data controller.

Further, the exercise of the rights of the data subject to information access, rectification, deletion and blocking make sense in relation to the data controller and not the data processor (as the data subject does not have any knowledge of or relationship with the data processor). It would be the data controller who then informs the data processor to take the necessary actions, and enforce those actions (if necessary) through contract. In relation to the obligation to ensure accuracy, the data processor may not be able to determine or verify accuracy as the information is collated and passed from the data controller.

A failure to distinguish between data controller and the data processor would result in entities being responsible for obligations which they are unable to control both commercially and practically. In the majority of outsourcing arrangements, the outsourcing service provider does not have any direct contact with the individual (and in some situations are prohibited from contacting such individuals directly). It is the outsourcing service provider's client that owns the customer relationship and obtains the necessary consents. The outsourcing service provider therefore does not obtain the individual's consent, and has to rely on the efforts of its client who owns the end-customer relationship.

Other data protection regimes recognize this distinction. For example, section 2(12) of the Hong Kong Personal Data (Privacy) Ordinance states that a person is not taken to be a data user if he holds, processes or uses personal data solely on behalf of another person, and not for any of his own purposes[2]. A practical illustration of this distinction would be telecommunications services provided to a banking institution. A banking institution sending a short message to an individual customer through a telecommunications service

[2] We note that Hong Kong will not be imposing additional regulatory obligations directly on data processors as mentioned in the Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance, October 2010

provider would have provided the mobile number to send the message to and the content of the message (e.g. name or account details). The banking institution would also have obtained consent for sending the message to the individual customer, and determined the purpose of that sending. The telecommunications service provider in providing the transmission service, merely processes that delivery information and sends the message to the end user. It cannot be said that the telecommunications service provider would be the data controller in that scenario. This position is consistent with the position taken in Recital 47 of Directive 95/46/EC of the European Parliament and of the Council wherein it is stated that

> "… *where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service"*

Making a distinction between the data controller and a entity that processes data on behalf of the data controller would also be consistent with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which excludes the following from the concept of data controller: (i) data processing service bureaux which carry out data processing on behalf of others, and (ii) telecommunications authorities and similar bodies which act as mere conduits. We note that Consultation Document (in paragraph 3.6) had acknowledged that it was important to ensure consistency with international standards such as the OECD Guidelines.

It is important that the proposed DP law recognises the factual reality in which entities operate in. Whether a service provider would be determined as a data controller or data processor would be a factual determination. So, for example, the telecommunications service provider providing transmission services in our example above could be a data controller if it uses the personal data transmitted over its network for its own marketing purposes, or has collected personal data by its own efforts (e.g. its subscribers' personal data).

In order to ensure that data protection standards are maintained, it is suggested that similar safeguards of mandating that the data processor processes data only on the instructions of the data controller, and ensuring that there is a contract relating to security measures between the data controller and data processor (see Articles 16 and 17 of Directive 95/46/EC), can be imposed. This would also be consistent with the approach taken by Hong Kong in requiring data users to use contractual or other means to ensure that its data processors and sub-contractors, comply with the Personal Data (Privacy) Ordinance[3].

[3] Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance, October 2010, at page 39

Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?

We note that there would be an exception to the restriction on collection, use and disclosure where it is reasonable for investigation or legal proceedings (see paragraph 3.42 read together with paragraphs 3.50 and 3.52 of the Consultation Document). We suggest this should be expanded to allow for use and disclosures where it is necessary for establishing, exercising or defending legal rights. The words "legal proceedings" may not extend to the pre-claim stage where information may need to be disclosed in response to initial allegations or demands, or where analysis needs to be done to determine whether legal rights or obligations exist. We suggest that the wording in section 35(2) of the UK Data Protection Act be taken into consideration, and be adapted accordingly. We note that a similar exception has been accepted in Hong Kong[4].

The proposed DP law should also contain an exception which allows for collection, use and disclosure where such requirements are imposed by or under any written law or by an administrative direction of a relevant regulatory authority.

Question 14: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?

We suggest that the proposed DP law states that the obligation to erase or delete personal data be regarded as complied with if the data controller can prove that it has taken reasonably practicable steps to erase such personal data.

Question 15: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?

We are of the view that organizations should not be required to specify the retention period when collecting personal data. As acknowledged in paragraph 3.67 of the Consultation Document, the question of what would be the appropriate retention period is a multi-faceted one. It depends on the purposes for which it was obtained and the nature of the information, and the context of its future use.

For example, if a customer relationship ends, an organization may not need to keep information about the individual for marketing purposes, but may continue to retain the individual's personal data to deal with any complaints or claims relating to the service which was provided. Hence, the retention period may not only be determined at the point at which the information is collected but may be re-evaluated at the end point of the relationship with the individual.

[4] Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance, October 2010, Proposal 31 at pages 104 to 105

Given the dynamic transactional nature of interactions between organizations and individuals, the retention period should be evaluated upon and determined by the organizations during the course of its retention. A requirement to specify the retention period up-front may also lead to the unintended consequence of organizations pushing the boundaries of such retention periods as they would want to keep the data as long as possible.

Question 16: Do you have any views / comments on the proposed rules on access to and correction of personal data?

A further exception should be added relating to negotiations where the application of the information request may likely prejudice the negotiations (see paragraph 7 of Schedule 7 of the UK Data Protection Act).

Question 17: Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?

We note that the Consultation Document states that the DPC may refuse to conduct investigations or reviews in certain circumstances (e.g. if the complaint is frivolous or vexatious). While this is a welcomed statement of intent, we would like the DPC to provide guidance (before the expiration of the sunrise period) on how it will determine whether a complaint is frivolous or vexatious when it first receives such a complaint (i.e. "the refusal to conduct"). We believe that the more likely outcome is that the DPC will still require the organization to respond to the allegations made by the individual. This would still mean that the organization would still need to respond (under timings specified by the DPC) to investigations or information requests based on complaints which ultimately turn out to be frivolous or vexatious. This will pose a real cost to organizations (the expenditure of time and resources) which have to deal with such complaints.

We suggest that it should be made clear that in the event that an appeal is made to the Appeals Board, any orders made by the DPC should be stayed until the determination or withdrawal of the appeal.

Further, it should be made clear that the time period for fulfilling those orders should not be shorter than the period specified for filing an appeal. This is currently the position in section 50(4) of the Hong Kong Personal Data Privacy Ordinance.

Question 18: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?

We are of the view that the amount of up to S$1 million is too onerous and is considerably higher than the financial penalty amounts that can be imposed by data protection regulatory authorities in other data protection regimes. For example, financial penalties that may be imposed under the Hong Kong Personal Data Privacy Ordinance range from HKD10,000 to HKD50,000. It should also be noted that the Hong Kong will not be (i) implementing the proposals to make contraventions of the data protection principles as offences, and (ii) imposing monetary penalties on serious contraventions of data protection

principles[5]. The Australian Privacy Act 1998 also specifies monetary amounts for specific offences but the amounts do not come close to S$1 million.

Further, we suggest that the proposed DP law expressly mentions that financial penalties will be used in serious situations only. In that regard, the power to impose financial penalties should only be exercised if the breach was deliberate or where the breach was likely to cause substantial damage or distress (see section 55A of the UK Data Protection Act).

Question 20: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate?

We are of the view that a two year "sunrise" period would be appropriate.

Question 23: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?

We are of the view that a Do-Not-Call registry would not be necessary given the combined operation of the proposed DP law and the existing Spam Control Act 2003.

The experience abroad with Do-Not-Call registries suggests that the benefit of Do-Not-Call registries is not conclusive. There have been reports that suggest that Do-Not-Call lists actually result in more unwanted calls[6]. This can result as spammers can obtain those lists themselves by registering to receive those lists, and can avoid prosecution as they can be based off-shore with various means of contacting individuals within Singapore[7]. Implementation of Do-Not-Call registries can also be complicated and results in legitimate businesses being excluded. For example, the National Do-Not-Call list implemented in India which only identifies messages sent by certain business sectors as being transactional messages which can be sent within a 9pm to 9am blackout period.

Further, individuals may also remember that they had signed up on the Do-Not-Call registry, but forgot the other instances where they had individually consented to receiving calls or messages. This would result in both confusion and unnecessary cost to organizations in dealing with frivolous allegations and complaints.

---

[5] Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance, October 2010, pages 133 to 140

[6] http://www.cbc.ca/news/technology/story/2009/01/23/donotcall.html

[7] The Commercial Affairs Department website (see http://www.cad.gov.sg/serv/pre/cri_pre_adv/Boiler-Room+Scams+or+Cold+Call+Investment+Scams.htm) contains a description of how such operations can work

SYBASE (SINGAPORE) PTE LTD
438A ALEXANDRA ROAD
#08-10
ALEXANDRA TECHNOPARK
SINGAPORE 119967

www.sybase.com

SYBASE®