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 & technology, SAP HANA, and cloud solutions. In 2012, SAP Asia delivered exceptional 22% YOY growth and €2.24-billion revenue in software & 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 statutory system of data protection in Singapore and thank the PDPC for the opportunity to provide comments in relation to the Proposed Regulations on Personal Data Protection 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 Proposed Regulations 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 recognise that the majority of the requirements set out in the PDPA and the proposals presented for discussion in the draft Regulations meet generally accepted international norms. Our comments reflect particularly on those proposals relating to Part III, the Transfer of Personal Data outside Singapore.

We seek to ensure commercial practicality as well as to promote a globally cohesive approach to data protection which, as Cloud technologies bring the world ever closer, we feel is essential. We advocate the introduction of the notion of "adequacy" as adopted in the EU in permitting certain cross-border transfers of personal data. We believe that the PDPA should recognize the data protection regimes of such well-developed jurisdictions as the European Economic Area by permitting transfers of data to them with no restrictions, as an accepted derogation from the general rule that data transfers outside of Singapore are forbidden, as set out in Clause 26 of the PDPA.

We also believe that data subjects should be afforded some degree of personal choice and control over their data by being permitted to consent to the transfer of their data outside of the jurisdiction, so long as such consent is fully informed and freely given.

2: Comments

2.1 Transfer of Personal Data outside Singapore

We agree with the OECD who, as far back as 2006 and before the advancement of Cloud, stated that developments in global communications networks and business processes have increased the volume of cross-border data flows. These data flows, which are so integral to the efficient functioning of multi-national corporations and international trade, have become an integral part of the global economy. As technological developments and globalization continue, cross-border data flows also increase.

We agree that it is conceivable that the increased global data flow could also bring with it an increased risk to the security of personal data, although we are reassured that so many countries have now implemented stringent data protection laws, most following the OECD and EU standards of data protection, that protect personal data held in or, often, transiting through, their jurisdictions. While the differing laws are not entirely uniform, the standards of protection remain nonetheless high. This affords a great deal of comfort to data subjects and conscientious data controllers and data intermediaries who wish to ensure the security of the personal data for which they are responsible as well as facilitating the commercial business of their organisation.

We welcome the fact that the PDPA will monitor cross-border data flows and agree that binding corporate rules are an excellent mechanism for ensuring the protection of data. We also see the benefit of contractual arrangements to achieve this security in certain circumstances but are conscious that questions of privity as well as the process of enforcement of such legal agreements may not promote the timely adherence to high standards of data protection which should otherwise apply.

We suggest that the PDPC should recognize the high level of statutory data protection controls that exist throughout the world today by introducing the notion of “adequacy” to the controls on cross-border data flows. As such, transfers of data to certain countries deemed to have an “adequate” level of protection for personal data would be permitted without the need for either contractual arrangements or binding corporate rules. This would mirror procedures already in place in the UK, for example.

We have seen the EU utilize the notion of “adequacy” to great effect in allowing cross-border transfers of data and this is noted in the consultation document. We believe that while contractual arrangements can be of benefit to promote the protection of personal data that has been transferred out of the jurisdiction to less secure environments, questions of privity (discussed further under 2.2 herein), enforcement and policing is best conducted by regulatory authorities in their home jurisdictions and we also note that the level of data protection compliance in countries deemed to be “adequate” is high.

Mirroring the EU, countries deemed by the PDPC in Singapore to have "adequate" controls could initially be members of the EEA, countries deemed adequate by the EU[1] and signatories to the Safe Harbor Scheme. These countries in any event impose stringent data protection controls with which data controllers and data processors must comply.

This would not only reduce the administrative burden on, and therefore be of significant practical benefit to, companies operating in Singapore, but it would also have the benefit of aligning Singapore to the EEA countries as well as Switzerland and, in some regards, the USA.

2.2 Contractual Protections

We note that contracts containing "appropriate safeguards" may be used to authorize the cross-border transfer of data between companies; however we do have concerns that this may not, in itself, be the most practical or secure solution to ensure the protection of data. Modern technologies and business processes often require data to be transferred between a number of parties. Once the data are transferred by the original data controller, albeit under a suitable contract, that data controller has a reduced ability to enforce against future recipients of the data, or indeed to ensure that those recipients enter into similar contracts.

It is a matter of law that the data controller may only enforce such provisions against parties with whom it has directly contracted. For reasons of privity of contract, enforcement of the contract against a company that is not a party to it is not possible. As such, Clause 7.9 of the proposed Regulations should be clarified to recognize that enforcement is at best only possible against those recipients who not only receive the personal data under the contract but, by virtue of being a party to it, are also directly bound by that contract.

Inter-company transfers of personal data out of the jurisdiction would be best secured through a system of data subject consents, supported by contractual arrangements, as well as the concept of adequacy which would then also place reliance for enforcement on local data protection authorities – most likely those same authorities with whom the PDPC envisages entering into "Co-operation Agreements" mentioned under Clause 10 of the PDPA - who are experts in the field of enforcement and monitoring of data protection abuses in their own jurisdictions.

2.3 Consent as a derogation

A number of countries[2] also allow clear and informed consent as cause for derogation from the fundamental rule against cross-border data flows. We believe that this allows individuals the chance to determine the fate of their own data. We propose that the derogation for consent be accompanied by a requirement that the consent be freely given and that the data subject be

[1] Currently, Andorra, Argentina, Australia (in certain specified cases), Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Jersey

[2] For example, Australia, Argentina, Belgium, Hong Kong, UK

fully informed not only of the risks of any potential data flow outside of the jurisdiction but also of the consequences of withholding consent. This consent should be in acknowledgement that personal data may be transferred out of the home jurisdiction to countries where the statutory standards of data protection do not match the home jurisdiction. While we strongly believe that modern developments in technology, in particular the advance of "Cloud", precludes the specifying of particular destination countries in this consent and that the consent given should be generic, we do believe it remains reasonable for the data controller to undertake to take all reasonable steps to ensure the continued security of the personal data. This not only empowers individuals in an age where awareness of data protection is elevated but it also recognizes that technology is increasingly blurring international boundaries and data subjects are increasingly prioritizing access to technologies over the safeguarding of their own personal data. For technologies such as Cloud, the cross border transfer of data is a fundamental facet of the business and technological model.

We respectfully request that the following derogations be introduced regarding restrictions on cross border data flows:

1. No restriction on transfers to countries that have an adequate level of protection (being at least EEA members, EU approved countries and signatories to the Safe Harbor Scheme).
2. Data subjects should be permitted to consent to the transfer of their data out of the jurisdiction, provided such consent is fully informed and freely given.

We also request that the matter of privity of contract and enforcement of contracts governing cross-border data flows be clarified.

3. Conclusion

In conclusion, SAP is supportive of the PDPA and of the PDPC's implementation initiative.

We recognize that business processes today are closely intertwined with technological advances and an increasing globalization of data flows. That in large part results from demands from consumers for those services that can only be delivered through the synergies that come from cross-border data flows. We recognize that those demands for cross-border data flows must be reconciled with the perceived threat to the security of personal data and we support achieving this in a manner most equitable to individuals, business and privacy needs.

As such, our comments and suggestions above represent an effort to achieve workable controls and obligations.

We would respectfully request that the PDPC gives consideration to our suggestions which are intended to maintain a high standard of data protection (in keeping with SAP's already existing policies) while allowing multi-national, technology driven, businesses to thrive.

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

www.sap.com