PDPC'S CLOSED CONSULTATION

ON

PROPOSED APPROACHES FOR COMPLYING WITH THE TRANSFER LIMITATION OBLIGATION FOR CLOUD SERVICES

COMMENTS

FROM

BSA | THE SOFTWARE ALLIANCE

13 JULY 2018

Contact:
Darryn Lim,
Director, Policy - APAC
darrynl@bsa.org
300 Beach Road, #25-08 The Concourse, Singapore 199555

PDPC'S CLOSED CONSULTATION ON PROPOSED APPROACHES FOR COMPLYING WITH THE TRANSFER LIMITATION OBLIGATION FOR CLOUD SERVICES
– COMMENTS FROM BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance ("**BSA**")[1] appreciates the opportunity to comment on the Closed Consultation on Proposed Approaches for Complying with the Transfer Limitation Obligation for Cloud Services issued on 13 June 2018 (the "**Consultation Paper**") by the Personal Data Protection Commission ("**PDPC**").

A. INTRODUCTION AND STATEMENT OF INTEREST

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members include several cloud services providers ("**CSPs**") who are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, artificial intelligence and the Internet of Things. Our members remain deeply committed to protecting personal data in order to foster trust among businesses and consumers and to reap the benefits of new technologies.

Data-driven innovation, enabled by cloud computing, powers the global economy and enhances the positive effect of cutting-edge technologies. Policies that create an environment conducive to cloud computing will produce significant, positive results as these new technologies evolve. It is therefore crucial that regulators such as the PDPC continue to strive to create an environment that favors the continued development and deployment of cloud computing so that these technologies can continue to promote societal benefits and economic growth.

BSA has worked closely with governments around the world in relation to national personal data protection policies and also publishes the annual Global Cloud Computing Scorecard.[2, 3]

B. COMMENTS ON THE CONSULTATION PAPER

BSA commends the PDPC for its ongoing efforts to review the relevance of the Personal Data Protection Act ("**PDPA**") to the modern digital economy. The success of cloud computing depends on users trusting that their information will not be used or disclosed in unexpected ways, and the right legislation can help create this environment of trust. At the same time, to maximize the benefit of cloud, CSPs and their customers must be free to move data through the cloud in the most efficient way. BSA sets out below our comments and recommendations on the proposed framework in the Consultation Paper.

---

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Mathworks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] The 2018 BSA Global Cloud Computing Scorecard is available at http://cloudscorecard.bsa.org/2018/index.html.

[3] We have also incorporated our learnings from working with governments around the world into our BSA Data Protection Principles, which can be found at http://bit.ly/BSA-Data-Protection.

B1. Further clarity needed on the purpose and scope of the proposed framework

BSA welcomes further dialogue on the PDPC's motivation behind the proposed framework. BSA stands ready to contribute whatever constructive inputs are necessary to reach desired outcomes sought by the PDPC. However, the current Consultation Paper is not clear as to what concerns the proposed framework seeks to address. To the extent that there are concerns about the protection of personal data transferred overseas, the existing framework is sufficient to manage the risks involved (please also see our reasoning in section B2 below). The proposed framework, which adds another layer of responsibility and review, will increase the challenges in administering the PDPA for courts and the Singapore government, whereas now the interpretation and enforcement of the PDPA seem fairly straightforward. Costs are likely to rise for CSPs, the government, and ultimately consumers. It is not clear what benefit the proposed framework would bring that would make these costs worthwhile. BSA therefore requests that the PDPC provide further details on why the proposed framework would be required and how it would improve the protection of personal data.

BSA also requests that the PDPC clarify whether the proposed framework is intended to extend the Transfer Limitation Obligation to all data intermediaries, or only to CSPs. Should the PDPC's intent be to extend the proposed framework only to CSPs, BSA would appreciate further clarification from the PDPC on why CSPs have been identified for unique regulatory treatment vis-à-vis other data intermediaries, and how the PDPC proposes to distinguish CSPs from other data intermediaries.

B2. The Transfer Limitation Obligation should not be extended to data intermediaries

Having reviewed the Consultation Paper and gathered feedback from our members, BSA recommends that the obligations under section 26(1) of the PDPA (the "**Transfer Limitation Obligation**") not be extended to data intermediaries under the PDPA, even in the limited case of data intermediaries that are CSPs in Scenario B of the Consultation Paper, for the reasons set out below.

a. The proposed approach would be out of step with international principles and risks undermining the accountability model.

At present, data intermediaries (including CSPs) are not required to comply with the obligations in Parts III to VI of the PDPA, other than the obligations in sections 24 (the "**Protection Obligation**") and 25 (the "**Retention Limitation Obligation**").[4] This framework acknowledges the fact that data intermediaries do not dictate how personal data they hold is processed and that they act on behalf of the organizations that control the data ("**data controllers**"). This approach also accords with the accountability model set out in the OECD Privacy Framework,[5] which has laid the foundation for the adoption of privacy laws around the world, and the APEC Privacy Framework.[6] These privacy frameworks emphasize that responsibility for compliance with personal data laws should lie with the data controller.

The existing framework under the PDPA protects the individual and fosters streamlined, robust data flows with its clear allocation of responsibility. Imposing direct, joint, or shared liability on data intermediaries would insert confusion into the accountability model. For example, if an

[4] Under section 4(2) of the PDPA.

[5] A copy of the OECD Privacy Framework can be found at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[6] A copy of the APEC Privacy Framework can be found at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

individual has a concern about his or her personal data, the current framework clearly places responsibility on the data controller and the individual is therefore clear about who to contact.

The proposed approach, however, creates a split in responsibilities for organizations and CSPs in Scenario B, resulting in less clarity for individuals and regulators. An individual is also unlikely to have visibility into whether an organization and a CSP fall under Scenario B or otherwise, leading to greater uncertainty and making it burdensome for the individual to get clarity on matters involving his or her personal data.

b. The existing framework is sufficient to manage the risks associated with overseas transfers.

While the data controller remains ultimately responsible for compliance with the Transfer Limitation Obligation, it is still able to impose contractual obligations on the data intermediary as necessary and this is already an established business practice.

Even if such contractual obligations are not agreed, the existing framework already has sufficient safeguards in place to prevent unauthorized data processing by data intermediaries. Regardless of where the data center is located, a CSP acting as a data intermediary still has to comply with the Protection Obligation and the Retention Limitation Obligation, which reflects the nature of control a data intermediary has over the data it holds. Once a data intermediary exceeds the scope of the processing authorization granted by the data controller, it no longer processes data on behalf of another and therefore ceases to be a "data intermediary" thus becoming directly subject to the requirements of the PDPA.

c. Organizations in Scenario B still have "choice" and "control" over their data center locations.

The PDPC's proposed approach appears to be premised on organizations in Scenario B not having any "choice" or "control" over the cloud storage locations. However, in the data processing lifecycle, it is the cloud user that determines and controls the key decisions around data collection and data processing.

In the example shared in Table 1 of the Consultation Paper, Organization GHI still retains control and choice as it is able to choose the option of storing its data in Singapore, Hong Kong, or Japan, or even select a different CSP altogether that will only store data in Singapore. Organization GHI should therefore still be considered the 'transferring organization' as it is the entity deciding that the personal data under its control should be hosted on a cloud service or not, and which cloud service it should be hosted on. This, again, underscores the fact that the existing framework is sufficient in managing the risks associated with overseas transfers by placing responsibility for the Transfer Limitation Obligation with organizations such as Organization GHI.

d. The proposed approach fails to maintain the distinction between data intermediaries and data controllers, as contemplated in the PDPA.

As the PDPA only obliges data intermediaries to comply with the Protection Obligation and Retention Limitation Obligation, it is unclear how the PDPC will implement the proposed approach as CSPs clearly remain data intermediaries even in Scenario B. In this regard, we reiterate our request from Section B1 above for the PDPC to clarify how the PDPC proposes to distinguish

CSPs from other data intermediaries and why CSPs have been identified for unique regulatory treatment vis-à-vis other data intermediaries.

Furthermore, if data intermediaries are required to comply with the Transfer Limitation Obligation, they would also be subject to the full range of obligations under the PDPA by virtue of regulation 9(a) of the Personal Data Protection Regulations ("**PDPR**").[7] This undermines the original intention of the legislature, which recognized that "*not all organizations have the same degree of control over personal data*" and thus only imposed the Protection Obligation and Retention Limitation Obligation under the PDPA on data intermediaries.[8] In the context of CSPs, requiring compliance with all the obligations under the PDPA would not be possible in many cases as CSPs often do not have access to or visibility into the data that they hold on behalf of a customer and would therefore be unable to comply. For example, if an individual wishes to exercise the rights under section 22 of the PDPA to request for the correction of the individual's personal data, in Scenario B the CSP would be responsible for responding to this request. However, this would be impractical since the CSP is unlikely to have sufficient information to determine whether the request is reasonable, and is also likely to lack sufficient controls to correct the information.

The CSP in most (if not all) cases has no direct relationship with the individuals whose personal data a cloud user has collected, will not know who those individuals are, and will not have insights into the purposes for which that personal data will be used by the cloud user. It is therefore unclear how an individual's right to privacy as set out in the framework of the PDPA will be improved by a CSP being the "transferring organization" as set out in Scenario B. The cloud user (i.e., the data controller), and not the CSP: (a) makes the decisions of when, why, and how to collect personal data from an individual; and (b) is typically the only party with the direct relationship with the individual whose personal data has been collected and therefore is able to communicate directly with that individual about the processing and treatment of their personal data. Accordingly, the cloud user/data controller is practically and logically best placed, as contemplated by the original legislative intent behind the existing PDPA, to ensure compliance with Parts III to VI of the PDPA when it decides to use a service offered by a CSP whether that service utilizes data centers located within Singapore and/or outside of Singapore.

e. The proposed approach may discourage CSPs from having data centers or providing certain services in Singapore.

The Consultation Paper contemplates that the Transfer Limitation Obligation would apply to a CSP only where it has data centers in Singapore and determines that its customer's data should be stored overseas. A potential drawback of this proposed approach is that it may encourage CSPs to close their Singapore-based data centers to ensure the Transfer Limitation Obligation and corresponding costs of compliance are not imposed on them.

There could also be instances where a CSP is required to send data to a centralized location for diagnostic or service improvement purposes. To ensure that it does not take on the obligations of the transferring organizations, a CSP may opt to not offer services in Singapore that depend on

---

[7] This requires a transferring organization to ensure compliance with Parts III to VI of the PDPA while the personal data is under its possession on control.

[8] *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts), which can be accessed at: http://sprs.parl.gov.sg/search/email/link/?id=023_20121015_S0003_T0002&fullContentFlag=false

the ability to send data to centralized locations. This could ultimately reduce the scope of innovative services available to Singaporean consumers as compared to their global peers.

Singapore has made great progress in encouraging CSPs to establish themselves in Singapore and to offer cutting-edge, innovative services to consumers in Singapore. These efforts have been highly successful and the market is flourishing, with CSPs, many of which are BSA members, making substantial investments in data centers and other facilities here. The proposed approach in the Consultation Paper risks undoing this progress.

C. CONCLUSION AND NEXT STEPS

BSA once again commends the PDPC's efforts to continually review and update the personal data protection regime in Singapore to respond to the ever-evolving needs of the digital economy. BSA requests that the PDPC consider the comments above to ensure that Singapore remains a global hub for cloud services and cutting-edge innovation while still safeguarding personal data.

Overall, the existing framework of the PDPA already manages to strike a balance between the protection of consumers' interests and the need to keep compliance costs manageable for businesses. Therefore, BSA recommends that the proposed approach not be implemented.

Further engagement with all parts of the industry is essential before any further steps are taken with respect to the proposed approach in the Consultation Paper. As such, BSA and its members suggest meeting with the PDPC to engage in further discussion on this Consultation Paper.

Please do not hesitate to contact Darryn Lim at darrynl@bsa.org for any further information on this submission and to arrange a dialogue session. Thank you.

Yours faithfully,

BSA | The Software Alliance