EU-ASEAN BUSINESS COUNCIL

26 May 2020

Yeong Zee Kin
Deputy Commissioner, Personal Data Protection Commission
Assistant Chief Executive (Data Innovation and Protection Group)
Infocomm Media Development Authority of Singapore
10 Pasir Panjang Road, #03-01
Mapletree Business City
Singapore 117438

Re: Public Consultation for the PDP (Amendment) Bill - EU-ABC Views and Inputs

The EU-ASEAN Business Council (EU-ABC) understands that Singapore's Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) has invited the public to provide feedback on the draft Personal Data Protection (Amendment) Bill. The Council fully supports Singapore's government's initiatives to guide the country's growing digital economy, while prioritising the protection of citizens' personal data. Overall, we believe that the proposed amendments will bring Singapore's PDPA closer in alignment to EU's GDPR, a move the Council fully endorses.

As part of the consultation process, please allow us to provide you with more details for your consideration. We have consulted extensively with our members on this matter and have developed a matrix outlining their key concerns and recommendations. I have enclosed it in the Annex for your reference. I have also outlined the key takeaways below:

- **Legitimate interest:** We welcome the introduction of "legitimate interests" as a basis for processing data. This practical, risk-based approach creates a more proportionate data protection regime, eases the compliance load, and in our view, moves in the right direction of harmonising legislation with the European Union. However, we would like to request additional guidance on the scope of "legitimate interests", since this is a significant departure from a consent-based privacy regime. If the intent and scope of legitimate interest materially diverges from the GDPR, it would be helpful if the PDPC explicitly addresses those divergences in any future Advisory Guidelines.
- **Accountability and fines:** We understand the need for greater organisational accountability but would encourage the PDPC to continue to take a pragmatic approach in the imposition of fines, especially if an organisation has demonstrated the spirit/intention of compliance.
- **Mandatory breach:** We understand the PDPC intends to elaborate on what constitutes a "significant scale". However, we ask that this threshold is as consistent with other major global privacy regulations as possible, so that greater interoperability of privacy regulations can be achieved, avoiding the need for multi-national corporations to introduce in an inordinate number of jurisdiction-specific breach notification processes and enhancing Singapore's attractiveness as an investment hub. Practically, we believe the 3-day notification deadline is feasible, but ask that the PDPC does not create onerous requirements in the prescribed form of notification.

The EU-ABC has had the opportunity to work with you in the past and we hope to be able to continue our engagement with you and work even more closely together in the future.

Please do not hesitate to contact me if you may require any further clarification.

Thank you.

With kindest regards,

Chris Humphrey
Executive Director
M: +65 81682199
E: chris.humphrey@eu-asean.eu

Annex

Article	Concern(s)
16. Organisations will also be required to **notify affected individuals** if the data breach is likely to result in significant harm to them.	• Please provide clarity whether one or more categories of personal data will be deemed as a data breach that will results in, or is likely to result, in significant harm to the individuals. • Is there a numerical threshold that warrants a notification to the affected individuals and/or PDPC?
20. Upon determining that a data breach meets the criteria for notifying affected individuals, the organisation must **notify all affected individuals as soon as practicable**.	• Who has the duty to notify the affected individual i.e. the entity that collected the personal data as opposed to the entities to which the data may have been transferred although the breach may have happened by the transferee entity?
20 Where a data breach meets the criteria for notifying PDPC, the organisation must **notify PDPC as soon as practicable, no later than three calendar days after the day the organisation determines that the data breach meets the notification criteria.**	• Suggest to notify PDPC as soon as practicable, no later than three working days instead of calendar days after the day the organisation determines that the data breach meets the notification criteria.
20. However, PDPC must be notified before or at the same time as affected individuals are notified, to allow PDPC to assist affected individuals who contact PDPC once they are notified	• Can the organisation proceed to notify the affected individuals or to pend for further advice from PDPC?
22 MCI/PDPC will provide the following exceptions to the requirement to notify affected individuals.	• For cases under exceptions, would organisation need to notify PDPC?
23. In addition, organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC.	• Would this mean that the notification to affected individuals is subject to directions from PDPC?

30. Besides strengthening organisational accountability, MCI/PDPC will also strengthen the accountability of individuals13 who handle or have access to personal data (e.g. employment or engagement by an organisation).	• Would this apply to individuals (e.g. employees from other locations) not based in Singapore?
44. Under the Data Portability Obligation, an organisation must, at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format.	• The data portability obligations could impose a burden on organisations that hold a lot of personal data at many touch points and may not have it all stored in a single platform. To be able to transmit all data requested by the customer could be onerous.