Asia Pacific MSME Trade Coalition (AMTC)

28 May 2020

Dear MCI Data Regulation Secretariat,

Subject: Industry submission on Public Consultation on the Draft Personal Data Protection (Amendment) Bill

On behalf of the Asia-Pacific MSME Trade Coalition (AMTC) and its members, we write to submit our feedback to the Singapore Government on the Draft Personal Data Protection (Amendment) Bill.

AMTC is the first and only pan-Asian Trade Association advocating on behalf of Micro, Small and Medium Enterprises (MSMEs) across Asia. AMTC comprises the largest and most diverse group of MSMEs in the region, with over 3000 members drawn from across 27 countries in Asia-Pacific, with 600 in Singapore alone, where we are headquartered. Many of our members, in a wide variety of sectors, might be called "digital natives." Almost all of our members, including traditional goods companies, exist either partially or fully online.

AMTC has been a consistent proponent of the importance of sensible data policies to unlock the promise of the digital economy for MSMEs. We believe that being online can, in a single stroke, soft-pedal the weaknesses of many MSMEs such as a lack of financial capacity and limited physical infrastructure and is the nearest thing to a silver bullet for MSMEs to flourish. In order to continue operating online, MSMEs need data policies that are easy to comply with and are not overly burdensome

To this end, Singapore has been a pathfinder in the region and beyond in promoting a business-friendly data regulatory environment that is easily navigable by large and small businesses alike while protecting the data rights of consumers. We thank the Singapore government for the opportunity to provide feedback on behalf of MSMEs and the chance to be heard.

Dr. Deborah Elms
President
Asia-Pacific MSME Trade Coalition (AMTC)

a) Details of Industry Association Submitting Comments

Company Name: Asia-Pacific MSME Trade Coalition

Address: 43 Niven Road

POC: Barath Harithas

Title: Director (Southeast Asia)

Contact Number: +65 97537412

b) Summary of Key Points

AMTC commends MCI and PDPC on its move to review the PDPA and ensure it keeps pace with the evolving technological and business landscape, while providing for effective protection of personal data in the Digital Economy.

We note its shift towards a risk-based, accountability approach which is in line with global trends. We commend the Singapore government on its principled approach to strengthen the accountability of organizations and provide consumers with greater autonomy over their personal data. However, we note that while the merits and reasons for specific provisions are apparent from a regulatory point-of-view, AMTC notes that for MSMEs who can ill-afford legal-compliance teams, some of them may be difficult to meet. The retention of all user activity data in order to respond to a portability request is costly and cumbersome, particularly for MSMEs. Similarly, privacy impact assessment are good practices, but they should only be required for sensitive data or for uses that present a risk of harm to individuals, rather than for data processing which takes place in the everyday course of business. Otherwise, this may be too resource intensive for MSMEs to comply with. In addition, a 3-day deadline to respond to data breach would be near impossible for many MSMEs to meet. It is difficult enough for a large firm to accomplish this within a two to three day period, much less a MSME.

Lastly, some of the punitive measures may be crippling for MSMEs. While we recognize the importance of enforcement, for MSMEs already teetering on the brink of collapse, a fine amounting to 10% of an organization's annual gross turnover in Singapore would certainly capsize their business.

Given the scale of the changes wrought and that need to be internalized and implemented by MSMEs, AMTC proposes a two-year phased implementation period to allow MSMEs the time necessary to collect information, draft processes, policies, and protocols to address the requirements of the Bill. Without such lead time, MSMEs will likely be unable to put in place well-established processes, policies, and protocols.

c) Comments

S/N	Section	Comments
1.	**Accountability**	We do not object to privacy by design, privacy impact assessments, the appointment of data protection officers etc. as these are generally considered good practices. The existence of a documented privacy program with these features should be a mitigating factor in any enforcement action against a company. Ideally, impact assessments will only be required for sensitive data or for uses that present a risk of harm to individuals, rather than for data processing which takes place in the everyday course of business. Otherwise, this may be too resource intensive for MSMEs to comply with and would require hiring someone which MSMEs can ill-afford during the current economic downturn.
2.	**Data Breach Notification**	We do not object to the requirement to notify PDPC and individuals in the event of a breach of personal data. It would however be helpful if PDPC could clearly outline a criterion for reportable breaches and provide clear guidelines on the items to be reported. These should not be too prescriptive as the necessary steps will depend on the type and manner of the breach, and MSMEs across varying sectors will have differing practicalities, resources, and internal processes to assess the breach. We support the proposal to limit notification to situations in which significant harm is likely to result or where the impact is significant, although greater clarity/comprehensive guidance on this threshold is needed. In particular, it will be important to avoid any "notification fatigue" that could arise from a threshold which results in too numerous or immaterial notices.
3.	**Timing**	The law should require notification to all parties within a reasonable time. Requiring notice to any party within 3 days imposes a significant burden on firms and supervisory authorities alike. When a firm becomes aware that a breach may have occurred, it typically begins an intense process of investigation involving its processors, outside computer forensic investigators, outside legal counsel, and internal legal and IT teams to determine whether a breach has occurred. A forensic investigation may take two to three weeks from engagement until completion, at which point the firm must determine whether it demonstrates evidence of a breach and the impact of such a breach. This is difficult enough for a large firm to

		accomplish within a two to three day period, much less a MSME. Such a 3 day deadline would be near impossible for MSMEs to meet. AMTC further notes that requiring notice to supervisory authorities before this process has concluded diverts resources from the important task of investigation. It also risks providing the authorities with incomplete or incorrect details about a breach and its scope, requiring subsequent clarification and communications. While GDPR has a similarly short timeframe for notice to authorities, many have indicated that voluminous data breach reports have overwhelmed their offices[1]. This would likely be the case with MSMEs based in Singapore. For these reasons, we ask that PDPC consider whether a requirement to notify it of a personal data breach "within a reasonable time, without undue delay" would strike a better balance between the interests at stake.
4.	**Criminal Penalties**	A Personal Data Protection law should impose fines for violations of its provisions rather than criminal penalties. The existing criminal code likely already has appropriate penalties for mishandling personal data. If such penalties are necessary, they should be added to the criminal code rather than the PDPA. The inclusion of criminal penalties in this law also seems inconsistent with the proposal to shift to administrative penalties for DNC.
5.	**Enable Meaningful Consent**	The proposals for deemed consent for contractual necessity and where notification is provided are positive, as they strike the right balance between allowing the use of personal data in the ordinary course of business and providing individuals with control. Clear statutory language would also improve on the confusing schedules contained in the current PDPA. We similarly support the exceptions to obtaining consent for legitimate interests and business improvement. The amendments appear to require opt-in consent to the use of personal data for direct marketing. We would propose that this data be subject to opt-out. Businesses should be able to communicate with their customers about new products and

[1] See - Angelique Carson, Dispatch from Paris: DPAs are flooded with complaints, IAPP Privacy Advisor, February 19, 2019, available at: **https://iapp.org/news/a/dispatch-from-paris-dpas-are-inundated-flooded-with-complaints/**; Mathew J. Schwartz, Data Breach Reports in Europe under GDPR Exceed 59,000, GovInfoSecurity, February 19, 2019, available at: **https://www.govinfosecurity.com/data-breach-reports-in-europe-under-gdpr-exceed-59000-a-12006**).

		offers, as this is an ordinary business function which presents low (if any) risk to individuals. An opt-out also seems more consistent with the proposals to improve controls for unsolicited commercial messages.
6.	**Increasing Consumer Autonomy**	The limitations on the right to portability are helpful to cabin this resource-intensive procedure. We would prefer that portability be limited to data provided to a company rather than user activity data. The retention of all user activity data in order to respond to a portability request is costly and cumbersome, particularly for MSMEs, and it is unclear how the transfer of this data benefits the individual. We also recommend that any data portability requirement must ensure that MSMEs' intellectual property rights and confidential and proprietary information are protected, and that the porting of data be required only under circumstances where data can be kept secure. For MSMEs attempting to distinguish themselves from the pack, their intellectual property (IP) is their singular leg-up on the rest of the market. As such any data portability requirement should be sensitive to these competitive concerns.
7.	**Strengthen Effectiveness Of PDPC's Enforcement Efforts**	While financial penalties are absolutely preferable to (and more proportionate than) criminal penalties, a fine amounting to 10% of an organization's annual gross turnover in Singapore is too punitive. For MSMEs already teetering on the brink of collapse, a fine of this size would certainly capsize their business.
8.	**Implementation Period**	Given the anticipated adjustment pains for MSMEs, AMTC proposes a two-year phased implementation period to ease businesses into compliance.
9.	**Capacity Building**	PDPC has done a commendable job of reaching out to firms in Singapore on regulatory changes. We request that data changes, like these proposed adjustments to the regulatory environment, require additional outreach to MSMEs to ensure that firms have sufficient knowledge and understanding of the rules, receive advice on appropriate measures to implement them within their company, and know about the enforcement penalties if the rules are not followed.