28 May 2020

To
Mr Tan Kiat How
Commissioner
Personal Data Protection Commission (PDPC)
10 Pasir Panjang Road,
#03-01 Mapletree Business City, Singapore 117438

Subject: Industry Submission by Asia Internet Coalition (AIC) on Personal Data Protection (Amendment) Bill 2020, ("the Bill)

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Personal Data Protection Commission (PDPC) and the Ministry of Communications and Information (MCI) for the opportunity to submit comments on the **Personal Data Protection (Amendment) Bill 2020, ("the Bill")**. AIC is an industry association comprising leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter, SAP, Booking.com, and Yahoo (Verizon Media).

We commend the PDPC's and MCI's efforts on steering three public consultations on the policy positions for the key proposed amendments to the Personal Data Protection Act and for releasing the amended bill, to ensure that this policy initiative strikes a balance between the need to protect individuals' personal data. Singapore's digital landscape and economy have evolved and capitalisation of data and cross-border data flows have become increasingly important for business innovation and economic competitiveness, which AIC strongly supports. In view of technological developments, we are also cognisant of the significant challenges, owing to which data protection laws are also shifting towards a risk-based, accountability approach to ensure organizations meet data protection standards.

Such efforts and dialogue are critical, particularly at a time when cross-border trade and data security has taken a center stage in a new global development. This rings particularly true given the current COVID-19 pandemic, due to which a great deal of our lives has been moved online. Therefore, it is now more critical than ever to protect individual data particularly when economies and companies are transitioning rapidly into the digital space.

As responsible stakeholders, we appreciate the ability to participate in this discussion and the opportunity to provide input into the policy-making process. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request PDPC and MCI to consider.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue around effective data protection framework in Singapore.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Cc:
Mr S Iswaran
Minister for Communications and Information
Ministry of Communications and Information (MCI)
140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369

1. Mandatory Data Breach Notification (DBN)

1.1. Interpretation in Section 26A

Recommendation: Revise the definition of "data breach" to more clearly state when the DBN should be triggered.

As per Section 26A, MCI/PDPC can consider revising the definition of "data breach" to be more consistent with international practices. For example, the EU General Data Protection Regulation (GDPR) states that " 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

1.2. Notifiable data breaches and Notification Criteria in Section 26B

Recommendation: Clarify the meaning of "significant harm" threshold

Applying a "significant harm" threshold to breach notifications helps to ensure regulators have visibility into the incidents that pose actual risk to users and ensures regulators will be able to focus guidance and oversight activities where they are most needed.

However, the threshold for notification to be based on the likelihood of "significant harm" is unclear. This could result in the PDPC and individuals being inundated with numerous immaterial notices, resulting in "notification fatigue" and a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm.

Recommendation: Remove the numerical threshold in the breach notification requirement.

The Public Consultation Document indicates that organizations will be required to notify PDPC of data breaches that (i) result in significant harm to the individuals, OR (ii) affect 500 or more users. We recommend that PDPC eschew numerical thresholds in the data breach notification requirement, and rely on a "significant harm" threshold instead.

By conditioning notification on size of impact OR harm, the proposed legislation doesn't effectively combat notification fatigue for users (since notification would be required for technical data breaches that affect many users but have only trivial privacy impacts) and burdens both regulators and entities subject to the regulation. For example, an email exposing 501 email addresses in the CC line would be reportable under this threshold.

In assessing whether an organization's security practices constitute a "systemic issue within an organization", the PDPC should examine the nature of the security incident rather than the volume of individuals affected. For example, an employee of a company that mistakenly accesses a database of information about 1,000 customers on a single occasion would not suggest systemic issues with an organization. By contrast, the mistaken disclosure of a single patient's medical history through unencrypted channels might suggest systemic issues. In encouraging notification in both instances, PDPC will make it more difficult to distinguish security incidents that create no risk of harm from security breaches that may create a significant risk of harm.

Should the PDPC decide to implement a mandatory data breach notification requirement, we suggest:

- to provide a clear definition of a reportable data breach as well as examples;
- to increase the numerical threshold on what constitutes "a significant scale" from 500 to 1,000 individual as a breach of less than 1,000 is unlikely to represent a systemic issue within the organization; and
- to provide an exception to the notification requirement where an organization has taken remedial action early enough for serious harm not to have occurred or not to be likely to still occur.

1.3. Duty to conduct assessment of data breach in Section 26C

Recommendation: A Data Intermediary (or "DI") should only be required to notify the organization after becoming aware of an actual data breach, rather than where it has "reason to believe that a data breach has occurred in relation to personal data" (proposed Section 26(C)2). Further, Section 26C(2) should be revised to make clear that data intermediaries do not have the obligation to monitor security breaches that are the responsibility of the main organization.

As currently proposed in the Bill, the Data Intermediary is required to notify the organization without undue delay where it has "reason to believe that a data breach has occurred". The requirement for a DI to notify of suspected breaches is unduly burdensome on data intermediaries and may result in "notification fatigue" to the data controller if the intermediary notifies all suspected breaches. The requirement also goes beyond other international standards, including Article 33 of the GDPR, which requires the processor to notify the controller without undue delay after *becoming aware* of a data breach. The

proposed language is overbroad and confuses the obligations of the DI and the main organization on whose instructions the DI acts. The Data Intermediary's obligation to notify should apply where the Data Intermediary has actual knowledge of a data breach and the breach extends to data or systems over which the Data Intermediary exercises control and has visibility into the content. As currently drafted, Data Intermediaries could be required to not only monitor their own systems but also proactively monitor the systems and content of the main organization in order to be able to comply with their obligations, which blurs the responsibilities between the parties and could create a situation where the main organization fails to implement its own appropriate security measures and monitoring systems because it expects the Data Intermediary to carry out these obligations on its behalf. We therefore recommend that MCI/PDPC revise the PDP Amendment Bill to make clear that the DI should not be responsible for monitoring the security of the responsible organization (for which it is acting on behalf on), or verifying whether instructions on processing the data given by the responsible organization to the data intermediary are duly authorized.

1.4. Duty to notify occurrence of notifiable data breach in Section 26 D

Recommendation: Clarify the scope of the exceptions for notifying individuals, while maintaining flexibility for organizations

The scope of the exceptions for notifying individuals of a data breach is not clear, especially in relation to the actions that the organization must have taken, or the technological measures that the organization had implemented, as to render it unlikely that the data breach will result in significant harm to the affected individual.

While we welcome additional clarity on these requirements, we recommend that they are not overly prescriptive and are technology agnostic, to maintain flexibility for organizations operating under different circumstances and having different processes and resources. Further, it is recommended that the requirements are set out as guidance rather than legislative requirements in order to maintain flexibility over time.

As mentioned above, we recommend that MCI/PDPC **revise section 26(D) to make it clear that DIs are not required to notify the Commission and Individuals of a "notifiable data breach"**. While we support the requirement for DIs to notify organizations of data breaches "without undue delay", it should however remain the responsibility of the organization to assess whether a data breach constitutes a "notifiable data breach" and notify the Commission and/or individuals, as the case may be. The current drafting of section 26D is ambiguous as to whether such notification obligations would apply to DIs. We therefore propose amendments to the language to make it clear that this obligation **would not apply to data intermediaries**, as MCI/PDPC intends.

Further, mandatory information referenced in Section 26D(3) should not require organizations to provide detailed information related to the data breach, as investigations

may still be ongoing at this relatively early stage of the notification period. Further, we also request clarity on the provisions in Section 26D(7) where the Commission may waive the requirement for organizations to notify affected individuals, so that organizations have greater visibility on the circumstances and factors that the Commission may take into account in determining whether a waiver may apply.

2. Removal of exclusion for organizations acting on behalf of public agencies

PDPA now applies to DIs acting on behalf of the government. However, DIs acting in such capacity were previously excluded.

Recommendation: Sections 24 and 25 of the PDPA, be further amended to make clear that where the relevant processing activity relates to a DI acting on behalf and for the purposes of a public agency, that such reasonable protection or retention should be in accordance with their contractual arrangements, and/or any other applicable law or regulation.

Further, the removal of the exclusion for organizations acting on behalf of public agencies, is confusing as it is unclear whether a DI would be reasonably able to take on its relevant obligations (i.e. retention and protection), given that the organization it is acting on behalf for (i.e. public agencies), is not subject to the PDPA.

3. Data Portability

3.1. Clauses 2 and 3 of the draft PDP (Amendment) Bill pertaining to the definition of "derived personal data" and rules to the Correction obligation

Recommendation: The Public Consultation Document states that "derived personal data" will be excluded from the Correction Obligation and the Data Portability Obligation, however the latter exception does not appear to be reflected in the Bill. This should be made clear. Further, we request further clarity on the definition of "derived personal data", so that organizations can better understand the scope of the exception.

3.2. Clause 15 of the draft PDP (Amendment) Bill pertaining to enabling the Commission to refer complainants to resolve disputes via mediation, without the need to secure consent of both parties to the complaint or dispute

Recommendation: We recommend clarifying the factors the Commission will consider before referring disputes to mediation, to avoid this being abused as a mechanism used by parties to pursue frivolous claims by data subjects, given the costs and resources of having to engage in mediation.

3.3. Data portability obligations in Clauses 13 and 16 of the Bill

Recommendation: Overarching clarifications required on Data Portability obligations.

a. clarifying the scope of "applicable data" and including a mechanism allowing organizations to weigh the burden of making such data available for porting against the benefits to the individual.
b. clarifying whether the scope of "applicable data" includes information pertaining to non-requesting individuals, and if so, how the rights and freedoms of other individuals should be protected.
c. clarifying what the requirements for the data porting request are and allowing some flexibility for organizations to prescribe requirements themselves.
d. clarifying the timeframe porting organizations have to respond to or comply with requests.
e. clarifying what the factors for determining an "ongoing relationship" are.
f. clarifying the obligations of transferring organizations with respect to the data protection practices of recipients.
g. clarifying whether recipients are obligated to import ported data.
h. including an express provision in the Bill that the Fifth Schedule exceptions will also apply to the data portability obligation.
i. clarifying what the technical and process requirements for porting will be.
j. clarification on whether the Bill's definition of "derived personal data" includes inferred data.

Recommendation: Broad data portability requirements should *not* be mandated.

- If MCI/PDPC nonetheless proceed with mandating data portability, **we recommend that the data to be ported be limited to the purpose of providing individuals with greater autonomy and control over their personal data.** We also recommend that any data portability requirement must ensure that organizations' 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.

    - To elaborate on the above, there exist different implications for subsequent decisions on the 'whitelist' of data categories to which the data portability obligation applies. This is particularly relevant when we

consider the scope of "user activity data" that would be included. The inclusion of "user activity data" with its current broad definition gives rise to serious concerns over the potential leakage of proprietary and confidential commercial information. As an example for illustration, "user activity data" can contain proprietary attributes, and the combination of any number of categories can easily be retro-engineered to derive underlying algorithms that are proprietary to the porting organization. We would recommend that if information contains the personal data of an individual and that of third parties, companies must consider whether it is reasonable to disclose this information and whether this would adversely affect the rights and freedoms of others.

- We would also like to stress the significant implementation effort and costs for organizations to comply with the data portability obligation. We strongly urge MCI/PDPC to ensure that the realized benefits of data portability to individual users are proportional to the costs of implementation. To ensure this, we further urge MCI/PDPC to ensure that the scope of data subjected to data portability is clearly set out by way of a 'whitelist' of specific data categories (e.g. name, transaction date and time, other transaction-specific related information), as opposed to a general definition of "user activity data", and is limited to only that which is necessary for the defined purpose and based on clearly defined user benefits, which should be further clarified on a sectoral basis, with broad industry consultation and agreement on the exact in-scope data categories. We also seek MCI/PDPC's confirmation that organizations would be allowed to recover the incremental costs of implementing the new Data Portability Obligation, and further, to provide clarity on which parties (i.e. the porting organization, the receiving organization, the data subject) the costs would be accrued to.

- **We recommend that any direct service-to-service portability is limited to where it is "technically feasible".** This is because it may not always be technically feasible to provide data directly to other service providers, and is in line with the approach under GDPR. Nevertheless, it is worth noting that companies involved in the Data Transfer Project are working to address interoperability issues by creating an open source platform to allow users to more easily move their data between online service providers. Technical feasibility is an important condition that we recommend PDPC include in a finalised data portability obligation. If requests are permitted in circumstances where they are not yet technically feasible, individuals' expectations may not be met and organizations may attempt transfers that are neither technically sound nor secure, to the detriment of individuals' data protection interests and expectations.

- We also **recommend that the scope of "user activity data"** (pursuant to proposed Section 2(b) of the PDP Amendment Bill) **be further amended to to the extent that** portability should not focus exclusively or put much emphasis just on encouraging switching service providers but the goal should be to

enhance user control and should support the full range of potential consumer behaviors that result from portability, from switching to multi-homing.

- The definition of "user activity data" is currently overly broad and may result in undue burden or cost to organizations which outweigh the potential benefits to the individual. An overly wide definition of "user activity data" risks countering the intended objectives of promoting competition if industry first-movers do not have the assurance that their innovations would be protected, e.g. if other players can easily reverse-engineer ported data to glean proprietary information. Accordingly, **we recommend that there is an exception or balancing test which allows organizations not to comply with the data porting request where the burden or expense of making the data available for porting outweighs the benefit to the individual.**
- To this end, we strongly recommend that the "whitelist" of data categories be narrowly scoped to meet the purpose of allowing individuals to switch to new service providers more easily. For example, it may be helpful for online retail users to port transaction details of their shopping history. However, data generated from using specific features provided by a company, such as browse and discovery tools, or dedicated loyalty or gift card programs, is unlikely to be readily usable by other companies. Further, most types of user-generated content are sensitive in nature and their sharing across companies could gravely undermine the privacy of both the requesting individuals and third parties.
- **We also recommend that unstructured or pre-processed data should be clearly excluded** as this would cause an undue compliance burden on the organization to structure and process the data, and be of little value to individual users. By unstructured data, we mean data may reside in data streams or lakes and may not be in a processed or structured form.
- To summarize, **we recommend that the "whitelist" of data categories exclude (i) user activity data generated from the use of proprietary tools or features, (ii) user-generated content (such as voice recordings, images, and customer reviews), and (iii) unstructured data.**

- **The PDP (Amendment) Bill should expressly state that the exceptions in the Fifth Schedule of the PDPA apply to the data portability obligation** (i.e. an organization is not required to comply with a data porting request in respect of the matters set out in the Fifth Schedule)**.** This is stated in the Public Consultation Document, but does not appear to be reflected in the draft PDP (Amendment) Bill.

- **We also request that MCI/PDPC commits to consulting with industry prior to the development of prescribed requirements in the Regulations**, particularly when the new Data Portability Obligation comes into effect.

- The **Regulations should also allow flexibility for organizations to prescribe certain requirements themselves**, for example in relation to data porting requests, technical and process requirements for porting, etc.

4. **Increase in financial penalty cap**: maximum financial penalty to (i) up to 10% of an organization's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.

Recommendation: Deletion of "10% annual gross turnover".

We note that in recent years, a few data protection authorities have strengthened the enforcement of their data protection by increasing/proposing to increase the financial penalty cap for non-compliance. This includes data protection authorities in the EU member states and Australia. However in these countries, data protection laws have been established for many years, providing sufficient time for local companies to enhance their processes and systems. Further we note that the PDPC is introducing several new obligations in this public consultation paper. Before increasing the financial cap, we would recommend the PDPC to issue first the relevant regulations and guidelines to ensure that companies have a clear understanding of their new obligations.

Finally, the PDPC recently explained in its seven global personal data protection priorities for 2020 that "deterrence and punishment alone have proven to have limited effectiveness in achieving desired results, much less encouraging a race to the top in the market. If regulators want to be effective, they must apply modern and innovative regulatory approaches as well and prioritise open and constructive relationships with the organizations they regulate". We agree with such an approach and welcome the PDPC's proposal to introduce statutory undertakings and mediation as this would assist companies to be more accountable.

With respect to civil penalties, they should not be tied to a regulated entity's turnover, and should be proportionate to the harm caused to the data subjects and whether there are any aggravating or mitigating factors. Civil penalties frameworks should also not impose undue hardship on an otherwise responsible entity.

If MCI/PDPC proceed with the 10% annual gross turnover penalty, **the new Section 29(2A) of the PDPA should be clarified so that it refers to 10% annual gross turnover in Singapore only.** This is stated in the Public Consultation Document, but does not appear to be reflected in the draft PDP (Amendment) Bill. To avoid penalising organizations that act in good faith, PDPC should also consider introducing a provision that it may impose a financial penalty only if the infringement has been committed intentionally or negligently, similar to section 69(3) of the Competition Act.

The Bill also introduces a new offence for a person to fail to comply with an order to appear before PDPC/an inspector and provide his/her statement(s) in relation to an investigation. We are of the view that obstructing the PDPC during the course of investigations is already considered as an aggravating factor when calculating a financial penalty. Current financial penalties are already a significant deterrent.

5. **Further clarification to "voluntary undertakings"** scheme including on due process and appeals mechanisms in Clause 18 of the Bill

Recommendation: PDPC should further clarify that voluntary undertakings are undertakings that are proposed by an organization or person, and such undertakings (including any variations) will not be imposed by the PDPC, without prior agreement from the relevant organization.

In addition, given the requirements that failure to "comply with an undertaking" could result in the voluntary undertaking being publicized and cost recovery (proposed Section 31A-5) – **we also recommend that PDPC avoid mandating that organizations or persons to be subject to the voluntary undertaking mechanism – and provide organizations or persons the ability to reject such a proposed undertaking, without prejudice**. Furthermore, this scheme should reflect existing obligations of organizations and powers of the Commission, i.e., proposed undertakings should not go beyond the commission's existing powers or existing obligations of the organization.

6. **Deemed consent by notification**

Recommendation: The opt-out requirement (proposed in Section 15A(3)(b)(iii)) should only be provided where feasible.

- Deemed consent by notification is likely to be relied on by organizations where it may not be practicable to obtain consent. Under the same circumstances it is likely that it also may not be practicable to provide the individual with an opportunity to opt out.
- Accordingly, organizations should only be required to allow individuals a reasonable time to opt out, where it is feasible to do so. This is consistent with the PDPC's position in its Public Consultation for Approaches to Managing Personal Data in the Digital Economy, where it was proposed that "where feasible, organizations must allow individuals to opt out…".

7. **Exceptions to consent**

Recommendation: The Legitimate Interests exception should be expanded to include any third party's legitimate interest.

- The proposed legitimate interest exception allows for the collection, use, and disclosure of personal data without consent where it is in the legitimate interests of the organization, and the benefits (economic, social, or security) to the public (or a section of the public) outweighs the adverse effect on the individual (following internal assessment). We recommend that legitimate interest should be expanded to include any third party's legitimate interest, in alignment with the GDPR.
- The scope of what is considered to be a benefit to the public, or a sector thereof, should also be clarified, and we note that the GDPR does not impose a similar limitation on the legitimate interests concept.

Recommendation: Align the assessment for relying on the "legitimate interests" exception with the internal assessment for deemed consent by notification .

- To rely on legitimate interests as an exception to consent, organizations are required to conduct an assessment that the benefit to the public of the collection, use or disclosure of personal data is greater than any adverse effect on the individual.
- The assessment must include the identification of any adverse effects on the individual, measures to eliminate the adverse effect or if not possible, to reduce or mitigate the effect. This appears to be a more stringent assessment than the assessment required for deemed consent by notification.
- Accordingly we would recommend that the same assessment is applied for both deemed consent by notification and for legitimate interests, so as to avoid confusion for organizations.

Recommendation: Clarify that the "business improvement" exception to consent applies across all group entities (as proposed in Section 32 of the draft PDP (Amendment) Bill).

- The Public Consultation Document states that the exception applies to a group of companies, however this does not appear to be reflected in the draft PDP (Amendment) Bill.

8. Related amendments to Spam Control Act (SCA) in Section 38

Recommendation: We would request for PDPC's clarification on whether the expansion of the Spam Control Act would lead to a deletion / opt-out requirement for instant messaging.