ASIA
INTERNET
COALITION

27 July 2020

To
The Personal Data Protection Commission (PDPC), Singapore
10 Pasir Panjang Road,
#03-01 Mapletree Business City, Singapore 117438

Subject: Industry Submission by the Asia Internet Coalition (AIC) on the proposed classes of personal data that, when compromised in a data breach, organisations would be required to notify affected individuals and the Personal Data Protection Commission (PDPC) of the breach

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) for the opportunity to submit comments on the **Proposed Classes of Personal Data, in regard to the Data Breach Notification Requirement.** 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 members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter, SAP, Booking.com, Cloudflare and Yahoo (Verizon Media).

We commend the PDPC's efforts on steering this consultation with AIC to strengthen the Personal Data Protection Act (PDPA) to govern the protection and management of personal data by the private sector. The AIC understands the importance of data breach notification requirement, resulting from significant harm to individuals. 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.

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 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,

JPaine

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations on the Proposed Classes of Personal Data Subject to Data Breach Notification Requirement

1. Circumstances in which data breach notification obligation is triggered

The circumstances in which data breach notification obligation is triggered should be subject to the actual breaches, and not unconfirmed data security events, and in cases where organisation has not been able to prevent the likely risk of serious harm with remedial action. E.g. if data is encrypted, it should not trigger notification obligation. If certain access credentials are compromised, but there are other safeguards (e.g. two factor authentication) that ensure security is not affected, it should not trigger a notification obligation.

2. Proposed data fields

The data fields must be concrete enough to be easy to search through *automated means*. The information defined in (a) and (b) in Appendix: Table on classes of data can mean a lot of subjective interpretation and manual searching, and that should be avoided.

- E.g. the table represents "Full name*" but qualifies "* Full name **may include** his/her principle name, hanyu pinyin, alias, alias in hanyu pinyin, married name, name in ethnic characters (e.g. Chinese, Jawi, Tamil), whether in full or in parts." **We therefore recommend clearly defining what constitutes a full name (i.e. comprising of first name and last name, as reflected in the NRIC or passport).** One suggestion is for the full name to be verifiable by official sources such as the Singapore government's MyInfo service. This will make it more concrete and easier to search by using automated means. Therefore, clarification is sought to mentioning the definition of full name (combination of first, last names), whichever form it takes (alias, hanyu pinyin, others).
- **We also request clarification whether the full name definition potentially include email addresses.** E.g. firstname.lastname@domain.com may imply someone that the data subject's name is FirstName LastName.

3. "Financial information" is a very broad category that should be narrowed down to those essential pieces of information that cause significant harm to the individual, with examples of some specific circumstances that may apply, such as identity theft or disclosure of financial situation like bankruptcy status.

3.1. We request clarification from PDPC if receipts and e-commerce transaction records are included under the said "financial information"

- E.g. if a system or solution handles a lot of receipts. Do receipts count as "financial information" in this context?
- E.g. if one buys a book online. Would the transaction record be considered "financial information" (excluding credit card information)?
- E.g. updates to e-wallets or online accounts. Would a top-up or deduction of "X" amount on a certain date to an e-wallet or other online account be considered "financial information"?

3.2. Further, we are of the view that "Life/Insurance information" is another very broad category that should be narrowed down to those essential pieces of information that cause significant harm to the individual if exposed.

- We propose to exclude circumstances such as email communications to policy-holders where the name of individual is included in an administrative email that has the plan name, coverage status (e.g. whether the plan is still valid or has lapsed), or other details that are publicly available (e.g. coverage details of the plan, publicly available online).
- We seek clarification from PDPC on the insurance categories that would be included:

    - E.g. for insurance insurability, this may be a result of factors such as age eligibility. Would an email to inform/update individuals that they are hitting the age limit for coverage be included under this category?
    - E.g. would investment-type/endowment insurance plans that are structured as some form of "life insurance" be included?
    - E.g. would disability or personal accident insurance be considered "health insurance"?

4. There are overlaps with sectoral legislation. We may want to consider adding such data class regulations into sectoral legislations, instead of the list of proposed data classes under the Personal Data Protection Act.

As data privacy law is universal (not sectoral), it applies to everyone regardless of circumstances. Data should only be included in this list if it makes sense to impose such regulations on everyone, including a Mom and Pop convenience stores.

- E.g. banking laws already cover protection for financial records, salary information; insurance laws already cover insurance coverage and insurability information. And this class of information is already well protected as confidential information under contracts.
- The challenge of this proposal is imposing on non-regulated entities (like a neighborhood clothing store in Ang Mo Kio) the same regulatory burden as a regulated entity (like a bank). If the concern is with financial service providers' not informing data subjects of data breach, we recommend regulating the financial service providers, and not introduce such a list into privacy laws.

5. Identification information

It should be made clearer that notification is necessary only under situations of high risk. To trigger the data breach notification obligation to the authorities, e.g. **in high risk situations** when a third party can continue to use that information to access the account even ***after the remediation actions are taken***.

- If remediation actions are taken and users' privacy are protected, then such situations may not trigger the notification obligation.
    - E.g. the identification information that was compromised alone is insufficient to gain access to account because of 2FA requirements or geo-fencing technology.
    - Or if there are no log-in attempts during the relevant time window, and the administrator has already triggered a "forced" password change on the user, during which there will be another user authentication process.
- The AIC would also like to seek input on: Is a "forced" password change considered a notice under the proposed law? The user may only know about it when he or she attempts to log-in again. We therefore recommend that the law should consider a "forced" password change as one avenue to satisfy the requirement of notice to the data subject.

6. **The proposed law should separate the two types of notification**: **(i) notification to authorities only, and (ii) notification to data subjects**.

    - Like GDPR, the threshold for notification and the contents of notification should be distinguished. This is because the purpose of notification the authorities and notification of data subjects is different. The associated costs and effort of notifying data subjects (and managing public communications) is also potentially many times higher than a single notification to the authorities.
    - We recommend that PDPC only limit notification to data subjects if there is high risk to the rights and freedoms of natural persons and the organisation has not been able to prevent the likely risk of serious harm with remedial action

7. **We suggest the following edits and recommendations in the table provided in the Appendix: Table on classes of data**

    We are supportive of the proposed approach to develop a "whitelist" of data classes and specific types of data under each class, which, when compromised, will require notification to be made to the PDPC and affected individuals. This "whitelist" will provide much needed clarity to organisations on when the Data Breach Notification requirement applies. To ensure clarity however, it should be clearly stated that this "whitelist" is comprehensive, and that all data classes or specific types of data not excluded from the "whitelist" will not be subject to the Data Breach Notification Requirement—except when more than the prescribed threshold are involved.

    With regard to the proposed classes of data listed at paras (a) and (b) in the Appendix: Table on classes of data, we would like to clarify with PDPA what the basis is for differentiating between the two data classes (a) and (b). Is the intention for the breach of each data class to have different reporting requirements e.g. breach of class (a) will require notification to PDPC and the affected individual while breach of class (b) will require only reporting to the affected individual?"

    On the specific types of data in (a), we would like to better understand the thinking behind not including that financial account information, which is considered sensitive in some jurisdictions, but including salary? Access to someone's banking information could result in more harm than access to someone's salary.

Appendix: Table on classes of data

(a)	• **Full name*; or** • **Full national identification number** (e.g. NRIC number, Birth Certificate number, FIN, Work Permit number and passport number) in combination with any of the following data relating to an individual: + **Financial information** (e.g. financial records, salary/remuneration, loan/credit history) excluding financial account numbers (e.g. bank account, credit/debit card numbers) + **Life/health insurance information** where it reveals health and financial information (e.g. insurance coverage, insurability) + **Medical information** (e.g. medical history, medical diagnosis/condition and treatment, including mental or physical infirmity, disability or incapacity) - ***Comment regarding medical information:*** *It should be made clear that this category is limited to actual medical information (e.g. information required to provide a medical service / as overseen by a medical professional). It should not include general biodata / health-related data such as number of steps taken or other data collected through mobile phones such as heart rate, sleep monitors etc.* + **Personal data of a child or young person** (as defined under the Children and Young Persons Act) ** Full name may include his/her principle name, hanyu pinyin, alias, alias in hanyu pinyin, married name, name in ethnic characters (e.g. Chinese, Jawi, Tamil), whether in full or in parts.*
(b)	• **Identification information** (e.g. username or account number in combination with any required security code, access code, password or answer to security question) **used to permit access to or use of the individual's account** where the account can be subsequently misused for fraudulent transactions or to access any information in (a); OR - ***Comment:*** *We suggest removing "or to access any other information.* • **Signature or private key used by an individual to authenticate or sign an electronic / physical record** (e.g. signature, thumbprint). - ***Comment:*** *This is too broad as many documents may contain scanned signatures or similar. This should be more narrowly defined or include certain exceptions, such as for data that is generally collected for legitimate purposes outside of biometric identification. We also suggest removing "signature", and consider limiting to biometric information (e.g. iris scan, fingerprints)*