28 May 2020

Ms. Yong Ying-I
Permanent Secretary
Ministry of Communication and Information
140 Hill Street 301-01A, Old Hill Street Police Station
Singapore 179369
DataRegulation@mci.gov.sg

Mr. Tan Kiat How
Commissioner
Personal Data Protection Commission
460 Alexandra Road #10-02 PSA Building
Singapore 119963
corporate@pdpc.gov.sg

Dear Ms. Yong Ying-I and Mr. Tan Kiat How,

Public Consultation for the Personal Data Protection (Amendment) Bill

The Asia Securities Industry & Financial Markets Association (ASIFMA)[1] and its members strongly support Singapore's commitment to allowing financial services firms to transfer data across borders and opposition to data localisation requirements provided financial regulators have access to data needed for regulatory and supervisory purposes. Earlier this year, we noted the Monetary Authority of Singapore's and US Department of Treasury's joint statement on financial services data connectivity, as well as the Digital Economy Agreement (DEA) between Singapore and Australia.

The industry views these developments as important milestones representing thoughtful policymaking and inter-governmental collaboration, and commend Singapore for its ongoing efforts and leadership in embracing data innovation while protecting personal data privacy.

We take this opportunity to express our support for the overall policy direction reflected in the Ministry of Communication and Information's Personal Data Protection (Amendment) Bill while, in the appendix following, set out some specific comments in response to proposals in the consultation paper, including areas where the industry seeks clarification.

We appreciate the opportunity for participating in this consultation.

[1] ASIFMA is an independent, regional trade association with 130+ member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

ASIA SECURITIES INDUSTRY & FINANCIAL MARKETS ASSOCIATION | Unit 3603, Tower 2 Lippo Centre | 89 Queensway Admiralty, Hong Kong | Tel: +852 2531 6500 www.asifma.org

We also encourage Singapore to continue to play a leading role in the region in developing forward-thinking policy enabling data connectivity to support international financial services, and welcome the opportunity for continued engagement with the Ministry of Communication and Information (**"MCI"**) and the Personal Data Protection Commission (**"PDPC"**), including in relation to operational details as regulations and guidance materials are developed in the future.

If you have further questions or would otherwise like to follow up, please contact Matthew Chan, Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560.

Sincerely,

Mark Austen
Chief Executive Officer
Asia Securities Industry & Financial Markets Association

APPENDIX - COMMENTS

Section 6 – Deemed Consent by Contractual Necessity

Section 6 of the Amendment Bill provides that consent may be deemed to be given for the purpose of disclosure and use of the personal data by third-party organisations, including the collection and use of the personal data by such third-party organisations where it is reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation.

We welcome further guidance on the types of data (e.g. data relating to KYC/AML/ fraud) to which 'deemed consent by contractual necessity' will apply, particularly as it relates to the context of financial services firms seeking to enable effective compliance.

Section 7 – Deemed Consent by Notification

Section 7 of the Amendment Bill states that consent to process personal data may be deemed to be given if (i) the organisation provides appropriate notification to inform the individual of the purpose of the intended collection of personal data, with a reasonable period for the individual to opt-out of the collection, use, or disclosure of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period.

We note that reliance on this 'deemed consent by notification' requires an organisation to assess and ascertain that the intended collection, use, or disclosure of personal data is not likely to have any adverse effect on individuals after implementing measures. As such, we welcome further clarification on the concept of 'appropriate notification' and 'reasonable period' (including guidance on the form of notice, notice period and details required for opt-out) and 'adverse effect' in the Act, updated Regulations and/or new Guidelines.

We also note that 'deemed consent by notification', where given a reasonable opportunity to opt-out, is especially important for financial services firms to make decisions and categorise data with certainty. However, as it is unclear as to how the opt-out period should work (considering that collection of data often occurs at the same time or right after the individual gets informed about the purposes for collection of his personal data), we request clarity on this point, and further suggest that the opt-out provision be deleted as it will not be necessary if the data subject has the right to withdraw his consent anytime.

Further, we note that the proposed new clause 15(4) of the Act imports the concept of 'reasonable necessity'. In particular, an individual (P) who enters into a contract with an organisation (A) and provides personal data to A is deemed to have given consent to:

- A's disclosure of the personal data to another organisation (B) is deemed, where the disclosure is 'reasonably necessary', for the performance of a contract between P and A;
- the collection and use of that personal data by B, where the collection and use are 'reasonably necessary' for any purpose mentioned in paragraph (a);

- the disclosure of that personal data by B to another organisation where the disclosure is 'reasonably necessary' for any purpose mentioned in paragraph (a).

Whilst we note that the concept of 'reasonable necessity' must have a nexus with the purposes of the contract with P, or where the contract is in P's interest, we welcome further clarification on its meaning and application in the Act, updated Regulations and/or new Guidelines. Where global businesses are concerned, it is often necessary to rely on outsourced service providers and specialist services to benefit from economies of scale and leverage international best practices. We respectfully submit that the concept should be wide enough to embrace the example described as various value/supply chain partners essential in the performance of the contract.

Section 10 – Prohibitions to Providing Consent

Section 10 of the Amendment Bill states that in relation to the data access right, the Amendment Bill will now allow organisations to provide access to the requested data, regardless of whether providing access could (i) reveal personal data about another individual, or (ii) reveal the identity of an individual who has provided personal data about another individual and that individual does not consent to the disclosure of his/her identity.

Some of our members suggest this provision be deleted and maintain the current exception as it could have an adverse impact on internal investigations, and ultimately, possible compliance with the law. This may in fact refrain employees from reporting wrongdoings of colleagues, as their identity could no longer be kept confidential in case the data subject makes an access request to, for instance, interview notes. Other members interpret this differently as that the current amendment preserves the 5th Schedule 1(h) of the PDPA, which explicitly provides an exception against access requirement under section 21(1) in respect to personal data collected/used/disclosed without consent for the purpose of an investigation and associated proceedings and appeals have not been completed.

Given the ambiguity, we request further clarification on this point and welcome the opportunity to provide further comment once it has been clarified.

Section 12 – Notifiable Data Breaches

Section 12 of the Amendment Bill provides that a data breach is a notifiable data breach if it affects no fewer than the minimum number of affected individuals prescribed. The consultation paper further provides that the MCI and PDPC intends to prescribe in the Regulations a numerical threshold on what constitutes a significant scale.

Based on past enforcement cases, the PDPC notes that data breaches affecting 500 or more individuals would be an appropriate threshold. To this end, we would like to request that the significant scale not only be determined by the number of affected individuals, but for consideration of the circumstances to also be given (e.g. meeting a 'significant harm' requirements also).

Section 12 further states that an organisation must also notify, on or after notifying the Commission, each affected individual to whom significant harm results or is likely to result from a notifiable data breach except if (i) the organisation takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual or (ii) the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

We note that as currently drafted, it seems that exceptions listed under (i) and (ii) above apply only to the notification of the breach to the data subjects while notification to the Commission is still required. We request that the Bill considers extending the above exceptions also to notification to the Commission, such that if the measures listed in (i) and (ii) are adopted, the significant harm to the data subjects is excluded and the breach becomes not notifiable in the first place.

Lastly, **section 12** of the Amendment Bill states that notification to the affected individual is prohibited if it is so instructed by the PDPC or other prescribed law enforcement agency, or if it is not desirable. Under this point, it is unclear as to how and when the PDPC should inform the reporting organisation not to notify the affected individuals, which also seems to contradict the general prescription to notify the affected individuals as soon as practicable. It is also unclear as to whether it is actually the legislative intent of the Amendment Bill to confine the circumstances for the Commission to waiver notification to the affected individuals in accordance with section 26D(2), only to where an organisation has made an application under section 26D(2), but not otherwise. As such, it would be helpful to clarify how and when an organisation should await specific instructions from the PDPC before notifying the affected individuals.

Section 26E – Data Portability

We note that additional requirements will be prescribed for data porting requests and transmissions of personal data thereunder. The industry is of the view that broad data portability requirements should not be mandated and that market participants should play a part in the development of the ecosystem; therefore, while we welcome the development of practical regulations in order to build the data sharing framework and mechanism to help drive the industry towards common and interoperable standards, we do not think participation should be mandatory.

A broad implementation of the data portability right may impose excessive burdens on organisations and require unrealistic efforts from controllers in order to have the technical systems in place to facilitate the data portability right. We would like to further highlight that the portability obligation should ensure a level playing field between the entities obliged to share the data (data transmitters) and those with whom the data should be shared (data receivers), so that information can port in both directions. An absence of bidirectional flows of data has the potential to create competition concerns and so it is key that the principle of reciprocity be embedded within the data portability framework.

To this effect, it would be helpful if the Act, updated Regulations and/or new Guidelines could provide for, or clarify, the following:

(a) Users should be able to request that their provided and observed data (but not inferred data) be transferred directly from one data holder to another in a real-time, standardised way that allows them to maintain full control over the process and to leverage their data's economic value.

(b) A cross-industry framework as proposed by the PDPC would reflect the value of data beyond the firms where they were originally generated, and also of the increasingly blurred borders between firms operating in different sectors. Opening up data only in some sectors will reduce the benefits for end-users, who would be unable to combine data they themselves have generated across all industries.

(c) Data to be shared should cover all inputted and observed electronic data. That is, data that a user knowingly and actively provides (e.g. name, address) or produces through their use of a good or service (e.g. geolocation, energy use, search history). Data that has been inferred or derived from this should be excluded in order to protect the value creation performed by the firm holding the data and preserve incentives for new data-driven innovation.

(d) A number of building blocks are required in order to make all of the above a reality:

i. **an obligation on firms to make available a real-time, standardised sharing mechanism** - without a requirement to provide a mechanism to users there will be little action, as there are insufficient incentives for individual firms. To ensure sharing is easy and generates useable information, data should be shared in real-time, in common formats, with defined transmission mechanisms. For example, with Application Programming Interfaces (APIs) that follow agreed standards and taxonomies.

ii. **consent** - data should only be shared at the user's request and with their consent, where the receiving firm solicits the minimum data required. For personal data this should be fully aligned with data protection requirements.

iii. **security measures** - appropriate requirements would be needed to protect users from unauthorised sharing, for example by verifying their identity through a secure authentication process, and ensuring data is communicated securely.

iv. **licensing** - a small set of highly sensitive data, such as health or financial information, should only be accessible by firms with an appropriate license, with robust oversight.

v. **liability and redress mechanisms** - users should be able to understand who is responsible if something goes wrong and be able to easily seek redress.

(e) A porting organisation shall have no legal liability to the receiving organisation for the personal data. This is because (i) there is no contractual nexus between the parties, and (ii) an organisation that collects and uses personal data assumes responsibility for the personal data, including verification of the personal data and having to comply with the Accuracy Obligation under the PDPA.

(f) A **transmitting organisation** reserves the right to reject a porting request "if the request is otherwise frivolous or vexatious." (This is similar to the Access Obligation and PDPC's current advisory guidelines on individual's access to their personal data)

(g) A **receiving organisation** shall have a right to refuse the ported data, if the personal data is (a) not necessary for the conclusion of an agreement, performance of an agreement or the relationship between the receiving organisation and the individual, or (b) not relevant for the purposes of the receiving organisation. This is because the receiving organisation remains responsible for complying with the requirements under the PDPA when collecting personal data, including verification of consent or such other legitimate purposes and ensuring accuracy of the personal data from the relevant individual.

Section 29 – Financial Penalty

Section 29 of the Amendment Bill states that the amount of the financial penalty is 10% of the annual turnover for an organisation or a person with an annual turnover exceeding $10 million, or $1 million in any other case.

We note that the 10% of local annual turnover does not have a guideline or graduated scale for fine levels. If we compare to GDPR, the EU Regulation adopts a graduated scale of certain infringements attracting fines of up to 2%/$10 million Euros (whichever higher), and certain infringements attracting fines of up to 4%/$20 million Euros (whichever higher). This graduated scale may present organisations with an impression of the areas of compliance which have the highest importance and deserve immediate remediation, and we propose consistency with established regimes be considered in relation to the PDPA.

Section 31 – Legitimate Interests Exception

Section 31 of the Amendment Bill states that organisations can collect, use or disclose personal data in circumstances where it is in the legitimate interests of the organisation and the benefit to the public (or any section thereof) is greater than any adverse effect on the individual.

While we support the addition of "legitimate interests" as grounds for processing, it is not very clear as to how the assessment about the benefit to the public should work, especially since such legitimate interest exemption can only be invoked if the legitimate interest and benefit to the public is greater than the adverse effect on the individual. In reality, it would be difficult to understand the scope of acceptable benefits that are real and can outweigh the residual adverse effect, moreover, it could be challenging for organisations to factor in such assessment. We therefore request guidance to be published around the scope of this term, and would also like to suggest the assessment test be limited to the direct and/or indirect adverse effect the data processing could have on the impacted individuals.

We further note that the EU GDPR has provided guidance on the use of this term within recitals. In correlation, we appreciate if clarification could be provided that analysing individual creditworthiness, fraud prevention, and guaranteeing the security of the financial institution's network or system are

covered as discussed in the EU case [AEPD Gabinete Juridico (Informe 195/2017)]. Also, given that this ground might interact with Banking Secrecy obligations, it would be good to clarify the interrelationship between the PDPA legitimate interest grounds, MAS notice 654 and 626, and Banking Secrecy requirements. The industry welcomes further guidance around the circumstances, within the context of the financial services industry, in which the 'legitimate interests exception' and 'business improvement exception' can be relied upon, as the guidance would give firms confidence to rely on these ground.

General Point on Transitional Provisions and Sunrise Period

In light of the efforts that will be needed to update internal processes and comply with the new and significant requirements, we would recommend that the Act expressly provides for transitional provisions where the changes act can be implemented in phases. For example:

> *Phase 1:* Updated Do-Not-Call Provisions and New Data Portability Provisions will be effective 6 months from date the Amendment Act is passed in Parliament
>
> *Phase 2:* New Provisions requiring mandatory Data Protection Impact Assessments for Use of Personal Data, e.g. (i) Updated Deemed Consent Provisions and (ii) Legitimate Interests Exceptions will be effective 12 months from date the Amendment Act is passed in Parliament.
>
> *Phase 3:* New Breach Notification Provisions will be effective 18 months from date the Amendment Act is passed in Parliament.

The transition and sunrise period would also be helpful (i) to allow individuals and organisations to be educated on the new rights and obligations, and (ii) to allow organisations to regularise their existing contracts with data intermediaries to account for the new changes, the details of which are to be further provided under regulations or guidance.