asifma
Growing Asia's Markets

22 September 2017

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

Dear Commissioner Tan:

Re: ASIFMA response to the PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

The Asia Securities Industry and Financial Markets Association (ASIFMA)[1] is pleased to respond to the Commission's consultation on this important review of approaches to managing personal data under the Personal Data Protection Act 2012 (PDPA). With the assistance of Norton Rose Fulbright (Asia) LLP, we have set out in this letter our comments in response to the proposals in the paper.

We welcome the opportunity for continued engagement with the Commission on this issue. If you have further questions or would otherwise like to follow up, please contact Wayne Arnold, ASIFMA's Executive Director and Head of Policy and Regulatory Affairs, at warnold@asifma.org or +852 2531 6560.

Sincerely,

Mark Austen

Chief Executive Officer
Asia Securities Industry & Financial Markets Association

[1] ASIFMA is an independent, regional trade association with over 80 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

Comments

Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

1. Yes – ASIFMA supports this proposal. We are of the view that it is useful to have this as an alternative basis to collecting, using and disclosing personal data in the digital economy. Specifically, ASIFMA agrees that consent is often not practical or appropriate particularly as consent can be withdrawn, e.g. where Internet of Things devices are concerned.

Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (*i.e.,* impractical to obtain consent and not expected to have any adverse impact on the individual)?

2. ASIFMA notes that many other jurisdictions including Hong Kong are notice-based regimes, *i.e.* consent is only required if personal data is to be used for a new purpose and there are no conditions imposed on this requirement. We note that the Singapore PDPA permits deemed consent, however these provisions are often not robust enough for financial institutions to rely on and in certain circumstances, for example, where collection/use is pursuant to performing a contract/service for the individual (which is similar to an exemption under the EU's General Data Protection Regulation (**GDPR**)), notification of purpose should be sufficient in these circumstances without additional conditions. Financial institutions are increasingly subject to various transaction reporting and other disclosure requirements on a cross-jurisdictional basis and it is proving difficult and resource intensive to implement these (some of these reporting requirements may implicate data protection laws).

3. However, if conditions are to be imposed on the Notification of Purpose approach, ASIFMA broadly agrees with the conditions proposed by the Commission, save for a few aspects which are set out below.

Materiality

4. Under the current proposed conditions in paragraph 3.8(b) of the consultation paper, it would not be possible to rely on Notification of Purpose if there is an ***insignificant*** adverse impact on individuals. This would limit the circumstances in which Notification of Purpose may be relied upon by organisations to collect, use or disclose personal data. In our view, there should be an additional materiality threshold. Accordingly, Notification of Purpose should be permitted where the collection, use or disclosure of personal data is not expected to have any material adverse impact on the individuals determined by a risk and impact assessment conducted by the organisation.

5. With reference to paragraph 3.8(b) of the consultation paper, ASIFMA requests the Commission provide examples of adverse impact to clarify the Commission's expectations, e.g. selling of information to third parties. In particular, ASIFMA is of the view that this should be differentiated from decisions made to address legitimate risks to the organization, e.g. the decision to terminate an employment relationship due to fraud identified through monitoring.

Risk and impact assessment

6. With reference to paragraph 3.10 of the consultation paper, ASIFMA assumes that a single assessment could be used to assess multiple cases of collection, use and disclosure of personal data that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. ASIFMA requests that the Commission confirm that this is the intention. In addition, we propose that the assessment be updated where appropriate, e.g. if there is a change to processing of data could materially impact the risk profile of the collection, use or disclosure.

7. ASIFMA would also like the Commission to clarify whether risk and impact assessments will be subject to review by the Commission or the Singapore courts. In particular, we would like to know whether there would be any consequences (including penalties) imposed on organisations for arriving at the "*wrong*" conclusion in their impact assessments. In our view, in light of the multi-factorial nature of such assessments, the Commission should focus on whether an organisation has properly carried out the risk and impact assessments from a process standpoint, rather than focus on the outcome of such assessments.

8. We refer to paragraph 3.10 and 3.17 of the consultation paper. ASIFMA assumes that the risk and impact assessment can be completed at a frequency determined by the relevant organisation. In this regard, ASIFMA further assumes that financial institutions can leverage their internal risk methodology for such assessments under the PDPA, rather than any specified form of risk and impact assessment mandated by the Commission. ASIFMA requests that the Commission clarify whether these assumptions are correct. Further, ASIFMA requests that the Commission publish guidance on the key considerations in risk and impact assessments to provide consistency in approaching such assessments and to assist organisations in understanding the main outcomes desired by the Commission.

9. ASIFMA further requests clarification from the Commission that a risk and impact assessment will not be required in certain specific circumstances, such as:

   (a) Compliance with legal or regulatory obligations including codes, guidance and foreign laws and regulation including those of select other jurisdictions (including the EU) or international disclosures to foreign regulators;

   (b) Public interest, e.g., for prevention of cybercrime, terrorism/terrorism financing, financial crime and fraud;

   (c) Establishment, exercise or defense of legal claims; or

   (d) Contract performance.

Guidance from Commission

10. We ask that guidance (with various examples) be issued in relation to the interpretation of the conditions, particularly the terms "*adverse impact*" (and "*material adverse impact*" if a materiality threshold is included) and risk and impact assessment. In our view, the Commission should consider aligning such guidance with of the GDPR, to reduce costs for

organisations in complying with multiple different sets of regulations (although in our view, not all risk assessments under the PDPA need to be as high as GDPR standard *i.e.,* a less comprehensive/formal risk assessment should be appropriate in certain circumstances, e.g. in the case of low risk arrangements). We further ask that the Commission considers issuing a "*white-list*" whereby risk and impact assessments conducted in compliance with regulations of select other jurisdictions (including the EU) are deemed automatically acceptable for compliance under the PDPA (such as the examples listed in paragraph 9(a) to 9(d) above).

11. The issuance of guidance together with examples on these issues will encourage convergence among industry participants. We assume that the Monetary Authority of Singapore (**MAS**) will be consulted on such guidance so that sector specific guidance will be available to financial institutions. This will go a long way in reducing regulatory risk and reducing diverging practices in this area. As noted above, it would be helpful for the Commission to list the acceptable circumstances that will be considered to meet these conditions.

Data analytics and withdrawals of consent

12. ASIFMA notes that the intent of using Notification of Purpose as an alternative to consent is to encourage activities in the digital economy and to support innovation such as data analytics and machine learning. The nature of these activities is that organisations are often unable to determine whether the data being gathered is personal data and whether a specific individual has withdrawn his consent to its collection, use or disclosure. ASIFMA expects to see an increase in the number of individuals approaching its member financial institutions to issue blanket withdrawals of consent if the Notification of Purpose approach is signed into law. The cost and effort required to track these withdrawals would be significant.

13. Therefore, while ASIFMA welcomes the introduction of the Notification of Purpose approach, we propose that individuals should not be permitted to withdraw consent in relation to automated data-collection activities, including data analytics and machine learning, in order to meaningfully encourage the growth of such activities in Singapore.

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

14. ASIFMA supports this proposal.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

15. ASIFMA broadly agrees with the conditions proposed by the Commission, save for a few aspects which are set out below.

    (a) With reference to paragraph 3.15(a) of the consultation paper, ASIFMA proposes that this condition be amended to: "*it is not **practical,** desirable or appropriate to*

obtain consent from the individual for the purpose". As an example, internal company investigations often require the use of personal data of ex-employees. However, these ex-employees may be uncontactable. As there is a clear public benefit in allowing an organisation to investigate and remediate suspicious activities, organisations should be permitted to dispense with obtaining the consent of ex-employees' in such situations given that it would be impracticable to obtain consent.

(b) With reference to paragraph 3.15(b) of the consultation paper, ASIFMA proposes to remove the word "*clearly*". As long as the benefit to the public outweighs adverse impact or risk to the individual, this condition should be satisfied. In addition, we request that the Commission provide specific guidance on the types of 'benefit to the public' that would meet this condition, e.g. whether international disclosures to foreign regulators would be sufficient to meet this condition.

(c) As a general comment, ASIFMA supports these proposals but requests that the Commission issue guidance on in its interpretation of phrases such as "desirable", "*appropriate*" and "*adverse impact*" to give organisations sufficient comfort in relying on these exceptions to consent. We request that the guidance includes examples of Legal or Business Purposes which the Commission believes are in scope, will help the industry apply such assessment consistently. The assessment of what constitutes a valid Business Purpose may be applied more onerously by some entities but not others, hence having guidance will be very helpful to the industry. In particular, the Commission should confirm the circumstances that are in scope such as police/legal investigations, internal investigations of suspected fraudulent activities, managing human resources, preventing data leakage or to deal/detect/prevent cyber-attacks or threats and other IT constraints which cannot be avoided. We also request that the Commission clarify that Legal and Business Purposes are not restricted to compliance with Singapore laws/regulations given that organisations are subject to international laws and regulations obligations and supervision by third country regulators.

(d) As noted above, ASIFMA assumes that the MAS will be consulted on such guidance so there is sector specific guidance available for financial institutions.

Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to the Commission? Specifically, what are your views on the proposed number of affected individuals (*i.e.,* 500 or more) for a data breach to be considered of a significant scale to be notified to the Commission?

<u>Notification to affected individuals and to the Commission if the data breach poses any risk of impact or harm</u>

16. With reference to paragraph 6.2(a) of the consultation paper, ASIFMA is of the view that the Commission's proposal to require organisations to notify *both* affected individuals and the Commission if the data breach poses *any* risk of impact or harm to the affected individuals is too onerous.

17. ASIFMA notes that in some situations, the risk of impact or harm of a data breach to affected individuals may be minimal or insignificant, e.g. if the nature of the breach itself is

unlikely to result in actual access or use of the data by a third party (e.g. in a Ransomware attack) or if the data breach was discovered early and sufficient migratory measures had been put in place to minimize such risks. In such situations, it is unlikely that affected individuals will need to take steps to protect themselves from such risks. Notification may instead cause undue concern to such individuals. Similarly, ASIFMA is of the view that notification to the Commission is unnecessary where risk of impact or harm to affected individuals is minimal because it is unlikely that substantial post-breach remedial actions are required.

18. Instead, ASIFMA proposes that a materiality threshold be introduced, *i.e.,* that affected individuals and/or the Commission be notified only if the breach poses a material risk to the affected individuals or if the nature of the breach is material. In this regard, ASIFMA notes that the materiality approach is consistent with the GDPR mandatory notification requirements for data subjects, which is based on whether the breach is likely to result in a "*high risk*" to the data subjects' rights and freedoms. In this regard, ASIFMA further proposes that materiality be assessed in the context of a risk-based approach and that the Commission should consider allowing organisations to take this into account when organisations conduct an overall risk and impact assessment, rather than designate specific types of personal data as material. In our view, this approach would be preferable in that it focuses on breaches that may result in actual impact or harm and minimizes notification fatigue on organisations, individuals and the Commission, and would not unduly and/or unnecessarily increase compliance costs.

Notification to the Commission where the scale of the data breach is significant, *i.e.,* involving 500 or more affected individuals

19. With reference to paragraph 6.2(b) of the consultation paper, ASIFMA is of the view that the Commission should not introduce a notification requirement that is based on the scale of breach. In our view, the scale of the data breach *alone* is not an accurate gauge of whether the organisation faces any systemic issues. In some instances, a significant data breach may be caused by technological vulnerabilities not within the organisation's control, e.g. breaches due to inherent vulnerabilities in third-party programs. In any event, whether a breach involving 500 or more affected individuals should be considered significant depends on the size of the organisations and their customer bases as well as other factors such as the nature of data involved in the breach. It would not be appropriate to simply pick 500 as a figure.

20. Instead, ASIFMA proposes that a mandatory notification regime based on materiality (see above at paragraph 18) would be more appropriate. When considering materiality, the number of affected individuals will be one of multiple factors to be considered.

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

21. ASIFMA is of the view that the Commission's proposed concurrent application of PDPA's data breach notification with that of other laws and sectoral regulations is too onerous.

22. ASIFMA notes that financial institutions are currently subject to extensive supervision by its sectoral regulator, the MAS on such matters. In addition, many of ASIFMA's members are

likely to be designated as Critical Information Infrastructure (**CII**) owners and may therefore also be supervised by the Cyber Security Agency (**CSA**) in due course. Notification to the MAS and the proposed notification regime to the CSA should be adequate to ensure that data breaches in the financial industry are mitigated promptly and satisfactorily. The PDPA's proposed concurrent application of PDPA's breach notification requirements would simply increase the compliance burden on financial institutions.

23. Therefore, ASIFMA proposes that financial institutions be exempt from the proposed concurrent application of PDPA's data breach notification requirements.

24. In the alternative, if the Commission considers concurrent application to be necessary in order for the Commission to fulfil its broader public objectives, ASIFMA proposes that the Commission considers streamlining the notification and reporting process such that financial institutions need only have a single set of reporting requirements and can deal with a single point of contact in order to fulfil such obligations. In this regard, ASIFMA further proposes that the Commission consider the approach of appointing Assistant Commissioners that are officers from "*Sector Leads*", *i.e.,* government lead agencies in charge of each sector. Therefore, in the case of the financial industry, Assistant Commissioners would come from the MAS, who would already be familiar with the existing MAS regulatory framework and prevent financial institutions from having to report to yet another regulator on overlapping matters. This approach is also consistent with the approach proposed by the CSA and the Ministry of Communications and Information in the public consultation paper on the draft Cybersecurity Bill. In this regard, ASIFMA urges the Commission to consider engaging the industry in an industry-specific consultation to consult on this issue. Given the regulatory and compliance burden that financial institutions are currently subject to, ASIFMA welcomes any initiative to relieve the compliance burden of financial institutions.

Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

25. With reference to paragraph 6.6 of the consultation paper, ASIFMA requests that the Commission clarify whether this requirement applies to data intermediaries that are overseas service providers. In addition, ASIFMA proposes that data intermediaries should also be required to report data breaches to the Commission, particularly if the data breach affects multiple organisations that would meet the notification requirements on an aggregate basis. In this regard, organisations ought to be allowed to rely on data breach notifications made by data intermediaries to meet the relevant breach notification requirements under the PDPA.

26. With reference to the proposed exceptions and exemptions set out in paragraph 6.9 – 6.10 of the consultation paper, ASIFMA broadly agrees with the proposed exemptions and asks that the Commission clarify the following:

    (a) What the Commission considers to be a "*encrypted to a reasonable standard*" and whether it would provide examples for how such a standard is to be met. For example, would encoded or masked fields suffice in order to meet such a standard?

(b) What an organisation should do in the event that it has assessed that the breached personal data has been "*encrypted to a reasonable standard*" and thus did not notify the affected individuals of the breach, but later discovers that the breach personal data has been decrypted and accessed by unauthorized third parties?

27. In addition, ASIFMA proposes that the Commission consider including two further exceptions / exemptions:

(a) Notification is not required if the breach is unlikely to result in a material risk of impact or harm to the affected individuals.

(b) Notification to affected individuals is not required if the burden of individual notification is disproportionate to the risk of impact or harm to the affected individuals.

(c) Notification to affected individuals is not required if subsequent measures have been taken such that risk of serious harm to data subjects is adequately mitigated and unlikely to materialize.

(d) Notification to affected individuals is not required if disclosure is subject to subject to other secrecy provisions or laws prohibiting disclosures.

(e) Notification to affected individuals is not required if disclosure is necessary for the protection of the individual or rights and freedoms of others.

28. With respect to notification to affected individuals, ASIFMA is of the view that an organisations can determine the form and method of notification to the affected individuals, where notification is required, and that the Commission would not impose penalties if it determines that the form and method of notification to be inadequate. For example, some organisations may adopt a publicity campaign of a breach inviting individuals to approach the organisation if they suspect that they have been affected by the breach would satisfy the data breach notification requirements in respect of affected individuals depending on the scale and nature of the breach.

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

29. In the event that the Commission does not wish to exempt financial institutions from the proposed concurrent application of PDPA's data breach notification requirements, ASIFMA is of the view that in light of the MAS data breach notification requirements that financial institutions are currently subject to, financial institutions should not be subject to the proposed time frames for data breach notifications to the Commission. As stated in paragraph 24 above, ASIFMA is of the view that in respect of financial institutions, any concurrent notification requirement to the Commission should be streamlined with that of MAS, as the sectoral regulator for financial institutions. Therefore, any proposed time frame for data breach notification should also be streamlined with MAS' such that financial institutions need only comply with a streamlined set of requirements on such matters.

30. In the alternative, should the Commission wish to impose distinct time frames for data breach notifications for notifications to the Commission, we are of the view that the 72-hour time frame is too short for the following reasons:

(a) Data hosting and processing are outsourced in many organisations. Even if such activities are not outsourced, the relevant department is often situated some distance away geographically from the main operational offices of the organisation. Accordingly, the process from detection to escalation to notification would take some time, even if expedited.

(b) The process of assessing the nature and impact of data breaches itself is time-consuming and would require the input of personnel of different expertise, e.g., IT for technical knowledge, Legal / Compliance in relation to the relevant regulations.

(c) While it is possible to send an interim notification within 72 hours and then remaining information later after confirming the breach and obtaining further details, we submit that this would cause inefficiencies in the use of resources, both in the organisations and the Commission. For example, organisations may have to send notifications to meet the 72-hour deadline without having had the opportunity to ascertain whether it meets the criteria for notification, which the Commission would have to process and review, only to conclude subsequently that such criteria had not been met and therefore notification was not required.

(d) Instead, ASFIMA proposes that organisations should be given five (5) working days from the time the assessment of the data breach is complete.

As for the notification of affected individuals, ASIFMA agrees that individuals should be notified on a "*as soon as reasonable*" basis. This is because once the affected individuals are notified, it is likely an organisation would be required to devote significant resources to addressing and managing them. If the proposed time frame is too short, this may put unnecessary pressure on an organisation's resources, which could be better utilized to manage the breach itself. The strain on the organisation's resources may impair the organisation's ability to manage affected individuals and breed unnecessary discontent among them. An "*as soon as reasonable*" basis is preferred because it gives an organisation sufficient time to organize its resources and manage the affected individuals in a satisfactory manner. Furthermore, organisations also require time to ascertain the true extent and impact of the breach. The "*as soon as reasonable*" basis provides organisations with the opportunity to do, rather than rush to notify individuals and cause unnecessary alarm. In this regard, the determination of the "*as soon as reasonable*" basis could also be addressed by the organisation in its overall risk and impact assessment.