Taylor Vinters Via

5 October 2017

Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963

BY EMAIL ONLY

TAYLOR VINTERS VIA LLC'S FEEDBACK FOR PDPC'S PUBLIC CONSULTATION ON APPROACH TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

COVER PAGE

1 The Personal Data Protection Commission ("PDPC") invited the public to provide feedback on the proposed approach and amendments to the Personal Data Protection Act.

2 We have prepared the below comments and feedback for your consideration.

3 We are a local law firm that specializes in TMT (technology, media & telecommunication) law and IP (intellectual property) law, with a focused commitment to support innovative and entrepreneurial businesses. We also enjoy a cross-ownership structure with the UK-headquartered law firm Taylor Vinters LLP.

4 Many of our clients are multinational tech companies and our comments are based on our clients' queries and concerns.

5 Should you wish to contact us, our contact details are as follows:

Taylor Vinters Via LLC
152 Beach Road, Gateway East
#10-08
Singapore 189721
6299 0212
www.taylorvintersvia.com

TABLE OF CONTENTS

STATEMENT OF INTEREST

6 Our clients include international businesses that set up data centres in Singapore and/or collect personal data of individuals from around the world that are processed in Singapore. For example, multinational corporations that utilize Singapore as their headquarters for the ASEAN region. We also represent vendors/intermediaries who provide software or systems to manage the personal data of individuals around the world, e.g. notification systems to alert all its customer's employees across the world. We also advise foreign businesses on entering the Singapore market and the relevant privacy laws that may impact them; and conversely local businesses that are entering into foreign markets.

7 Accordingly, the proposed amendments will have significant impact on our clients, their commercial interests and their international privacy policies. We have made several recommendations or requests for clarifications in the interest of our clients.

SUMMARY OF MAJOR POINTS

8 We suggest a greater alignment of the PDPA with the privacy laws of other major jurisdictions and international standards. Many of our international clients have obligations in other jurisdictions, be it contractual or regulatory, to maintain certain levels of data

protection. As they will align themselves with the jurisdiction that has the strictest privacy/personal data law, the introduction of an enhanced framework may have limited impact in attracting data analytic talent into Singapore. Instead, if Singapore appears as a jurisdiction with weak data protection laws, this may deter foreign businesses with existing data protection obligations from entering into Singapore in that Singapore maybe seen as providing less than "adequate level of protection for the rights and freedoms of data subjects" for the purposes of transfer of data across borders (as required by other countries such as the EU and UK).

9 We are cognizant that the PDPC hopes to encourage more data sharing and data analytic activity in Singapore through the enhanced framework. We suggest that the current legislation can be refined to achieve that end.

10 For the proposed 'Notification of Purposes' basis, we are of the view that there are existing provisions in the PDPA that adequately address the driving concerns behind the proposal. Accordingly, we do not support the proposed addition of a 'Notification of Purpose' regime. Instead, the PDPC may wish to amend the existing legislation to better address data analytics.

11 For the 'Legal or Business Purpose' basis, the current proposal appears to be too broad and undefined, and significantly diminishes the privacy rights of individuals. We propose that narrower exceptions be added into the Second, Third and Fourth Schedule of the PDPA. We also propose that organizations should be required to notify the data subjects if they wish to proceed on the 'Legal or Business Purposes' basis, as data subjects will then have the ability to object or challenge whether the purported use correctly falls within the exceptions.

12 For the proposed Mandatory Data Breach Regime, we are supportive of its introductions and the PDPC's endeavours to align our regime with other major jurisdictions. However, we suggest the following amendments and/or seek further clarifications:

12.1 Further clarity on what constitutes a significant data breach;

12.2 The scale of the breach to be a non-exhaustive factor in assessing whether the data breach is significant;

12.3 Regarding the proposed concurrent application of breach notification, for the relevant authorities to collaborate and produce a standard notification report where specific information required by the different authorities can be attached as an appendix;

12.4 The Singapore's data breach notification regime to be applied concurrently with the mandatory data security breach notification regimes of other jurisdictions;

12.5 The proposed time frame for data breach notifications to commence from the point where the data organization should reasonably have known that the data breach is significant.

13 We are not supportive of the two proposed exemptions from the mandatory data breach notification regime.

14 We would also like to take the opportunity to suggest that the PDPA be amended to address the rise of giant data intermediaries. As data organizations may not have the necessary bargaining power to require the data intermediaries to comply or to provide further information, the PDPA should shift more duties onto such data intermediary and/or introduce a white mark regime for such data intermediaries.

COMMENTS

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

15 We are of the opinion that the PDPC should not provide for 'Notification of Purposes' as a basis for the **collection** of personal data without consent.

16 If the data organization is able to notify the data subjects of the purpose, we are of the opinion that the organization will also be able to collect consent or the concept of 'deemed consent' will most likely apply at the point of collection (i.e. if the data subject continues to provide the personal data after being notified, then the data subject is deemed to have given his consent).

17 Conversely, if it is impractical for a data organization to obtain consent form the data subjects, it would most likely be impractical for the data organization to provide meaningful notification of purpose (e.g. the operator of a drone that is monitoring a heavy traffic area).

18 As for PDPC's suggestion that 'Notification of Purpose' could be a basis for the **use** and **disclosure** of personal data without consent, we seek further clarification from the PDPC on the envisioned amendments to the PDPC.

19 We note that there are already provisions in the PDPC that are similar to the proposed regime. Paragraphs 1(i) and 2 of the Third Schedule and Paragraphs 1(q) and 4 of the Fourth Schedule of the PDPA already provide that personal data can be used and disclosed without the consent of the data subject *and* without notifying the data subject (Section 20(3)(b) of the PDPA) if:

19.1 The personal data is being used for a research purpose, including historical or statistical research;

19.2 The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

19.3 It is impractical for the organization to seek the consent of the individual for the use;

19.4 The personal data will not be used to contact persons to ask them to participate in the research; and

19.5 Linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clear in the public interest.

20 From the consultation paper, we understand that the main motivation behind the proposed amendments is to enable data organizations to carry out data analytics. We believe that the current provision already provides for this. Alternatively, we are supportive of an amendment to the existing provision to make express reference to data analytics and data mining (similar to the recent proposed "text and data mining" exception for the Copyright Act).

21 We are also supportive of the retention of the requirement that the personal data should be anonymized as much as reasonably possible.

22 Regarding the example of deploying recording devices or drone in high traffic situations that are likely to capture personal data, we are of the opinion that the PDPA already caters for such scenarios. We note that:

22.1 Such actions are most likely carried out by a public agency or an organization acting on behalf of a public agency hence the obligations of the PDPA will not be imposed on them;

22.2 The deployment of recording devices or drones in high traffic situations will likely already enjoy the "publicly available data" exception under the PDPA; and

22.3 For private organizations, such recording devices are most likely to be used for organized events (e.g. fairs or concerts) and notification can be given and consent can be practically obtained when individuals are buying the ticket.

23 **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)?**

24 As per our answer above to Question 1, we are of the opinion that the PDPA should not provide the 'Notification of Purpose' basis as an exception of the consent requirement for collection of data.

25 For the 'Notification of Purpose' basis for the use and disclosure of personal data without consent, we suggest that:

25.1 If the proposed enhancement is to be carried out as an amendment to the Third Schedule and Fourth Schedule of the PDPA, it should be clear that Section 20(3)(b) of the PDPA does not apply and notification of purpose should be provided;

25.2 similar wording to the existing Paragraph 2 of the Third Schedule and Paragraph 4 of the Fourth Schedule should be used to avoid confusion, and

25.3 there should be further clarification on what constitutes harm to the individual (as reflected in Paragraph 2(d) of the Third Schedule and Paragraph 4(d) of the Fourth Schedule).

26 For example, data being used to increase targeted marketing at an individual does not adversely impact the individual but an individual may not want to be targeted in such a manner; or individuals may not want targeted messages to be sent to them that may reinforce their confirmation bias.

B. Questions 3 and 4: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification? 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)?

27 In general, we do not support the proposed 'Legal or Business Purpose' basis for collecting, using and disclosing personal data without consent and notification. The current proposal may lead to a significant diminishment of privacy rights of the individual.

28 We are supportive of the adoption of a similar provision to the 'Legitimate Interests' provision of the GDPR to support a wider adoption of data analytics. Unlike the proposed 'Legal or Business Purpose' basis, the 'Legitimate Interests' provision of the GDPR (a) requires the data organization to notify individuals of the purported purpose and (b) upholds a higher standard on what constitutes a legitimate purpose.

29 The 'Legitimate Interests' test weighs whether the legitimate interests are overridden by an individual's *fundamental rights to personal data protection*. On the other hand, the Legal or Business Purpose can be invoked when benefits to the public (or a section thereof) clearly outweighs any *adverse impact or risks to the individual*. When analyzing the rights of the individual, assessing an adverse impact or risk is a lower standard compared to the *fundamental* rights of autonomy and privacy. Further, the 'Legal or Business Purpose' basis suggests that there are fundamental rights that absolutely cannot be denied whereas the 'Legal or Business Purpose' basis suggests that there are no unfettered rights for individuals.

30 We suggest that notification should still be necessary so that individuals can challenge or object to the purported 'Legal or Business Purpose'. Even if consent cannot be withdrawn, individuals may still have grounds to object. This is also the position for the EU Directive[1] ("EU Directive") and the GDPR.

31 Article 29 Data Protection Working Party ("A29WP") has also released an opinion on 'Legitimate Interest' grounds as set out in the EU Directive.[2] The A29WP hails a transparency policy as a form of best practice and as it is closely linked to the notion of accountability.[3]

32 The GDPR goes even further to incorporate such best practices as law. At Art 7.1(d) of the GDPR, controllers must inform the data subject of the 'legitimate interests'. At Art 21 of the GDPR, individuals have a right to object. Upon an objection, the organization is required to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedom of the individual before he may proceed to process the personal data further.

33 We understand that there are concerns that data subjects may suffer from 'notification fatigue' if they are bombarded with numerous notifications from organizations. However, we suggest that this can be adequately addressed if organizations adopt the principle of 'privacy by design' into their systems. Technology has evolved in recent years so that organizations and customers are given more avenues to communicate, and notification can be given in a manner that is effective. For example, Gmail's interface has changed in recent years to provide for several tabs: 'Primary', 'Social', 'Promotion', 'Updated', etc. This helps consumers to better sort their mail and information, and reduce notification fatigue. Instead of completely removing the need for consent, perhaps less emphasis can be placed on the "opt-in" mechanism.

34 The proposed 'Legal or Business Purposes' basis suggest a shift in counterbalances that may result in Singapore being seen as providing inadequate levels of protection for the rights

---

[1] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995, at Articles 10 and 14.
[2] Opinion 06/2014 of the Article 29 Data Protection Working Party of 9 April 2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
[3] Opinion 06/2014, at p 43.

and freedoms of data subjects. This may affect the ability of tech MNCs to transfer data from other jurisdictions into Singapore, or dissuade businesses with stricter privacy policies from entering into the Singapore market.

C. Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? 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 PDPC?

35 Regarding the criteria of risk of impact or harm to affected individuals, we understand that the PDPC will be formulating guidelines and agree that these underlying principles - (i) the type of data that has been breached and (ii) whether notification will enable affected individuals to take steps to protect themselves – are sound cornerstones to base guidelines on.

36 Regarding the criteria of a significant scale, there may be breaches where an organization is not able to establish the number of affected individuals. An organization may have detected a breach in their systems, but is unable to assess the precise number of affected individuals. A recent example would be the Instagram breach in late August 2017 where hackers were able to access the contact details of high-profile individuals. In Instagram's CTO's blog post, he said "we cannot determine which specific accounts may have been impacted". Another pertinent example would be the recent Equifax data breach in September 2017 where Equifax had difficulty identifying and notifying affected individuals.

37 An additional criteria could perhaps be the *type* of breach. For example, if there is evidence that a hacker had only viewed the personal data but not taken a copy, the former would be less severe.

38 We suggest that the three criteria above be taken jointly in deciding whether the notification requirement be triggered.

39 We also suggest that there should be a lower threshold for the data breach notification requirement to the PDPC. From the recent report data breach incidents, data organizations will normally require a substantial amount of time to discover the full details and extent of a breach. Once the lower threshold has been reached, the data organization should be required to notify the PDPC so that the PDPC can provide guidance and assistance to the data organization in managing the data breach.

D. 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?

40 While we appreciate the proposed concurrent application, we are concerned that breach notification requirements for other sectoral regulations may require a different set of information from the notification to the PDPC. For example, notifications to the PDPC will require information on the data subjects, whereas notification to MAS will require a description of the impact of the incident on the bank's compliance with laws and regulations applicable to the bank. In other words, the different authorities will naturally have different concerns and a singular report may not adequately address the other authority's concerns. We suggest that the government agencies collaborate and produce a standard notification report to be used for all breach notification requirements (e.g. general information on the details of the breach) but different appendixes to be attached for the different authorities (e.g. appendix on bank compliance, appendix on personal data affected, etc).

41 We would also like to propose a concurrent application of PDPA's data breach notification requirements with the mandatory data security breach notification regimes of other jurisdictions (e.g. UK, US, Australia, EU, etc), where possible. This will allow tech MNCs to report to the privacy authorities in multiple jurisdictions in an efficient manner and utilizing one singular report.

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

42 Regarding the proposed law-enforcement exception, we suggest that a delayed notification requirement would be more appropriate rather than a complete exemption. Organizations should still be required to notify individuals as soon as practicable (i.e. as soon as it no longer impedes investigations and/or there is unlikely to be investigations subsequently).

43 Regarding the proposed exemption where personal data has been encrypted, we understand that an organization would not be able to determine whether the encrypted personal data would be decrypted and hence compromised. Accordingly, we suggest that notification should still be required. Further, individuals may still wish to know about data breaches so that they can take pre-cautionary actions. Cybersecurity attacks may come in

waves – individuals may wish to have the choice to withdraw from the system before another attack

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

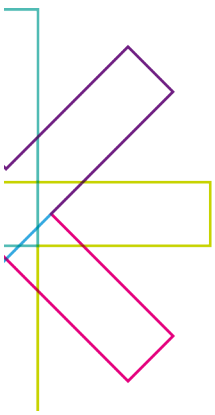
44 We are supportive of the PDPC's proposal that notifications to individuals should be as soon as practicable as this will allow organizations sufficient time to gather the necessary information and carry out thorough investigations.

45 In response to PDPC's proposed cap of 72 hours for data breach notifications to PDPC from the point of awareness of the breach, we suggest that the time frame should take into account that data organizations may not have the full facts and details of the breach at the time of detection. For example, a data organization may have detected the data breach but initially thought that it was not significant. Upon further investigation and analysis, more information of the breach may come forth and the data organization may only realize that it was a significant data breach weeks after the point of detection. Accordingly, the PDPC may wish to consider allowing the time-frame to start from the point that the data organization is sufficiently knowledgeable of the details of the data breach that it ought to reasonably have known that it met the criteria for notification.

G. ADDITIONAL COMMENTS

46 We would also like to take this opportunity to provide further feed back on the legal duties of data intermediaries and data organizations. Currently, data intermediaries are only required to comply with Section 24 and Section 25 of the PDPA, but a data organization is required to have the same obligations under this Act in respect of personal data being processed on its behalf by a data intermediary as if the personal data was being processed by the organization itself.

47 With the rise of major tech companies and large-cloud service data intermediaries that possess a significant amount of bargaining power, there is an increasing need for white marks for data intermediaries. However, white marks should apply only to large-cloud storage data intermediaries, and not cloud-based software as a service providers/vendors.



H. CONCLUSION

48 We are supportive of amendments and revisions to the PDPA to ease the regulatory burdens of business and allow for more data analytics and data sharing activities to be carried out in Singapore. However, to further strengthen Singapore's position as an international commercial hub and to attract more tech-focused MNCs into Singapore, it is also important to maintain robust personal data protection laws.

Yours truly

Yingyu Wang | Ruth Ng | Ahmad Firdaus Daud
Director | Associate | Senior Associate
yingyu.wang@taylorvintersvia.com| ruth.ng@taylorvintersvia.com |
a.firdaus@taylorvintersvia.com