Submission of Comments to the Personal Data Protection Commission

Public Consultation for Approaches to Managing Personal Data in the Digital Economy (issued 27 July 2017)

Submitting Organisation:

Clifford Chance Asia, a formal law alliance between Clifford Chance Pte Ltd and Cavenagh Law LLP.

Contact Persons:

Lena Ng, Partner

Direct dial: +65 6410 2215

Email: lena.ng@cliffordchance.com

Janice Goh, Counsel

Direct dial: +65 6661 2021

Email: janice.goh@cliffordchance.com

Date of Submission:

5 October 2017

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

1. We welcome the Personal Data Protection Commission ("**PDPC**")'s proposal to provide for Notification of Purposes as a basis for collecting, using and disclosing personal data without consent.

Comments to 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. Our view is that the Notification of Purpose approach should be subject to conditions, in order to distinguish between when consent is required and when Notification of Purpose would suffice. Without such conditions, it would be unclear to organisations when consent is required, and when Notification of Purpose would suffice.

3. However, the proposed conditions set out at the Consultation Paper are not sufficiently clear, for the reasons explained below.

4. In relation to the proposed condition where it is "*impractical to obtain consent*" – it would be unclear to organisations as to when exactly the threshold of "*impracticality*" would be met. There could be a variety of reasons why it might be "*impractical*" to obtain the consent of an individual. For example, technically, it might be "*impractical*" to obtain the consent of an individual, if the organisation is of the view that the individual is not likely to provide his consent. On the other hand, it might also be "*impractical*" to obtain the consent of an individual, if the individual is not contactable.

5. Accordingly, we suggest that the PDPC provides more guidance on the circumstances in which it is "*impractical to obtain consent*" of an individual.

6. In relation to the proposed condition where the collection, use or disclosure of personal data is "*not expected to have any adverse impact on the individuals*" – again, it would be unclear to organisations as to when exactly the collection, use or disclosure of personal data may have an "*adverse impact on the individuals*". It is also unclear what amounts to an "*adverse impact on the individual*". Specifically:

    a. We would be grateful if the PDPC could clarify when such "*adverse impact*" is to be assessed. For example, it is possible that an organisation could initially collect, use and disclose personal data of an individual without any "*adverse impact*" on the individual. However, subsequently, circumstances may change, such that the organisation's continued collection, use and disclosure of the personal data may result in an "*adverse impact*" on the individual. It would be helpful if the PDPC could clarify whether the organisation is expected to continually assess the situation, and what is required of organisations in the event that the circumstances change. For example, would the organisation be required to obtain the consent of the individual in such an event, and if so, is there any specific timeframe by which the individual's consent must be obtained?

b. We note that paragraph 3.8(b) of the Consultation Paper has elaborated that "*adverse impact*" would include circumstances where the personal data will be used to make a decision about the individual that may have an adverse impact on the individual, or to circumvent a prior withdrawal of consent. While such clarification is helpful, we think that the position would be more clearly set out if the PDPC could provide guidance on when there would be no such "*adverse impact*". Potential examples could include where the personal data is collected, used or disclosed only for data analytics purposes, or where the collection, use or disclosure is necessary to provide a contractually agreed service from the organisation to the individual.

Comments to 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?

7. We welcome the PDPC's proposal to include additional grounds for the collection, use and disclosure of personal data without consent and notification.

8. However, we note that the proposed concept of "*Legal or Business Purpose*" in the Consultation Paper has been fused and may potentially cause confusion. In this regard, we suggest that the PDPC considers simplifying the concept by adopting an exception which is expressed to pertain to "*legitimate interests*" instead, which more accurately captures the intent of this concept. We elaborate on our views below.

9. In relation to *"Legal Purposes*" –

    a. We note that the PDPA already states at Section 4 that Parts III to VI of the PDPA will not apply to the extent that other written law is inconsistent with those provisions.

    b. Further, the exceptions to the consent requirement at the Second, Third and Fourth Schedules to the PDPA also include that where the collection, use or disclosure of personal data is "*necessary for any investigation or proceedings*".

    c. It is therefore unclear what the concept of "*Legal Purpose*" is, as the PDPA appears to already provide for the collection, use or disclosure of Personal Data without consent in order to comply with legal requirements upon the organisation.

    d. We would therefore welcome the PDPC's clarification as to what "*Legal Purpose*" is intended to capture, in view of the current provisions in the PDPA. (For example, would "*Legal Purpose*" be broad enough to encompass compliance with foreign laws applicable to the organisation.)

10. In relation to "*Business Purposes*" –

    a. Our view is that the term is potentially misleading (although conditions may be imposed), given that in most instances, personal data is collected, used or disclosed by organisations for business purposes.

11. In this regard, we suggest that the PDPC considers simplifying the concept, by adopting an exception which is expressed to pertain to "*legitimate interests*" of the organisation.

For example, in the EU, organisations do not need to obtain the consent of individuals if they have a "*legitimate interest*" in processing the individual's personal data which outweighs the individual's rights to personal data protection (see paragraph 3.12 of the Consultation Paper). In this regard, we suggest that the PDPC provides guidance either in the PDPA itself or by way of Guidelines to be issued to clarify what are the circumstances which amount to such "*legitimate interests*", as further explained below.

12. In relation to whether notification is required – for a more balanced approach and as a safeguard to individuals, we suggest that the PDPC considers requiring organisations to notify individuals that their data is being collected, used or processed for such "*Legal or Business Purposes*" / "*legitimate interests*", unless the thresholds similar to that set out at paragraph 3.8 of the Consultation Paper are met.

Comments to 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)?

13. We agree that the proposed "*Legal or Business Purpose*" approach (which we have suggested above to be expressed as an exception pertaining to "*legitimate interests*" instead) should be subject to conditions.

14. In relation to the condition at paragraph 3.15(b) of the Consultation Paper:

    a. Our view is that it should be broadened to include the benefits to the organisation. As stated at paragraph 3.12 of the Consultation Paper, in other jurisdictions such as the EU and the Republic of Korea, organisations are able to collect, use and disclose personal data of individuals without consent if the legitimate interests of the organisation outweigh that of the individual's rights to personal data protection. Such legitimate interests of the organisation include enforcing a legal claim, preventing fraud, monitoring employees for safety or management purposes, and conducting scientific research.

    b. As stated above, we suggest that the PDPC provides guidance either in the PDPA itself or by way of Guidelines to be issued to clarify what are the circumstances which amount to such "*legitimate interests*". Such clear guidance would allow organisations to assess whether the circumstances fall within such "*legitimate interests*", and would prevent organisations from applying a liberal approach which may be potentially self-serving and compromising the interests of individuals.

Comments to 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?

15. In relation to paragraph 6.2(a) of the Consultation Paper - we broadly agree with the PDPC's proposal that affected individuals and the PDPC be notified, if a data breach poses any risk of impact or harm to affected individuals.

16. In relation to paragraph 6.2(b) of the Consultation Paper:

    a. We are also in broad agreement with the PDPC's proposal at paragraph 6.2(b) that organisations should notify the PDPC where there is a significant scale of breach.

    b. However, we do not think that it is useful or relevant to designate a particular number of affected individuals as a threshold test (whether 500 individuals or otherwise). This is because the number of affected individuals may not be representative of the scale of the breach – for example, the breach may be caused by an isolated one-off incident and is not related to any systemic issue within the organisation. In addition, the number of individuals affected is relative to the significance of the breach and varies across organisations – for example, 500 affected individuals in relation to a large company with millions of customers may hardly be considered to be of significance. On the other hand, 500 affected individuals in relation to a small company with only thousands of customers may be considered significant.

    c. Instead, we suggest that the PDPC considers requiring organisations to notify the PDPC of a breach, if the breach has a severe and widespread impact on the organisation's operations or materially impacts the organisation's service to its customers. Such a threshold would be similar to the reporting requirement to the MAS under the MAS Notice on Technology Risk Management (Notice No. 644).

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?

17. We agree with the PDPC that concurrent application would minimize the effort and cost involved to comply with notification requirements for the same data breach.

18. However, it would be of more convenience to organisations, if organisations only need to report to one regulator for the data breach. For example, it would be helpful if the organisation need not inform the PDPC of the data breach, if it is already informing the MAS of the data breach under the MAS Notice 644. In this regard, we request the PDPC to consider if a streamlined nation-wide system could be implemented, such that only one regulator needs to be informed of the data breach instead of the organisation having to inform multiple regulators or agencies of the same breach.

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

19. We agree with the proposals of the PDPC set out at paragraphs 6.9 to 6.11 of the Consultation Paper.

20. However, we would suggest that the PDPC considers expanding the exception relating to law enforcement to that of other jurisdictions. As a data breach is likely to have cross-border implications, law enforcement agencies in other jurisdictions may similarly impose a requirement on the organisation that affected individuals should not be notified of the data breach, if notification is likely to impede their investigations.

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

21. We agree with the PDPC that it is not necessary to impose a specific timeframe in relation to the notification to affected individuals, as the organisation should first be given the opportunity to take timely remedial action to mitigate the potential risk or harm arising from the data breach. Providing organisations with more time to prepare an appropriate notification to affected individuals would also prevent alarming them unnecessarily. We therefore agree with PDPC's proposal to require organisations to notify affected individuals "*as soon as practicable*", unless an exception or exemption applies.

22. We think that the proposed 72-hour timeframe for notification to the PDPC is reasonable.

Conclusion

23. We welcome the PDPC's proposals in the Consultation Paper on the overall. However, we would be grateful if the PDPC could consider our comments above, in order to ensure that sufficient clarity and guidance are provided such that organisations are able to implement and execute the proposed changes effectively and efficiently in practice.