CLIFFORD CHANCE ASIA'S RESPONSE TO THE PUBLIC CONSULTATION ON THE PROPOSED AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT AND SPAM CONTROL ACT

Clifford Chance Asia
Marina Bay Financial Centre
25th Floor, Tower 3
12 Marina Boulevard
Singapore 018982

Clifford Chance Asia is a formal law alliance in Singapore between Clifford Chance Pte Ltd and Cavenagh Law LLP.

28 May 2020

INTRODUCTION AND SUMMARY

1. This document contains our comments on the Ministry of Communications and Information's ("**MCI**") and the Personal Data Protection Commission's ("**PDPC**") consultation on the proposed amendments to the Personal Data Protection Act ("**PDPA**") and related amendments to the Spam Control Act ("**SCA**") in Singapore.

2. We have endeavoured to provide our comments on the proposed amendments both from legal and a practical perspective, based on our experiences advising commercial users both in Singapore and in other jurisdictions. Terms used but not defined in this response take their meaning from the Public Consultation Paper Issued by the MCI and PDPC (the "**Consultation Paper**")

3. We wish to emphasise that we are supportive of and welcome the proposed amendments, especially the efforts to recalibrate the balance between the individual's consent and organisational accountability, and, to strengthen the effectiveness of the enforcement regime. In broad terms, we agree that the amendments are consistent with the global shift towards risk-based organisational accountability to ensure that data protection standards are met.

STATEMENT OF INTEREST

4. Clifford Chance Asia regularly advises as legal counsel on data privacy issues, including regulatory reform and changes in Singapore and other jurisdictions worldwide.

COMMENTS ON THE PROPOSED AMENDMENTS

5. Our comments on the various aspects of the proposed amendments are as follows.

(a) The introduction of a mandatory data breach notification requirement

6. Under the proposed amendments, organisations will be required to notify PDPC of a data breach that (a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or (b) is of a significant

scale[1]. Organisations will also be required to notify affected individuals if the data breach is likely to result in significant harm to them.

7. We note that the MCI / PDPC intends to prescribe categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to individuals e.g., social security numbers, drivers' licence numbers, credit / debit card numbers etc. This would be welcome guidance and bring clarity to organisations as to their notification obligations.

8. In that regard, we would highlight that the MCI / PDPC may also wish to consider including one or more of the special categories of sensitive personal data prescribed under Article 9 of the General Data Protection Regulation ("**GDPR**") as warranting further protection. These currently consist of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. We acknowledge that the categories to be included would depend on the physical and social normal of the relevant jurisdiction.

9. We further note that the amendments have the effect of creating a new offence[2] where there is unreasonable delay in assessing or notifying the PDPC and, where applicable, each affected individual under the new data breach notification requirement.

10. Section 26D(1), Personal Data Protection Amendment Bill ("**PDP Amendment Bill**") provides that the PDPC must be notified no later than three days after an organisation determines that a data breach meets the criteria for notification set out in section 26B PDP Amendment Bill.

11. From a practical perspective, we query whether that is sufficient time for an organisation to make the requisite notification, especially in more complicated cases. For instance, taking the scenario depicted in Diagram 1, paragraph 21 of the Consultation Paper as a reference, there may be more complex permutations in which

---

1 Such significant scale requires 500 or more individuals under the proposed amendments (paragraph 17 of the Consultation Paper).

2 Sections 26A-D, PDP Amendment Bill read with section 29 PDPA.

organisations and data intermediaries store and process data in practice. There may be more than one data intermediary involved, sometimes based in jurisdictions without similar notification requirements. Given this, it may be sensible to have a slightly longer time frame to make the notification.

12. The GDPR requires organisations to notify the supervisory authority without undue delay within 72 hours of becoming aware of the breach. If an organisation takes longer than this timeframe it must give reasons for the delay. However, the GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4), GDPR therefore allows organisations to provide the required information in phases, as long as this is done without undue further delay.

13. In relation to the contemplated remedial action exception, guidance would be helpful as to when this is determined to be fulfilled. This is particularly so given that it appears to be contemplated that the organisation should assess whether the remedial action exception may apply *before* notifying the PDPC (and therefore, presumably, may have to notify the PDPC of its views as to the same).[3]

14. On that note, it would also be helpful to have some guidance in place as to the content of the notification to the PDPC such that organisations have clarity as to what they should include in the same e.g., whether they must include an assessment of whether the remedial action or technological protection exceptions may apply. Having clarity as to the requisite content of the notification would also be helpful to organisations in ensuring that the PDPC is promptly notified.

15. In relation to the notification of affected individuals, we foresee situations where organisations may be caught between wanting to notify the individuals, and, concern that the prescribed law enforcement agency or the PDPC may direct that such individual should not be notified due to pending investigations / enforcement actions. Accordingly, it may be helpful to consider whether it should be stipulated that, in all cases,

[3] Section 26B(2), PDP Amendment Bill.

organisations seek confirmation from the PDPC ahead of notifying the affected individuals.[4]

16. In that regard, we note that section 26D(7), PDP Amendment Bill provides that the PDPC may, on the written application of an organisation, waive the requirement to notify an affected individual subject to any conditions that the PDPC considers fit. We would suggest also clarifying that pending the determination of the written application by the PDPC, that the organisation will not be required to notify the affected individual in the meantime.

(b) The proposed expanded meaning of "deemed consent"

17. Under sections 15 and 15A PDP Amendment Bill respectively, "deemed consent" is expanded to include a situation where:

(a) personal data is disclosed and used by third-party organisations where reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation; and

(b) where an organisation provides appropriate notification to the individual of the purposes of the intended collection, use or disclosure of his/her personal data and the individual does not opt-out within the stipulated reasonable period.

18. The concept of deemed consent where it is reasonably necessary for the conclusion or performance of a contract or transaction is similar to the lawful basis for processing under Article 6(1)(b), GDPR which permits the processing of personal data where it is 'necessary to perform a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. However, one of the key differences under the GDPR is that the lawful bases for processing personal data are not considered to be deemed consent but are instead intended to ensure organisational accountability by providing lawful grounds which permit the processing of personal data without relying on consent. Under the GDPR, consent must be freely given, specific, informed and unambiguous and therefore the concept of deemed consent conflicts with the GDPR's requirements for consent.

[4] Section 26D(6), PDP Amendment Bill.

19. We note that the concept of deemed consent where an organisation provides appropriate notification to the individual is not consistent with the approach taken under the GDPR. Under the GDPR, notification of processing is not a lawful basis for processing personal data. Articles 13 and 14, GDPR set out the key transparency requirements of the GDPR, requiring organisations to provide clear and concise privacy information, however notification is not sufficient to permit the processing of personal data. There must be a lawful basis for processing personal data under Article 6, GDPR in order for the processing to be lawful, for example the processing is necessary to perform a contract or to comply with legal obligations, or, is in the legitimate interests of the organisation.

20. One of the main challenges organisations face when trying to achieve global data privacy compliance is that under the GDPR, it is not recommended to rely on consent to legitimise the processing of personal data; however under other data privacy regimes, including under the PDPA, the main method of legitimising the processing of personal data is by way of consent. Consent is not the preferred method of legitimising the processing of personal data under the GDPR because consent can be easily withdrawn and it can be difficult to prove that consent was freely given (for example if consent is the pre-condition to the provision of goods or services or because there is an imbalance of power in the parties such as in an employer-employee relationship). Given this apparent inconsistency, the MCI / PDPC may wish to consider further aligning the PDPA's grounds for processing to the GDPR.

(c) Feedback on the new Data Portability Obligation

21. Under the new Data Portability Obligation, organisations must, upon receipt of a request under section 26G, PDP Amendment Bill, transmit the applicable data specified in the data porting request to the receiving organisation.

22. This is similar to the right to data portability under Article 20, GDPR and is, again, a welcome amendment to bring the PDPA in-line with data regulations in other jurisdictions. However, the MCI / PDPC may also wish to consider that the GDPR limits the right to data portability where it is technically feasible (Recital 68, GDPR). This means that the right to data portability does not create an obligation on organisations to adopt or maintain processing systems which are technically compatible with those of other organisations. Organisations are required to take a reasonable

approach which does not create a barrier to transmission, for example by any legal, technical or financial obstacles which slow down or prevent the transmission of personal data. Recital 68, GDPR also considers that there may be legitimate reasons why an organisation cannot undertake the transmission of personal data. For example, if the transmission would adversely affect the rights and freedoms of others.

(d) Feedback on the PDPC's enhanced enforcement powers

23. Under section 29(2)(d), PDPA, the PDPC may impose a financial penalty of up to S$1 million for data breaches under the PDPA. The amendments will increase the maximum financial penalty to (a) up to 10% of an organisation's annual gross turnover in Singapore; or (b) S$1 million, whichever is higher.

24. We note that this adjustment brings the financial penalty cap closer to that in other jurisdictions. For instance, the GDPR provides for a revenue-based financial penalty of €20 million or 4% of the entity's global annual turnover of the previous financial year, whichever is higher.[5] Any penalty issued is intended to be effective, proportionate and dissuasive, and is decided on a case by case basis.

25. However, the GDPR regime provides for two tiers of financial penalties, depending on the severity of the offence. The higher financial penalty of €20 million or 4% of the entity's global annual turnover will apply for serious breaches, such as failures in IT security or in relation to prohibited transfers of personal data to third countries. Under article 83(4), the catalogue of less severe violations (such as infringements of administrative requirements) has a financial penalty cap of €10 million, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher. It may be worth considering whether a similar tiered scheme of financial penalties should be adopted here.

CONCLUSION

26. We hope our comments have been constructive and will assist the MCI and PDPC with their review of the PDPA and corresponding proposed amendments.

---

[5] Article 83(5), GDPR.

27. We are happy to be contacted for any follow-up discussions arising out of our response to the Consultation Paper. In particular, if the PDPC has any questions on data protection regimes in other jurisdictions, such as the GDPR, we would be more than glad to assist.

Clifford Chance Asia

Clifford Chance Asia

28 May 2020

Clifford Chance Asia is a formal law alliance in Singapore between Clifford Chance Pte Ltd and Cavenagh Law LLP.