CLIENT NOTE

AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT

10 November 2020

For any queries relating to this article, please contact:

Tan Tee Jim *S.C.*
Senior Partner, Intellectual Property
DID: 6557 4615
tanteejim@leenlee.com.sg

Zech Chan
Partner, Intellectual Property
DID: 6557 4710
zechchan@leenlee.com.sg

Tan Sih Im
Senior Associate, Intellectual Property
DID: 6557 4612
tansihim@leenlee.com.sg

Zhou Shiyin
Associate, Intellectual Property
DID: 6557 4604
zhoushiyin@leenlee.com.sg

Lee & Lee
50 Raffles Place
#06-00 Singapore Land Tower
Singapore 048623

Tel: +65 6220 0666

For more legal updates, please visit the News & Publication Section of Lee & Lee's website at www.leenlee.com.sg or follow Lee & Lee's facebook page at www.facebook.com/leenlee.com.sg/

I. Introduction

1. Eight years have elapsed since the Singapore Personal Data Protection Act 2012 ("**PDPA**") was first passed in October 2012. In the intervening years, the global data protection landscape has evolved considerably, with businesses deepening their data reliance and the number of high-profile data breaches burgeoning over time.

2. To keep abreast of these developments, the Ministry of Communications and Information ("**MCI**") and Personal Data Protection Commission ("**PDPC**") conducted three public consultations between 2017 and 2019 to review the PDPA and Spam Control Act ("**SCA**"). This has culminated in the Personal Data Protection (Amendment) Bill (the "**Bill**"), which was introduced and read for the first time in Parliament on 5 October 2020, and passed on 2 November 2020. This client update seeks to summarize the salient amendments introduced by this Bill and our views on these changes.

II. Strengthening Accountability

3. In the Public Consultation Paper on the draft Bill issued on 14 May 2020 (the "**Consultation Paper**"), the MCI and PDPC were unequivocal about their intentions to shift Singapore's data protection regime from a consent-based to an accountability-based model, where organisations are accountable for personal data within their possession or under their control and expected to be able to demonstrate compliance.

4. To this end, the Bill seeks to introduce the following amendments to the existing regime:

   (a) a move from a voluntary to a mandatory data breach notification regime;

   (b) the removal of the statutory exclusion for organisations acting on behalf of public agencies; and

   (c) the introduction of new offences for the egregious mishandling of personal data.

A. Mandatory data breach notification requirement

5. Under the former regime, where organisations were **encouraged** to notify the PDPC and affected individuals of a data breach if the said breach was likely to result in significant harm to the affected individuals or was of a significant scale, notification was **not** mandatory.

6. However, the new regime will mandate notification of affected individuals if the breach is likely to result in significant harm to them. Further, it will be **mandatory to notify** the PDPC of a data breach that:

   (a) results in, or is likely to result in, significant harm to the affected individuals; or

   (b) is of a significant scale.

7. To minimize doubts on what would constitute a notifiable data breach, the MCI and PDPC intend to prescribe in accompanying regulations (a) the number of affected individuals for a breach to be considered one of "significant scale" (likely to be 500 or more individuals) and (b) the categories of personal data which, if compromised in a data breach, will be deemed likely to result in significant harm to the individual.

8. The new regime also prescribes specific steps organisations must take in the event of a data breach and the associated timelines to do so. Significantly, an organisation will be required to take reasonable and expeditious steps to assess whether the data breach meets the abovementioned criteria for notification, and document the steps taken to demonstrate that it had acted reasonably and expeditiously and carried out the assessment in good faith. Any unreasonable delay in assessing or notifying the data breach will constitute a breach of the new mandatory data breach notification requirement.

9. Once an organisation determines that a data breach meets the notification criteria, it must notify:

   (a) all affected individuals as soon as practicable; and

   (b) the PDPC as soon as practicable but no later than three (3) calendar days from the day it determines that the breach is notifiable.

10. However, the Bill does provide for certain exceptions to the notification requirement. In particular, an organisation will not be required to notify affected individuals where:

    (a) the breach is unlikely to result in significant harm to individuals because (i) the organisation has taken remedial actions to reduce its likely harm or impact or (ii) the compromised personal data is subject to technological protection (e.g. encryption) that is of a reasonable security standard; or

    (b) a prescribed law enforcement agency or the PDPC prohibits such notification.

11. The Bill also imposes new notification obligations on data intermediaries. Specifically, where a data intermediary discovers a data breach, it will be required to notify the organisation on whose behalf it is processing the personal data without undue delay from the time it has credible grounds to believe that a data breach has occurred.

12. As the entities most involved in the actual processing of personal data, data intermediaries are often at the frontlines in discovering data breaches. As such, we are of the view that this new statutory obligation is a positive step towards ensuring that data breaches are escalated and dealt with as soon as possible.

B. Removal of exclusion for organisations acting on behalf of public agencies

13. Presently, an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data is exempted from complying with data protection obligations under the PDPA. This exemption constituted a regulatory gap since non-government entities acting on behalf of a public agency were not covered by the Public Sector (Governance) Act 2018 as well.

14. The Bill removes this exemption. We welcome this amendment to plug the present lacuna.

C. Offences relating to egregious mishandling of personal data

15. The Bill also introduces the following new offences to hold individuals (and not just organisations) accountable for the egregious mishandling of personal data in the possession of or under the control of an organisation or public agency:

    (a) knowing or reckless unauthorized disclosure of personal data;

    (b) knowing or reckless unauthorized use of personal data for a wrongful gain or a wrongful loss to any person; and

    (c) knowing or reckless unauthorized re-identification of anonymised data.

III. Enabling meaningful consent

A. Expanded concept of "deemed consent"

16. Singapore adopts a consent-based approach to data protection. In other words, organisations may only collect, use, and disclose personal data if they have obtained valid consent from the individual to do so, unless any statutory exceptions apply. The current iteration of the PDPA also provides that an individual may be deemed to consent to the collection, use, and disclosure of his/her personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so.

17. The Bill expands this concept of "deemed consent" to include the following:

    (a) deemed consent by contractual necessity; and

    (b) deemed consent by notification.

18. As regards "deemed consent by contractual necessity", consent may be deemed to have been given for (a) the disclosure to and use of personal data by third parties and (b) said third parties' collection and use of the personal data where it is reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation.

19. As regards "deemed consent by notification", consent may be deemed to be given if:

    (a) the organisation provides appropriate notification to the individual of the purpose of the intended collection, use or disclosure of his/her personal data, with a reasonable period for the individual to opt-out of the collection, use or disclosure for that purpose;

    (b) the individual does not opt-out within that period; and

(c) the organisation has assessed and determined that the intended collection, use or disclosure of personal data for the purpose is unlikely to have an adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of, or mitigate the identified adverse effect to the individual.

20. However, organisations may not rely on deemed consent by notification to obtain consent to send direct marketing messages to individuals. Further, individuals will be able to withdraw their consent to the collection, use or disclosure of their personal data.

21. This new deemed consent by notification model represents a sea change from PDPC's current recommended approach (*i.e.* an opt-in method of obtaining consent) and makes it much easier for organisations to harness personal data for business activities.

B. New exceptions to consent requirement

22. The Bill also introduces two new exceptions to the consent requirement:

(a) the legitimate interests exception; and

(b) the business improvement exception.

23. Under the legitimate interests exception, organisations may collect, use, or disclose personal data without consent where it is in the legitimate interests of the organisation and the benefit to the public is greater than any adverse effect on the individual. Although the Bill does not exhaustively prescribe situations where the legitimate interests exception may apply, the Consultation Paper lists fraud and money laundering detection and prevention, ensuring IT and network security, and misuse of services prevention as examples where the exception may be applicable.

24. To avail themselves of this exception, organisations would have to:

(a) assess any likely adverse effect to the individuals and implement measures to eliminate, reduce the likelihood of or mitigate identified adverse effects to the individual;

(b) determine that the benefit to the public outweighs any likely residual adverse effect to the individual; and

(c) disclose their reliance on legitimate interests to collect, use or disclose personal data.

Further, the exception must not be used for sending direct marketing messages to individuals.

25. Under the new business improvement exception, organisations may collect, use, or disclose personal data without consent where:

(a) the purpose of processing is for business improvement purposes, which include operational efficiency and service improvements, developing or enhancing products/services, and knowing the organisation's customers;

(b) the purpose cannot reasonably be achieved without the use of the personal data in an individually identifiable form;

(c) the purpose is what a reasonable person would consider appropriate in the circumstances; and

(d) the purpose is not for sending direct marketing messages.

26. Further, where the collection, use, or disclosure of personal data without consent for business improvement purposes is within a group of related companies, the following additional conditions apply:

(a) the personal data collected or disclosed must relate to an individual who is an existing customer of the disclosing corporation, and an existing or prospective customer of the collecting corporation; and

(b) the related corporations must be bound by any contract or other agreement, or binding corporate rules requiring the collecting corporation to implement and maintain appropriate safeguards for the personal data.

IV. Increasing Customer Autonomy

A. Data Portability Obligation

27. The Bill also introduces a new data portability obligation on organisations. Upon an individual's request, an organisation is required to transmit an individual's personal data in its possession to another organisation in a commonly used machine-readable format.

28. The purpose of this new obligation is two-fold. First, to provide individuals with greater autonomy and control over their personal data. Second, to facilitate more innovative and intensive use of personal data.

29. To ensure that the compliance burden is reasonable on organisations, the Bill set out exceptions to the data portability obligation in relation to (i) the types of data an organization is not required to port; and (ii) the circumstances under which an organization is not required to port data. In particular, personal data about an individual that is derived by an organization in the course of business from other personal data ("derived personal data") will not be covered by the data portability obligation.

B. Improved Controls for Unsolicited Commercial Messages

30. Currently, unsolicited marketing messages are regulated by the Do-Not-Call ("**DNC**") Provisions under the PDPA and the Spam Control Provisions under the SCA. However, there are gaps in the current controls as both the PDPA and SCA do not cover certain technological developments. The PDPA and SCA also contain overlapping requirements.

31. In order to allow for organisations to better comply with the requirements within both Acts and to keep abreast of technological advancements, the Bill introduces the following amendments to the PDPA and SCA:

(a) Unsolicited commercial messages sent to instant messaging (IM) accounts, such as Telegram or WeChat, are to be regulated by the SCA. Presently, such messages are not covered by the SCA or the PDPA;

(b) The amended PDPA will prohibit the sending of specified messages to telephone numbers through the use of dictionary attacks and address harvesting software; and

(c) The amended PDPA will also impose a new obligation on third-party checkers engaged by organisations to check the DNC Register(s) on their behalf. These third-party checkers are

obliged to communicate accurate DNC results to organisations and will be liable for DNC infringements resulting from erroneous information provided by them.

V. Strengthening Effectiveness of Enforcement

32. The Bill also proposes several new measures to allow for more effective enforcement of the PDPA.

A. Enforcement of DNC Provisions under the administrative regime

33. Under the former regime, breaches of certain DNC Provisions were enforced as criminal offences. Under the Bill, DNC Provisions will be enforced under an administrative regime instead. Specifically, the PDPC will be empowered to issue directions for infringements of the DNC Provisions, such as imposing financial penalties.

34. This new regime will enable the PDPC to resolve DNC complaints more efficiently and proportionately.

B. Increased Maximum Financial Penalty

35. Prior to the introduction of the Bill, the maximum financial penalty for breaches under the PDPA was S$1 million. The Bill introduces a new revenue-based maximum financial penalty, with tiered financial penalty caps for breaches of the DNC provisions, aligned with the egregiousness of the breach.

36. Under the new maximum financial penalties, an organisation with an annual turnover in Singapore exceeding S$10 million could be imposed penalties up to 10% of its annual turnover.

37. In the Closing Note to the Consultation Paper, the MCI and PDPC explained that the increased penalties are intended to serve as a stronger deterrent and enable PDPC to take effective enforcement action based on the circumstances and seriousness of the breach. However, the PDPC will continue to be circumspect and guided by the facts of the individual case when determining the appropriate financial penalty quantum. Relevant factors include the seriousness of the breach and its impact, level of culpability, need for deterrence and the overall proportionality of the amount.

38. Nonetheless, given the tougher penalties, businesses would have to exercise more caution in ensuring compliance with Singapore's data protection laws.

C. Compliance with PDPC Investigations

39. Prior to the introduction of the Bill, the PDPC did not have any recourse against organisations or persons who refused to reply to PDPC's notice to produce information or give a statement when required.

40. The Bill introduces two new offences against such uncooperative parties. To that end, it would be an offence for a person or organisation to:

(a) neglect or refuse to attend before the PDPC or an inspector; or
(b) fail to provide to the PDPC or an inspector any required information or document,

without reasonable excuse.

D. Statutory Undertakings

41. Prior to the introduction of the Bill, the PDPC allowed organisations to provide statutory undertakings as part of their enforcement regime. The current undertaking process involves a written agreement between the relevant organization(s) and PDPC in which the aforesaid organization(s) voluntarily commits to remedy breaches of the PDPA and take steps to prevent recurrence. However, this enforcement regime is not expressly provided for within the PDPA.

42. The Bill provides statutory clarification on the role of voluntary undertakings within the PDPC enforcement regime and sets out, *inter alia*, the circumstances under which a voluntary undertaking may be given, the matters which may be included in a voluntary undertaking, variation of a voluntary undertaking, and enforcement of a voluntary undertaking by the PDPC.

E. Mediation

43. Under the new regime, the PDPC is empowered to (i) establish/approve mediation schemes; and (ii) direct complainants to resolve disputes via mediation without the need to secure parties' consent.

44. This allows the PDPC to manage the increase in data protection complaints in a sustainable manner.

VI. Others

45. The Bill also introduces the following further amendments:

(a) Organisations that reject an individual's request to access their personal data are now required to preserve such personal data for a prescribed period. This ensures that an individual may access such requested data if they successfully seek recourse for the rejection of the access request.

(b) Exceptions to consent relating to the collection, use and disclosure of personal data are streamlined and consolidated. The Bill introduces (i) a new First Schedule for all exceptions to the consent requirement, which applies collectively to the collection, use and disclosure of personal data; and (ii) a new Second Schedule for all exceptions to the consent requirement which apply separately to the collection, use or disclosure of personal data.

VII. Conclusion

46. We are of the view that the Bill both toughens and simplifies the collection, use, and disclosure of personal data by organisations.

47. On the one hand, the new categories of deemed consent for processing personal data and the new legitimate interests and business improvement exceptions to consent mean that organisations are now relieved of the onerous duty of seeking valid consent for such purposes, making it easier for organisations to harness personal data for their business processes.

48. On the other hand, the introduction of the mandatory notification regime and the new data portability obligation imposes more onerous duties on organisations in their processing of personal data.

49. Further, the PDPC's new powers under the Bill to impose a fine of 10% of an organisation's annual turnover mean that organisations with an annual turnover in Singapore exceeding S$10 million must be prepared for higher fines that might exceed the previous cap of S$1 million.

50. In conclusion, it is evident that the MCI and PDPC are taking active steps to keep pace with new business realities and technological developments. Organisations should ensure that they examine their existing data protection policies and procedures and implement the necessary measures required for them to comply with these new obligations.

About Lee & Lee

Lee & Lee is one of Singapore's leading law firms being continuously rated over the years amongst the top law firms in Singapore. Lee & Lee remains committed to serving its clients' best interests, and continuing its tradition of excellence and integrity. The firm provides a comprehensive range of legal services to serve the differing needs of corporates, financial institutions and individuals. For more information: visit www.leenlee.com.sg.

The following partners lead our departments:

Kwa Kim Li
Managing Partner
kwakimli@leenlee.com.sg

Quek Mong Hua
Litigation & Dispute Resolution
quekmonghua@leenlee.com.sg

Owyong Thian Soo
Real Estate
owyongthiansoo@leenlee.com.sg

Tan Tee Jim, *S.C.*
Intellectual Property
tanteejim@leenlee.com.sg

Adrian Chan
Corporate
adrianchan@leenlee.com.sg

Louise Tan
Banking
louisetan@leenlee.com.sg