Opening Speech by Mr S Iswaran, Minister for Communications and Information, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020 on 2 November 2020

1. Mr Speaker, I beg to move, "That the Bill be now read a Second time".

Introduction

2. Sir, the Personal Data Protection Act, or PDPA, was enacted in 2012. Since then, there have been profound changes in the data landscape, most notably in the sheer variety and volume of data that is being generated and its economic significance. The typology of data is diverse – ranging from personal and machine-generated to meta data – with different risk implications.

3. The volume of data is growing at an unprecedented rate. Today, Tera/Peta/Zetta bytes of data – you can pick your prefix – are being generated by ubiquitous Internet-of-Things or IoT devices and sensors, our real and virtual world activities, and smart machines in manufacturing and supply chains. The International Data Corporation estimates that the volume of data that will be created in the next three years will eclipse the total data generated over the past 30 years.[1]

4. Data is also a key economic asset in the digital economy. Data analytics provides valuable insights that inform decisions, generate efficiencies, enhance products and services, and power innovation. It is a critical resource for emerging technologies like artificial intelligence, which hold much transformative potential.

5. Our regulatory architecture must evolve and keep pace with these magnitudinal shifts. For example, we have initiated digital economy Agreements to position Singapore as a key node in the global network of digital flows and transactions. The proposed amendments to the PDPA are another step to ensure our legislative and regulatory regime is fit for purpose for a digital economy with a complex data landscape.

6. Our digital economy must be built on a solid foundation of trust. Consumers must have the confidence that their personal data will be secure and used responsibly, even as they benefit from digital opportunities and data-driven services. Organisations need certainty to harness personal data for legitimate business purposes, with the requisite safeguards and accountability. The proposed amendments to the PDPA seek to strike this balance so as to maximise the potential benefits and minimise the risks of collecting and using personal data.

7. In drafting the Bill, we have studied the data protection practices in jurisdictions like Australia, Canada, the European Union, Hong Kong and New Zealand. The proposed amendments also incorporate valuable feedback received through four public consultation exercises.

8. Sir, I will elaborate on the amendments which aim to: first, strengthen consumer trust through organisational accountability; second, ensure effective enforcement; third, enhance consumer autonomy; and fourth, support data use for innovation.

(A) **Strengthening consumer trust through organisational accountability**

Accountability principle

9. Firstly, to strengthen consumer trust, organisations must undertake responsibility for the personal data in their possession or control. Today, this principle of accountability is implied in sections 11 and 12 of the PDPA. Clause 4 of the Bill inserts a specific reference to accountability at Part III to make the principle explicit and to underscore its centrality.

10. This shift towards an accountability approach is in line with international trends and best practices in data protection laws. It supports interoperability, allowing multi-national corporations to more easily adapt global best practices in Singapore, and minimises compliance costs for Singapore-based companies which are expanding globally.

Mandatory data breach notification

11. To further strengthen organisations' accountability, clause 13 introduces a system for mandatory notification to the Personal Data Protection Commission, or PDPC, when a data breach occurs.

12. Under this Clause, organisations must notify the PDPC of data breaches that are of significant scale. In addition, organisations must notify both the PDPC and affected individuals when data breaches result, or are likely to result, in significant harm to individuals. This places the onus on organisations to assess the scale and impact of data breaches, ensures they are duly accountable to individuals for the personal data in their care, and empowers individuals to take timely measures to protect themselves if a data breach occurs.

Remove exclusion for agents of Government and criminalise egregious mishandling of personal data

13. Sir, the Bill also incorporates the recommendations of the Public Sector Data Security Review Committee in its report of November 2019.

14. First, clause 3 removes the current exclusion for agents of Government, thereby making clear that all private sector organisations are subject to the PDPA, even when they are acting on behalf of public agencies.

15. Second, the Bill strengthens individual accountability for the egregious mishandling of data. Clause 22 sets out new offences for (a) disclosure of personal data; (b) use of personal data that results in personal gain for the offender or another person, or harm or loss to another person; and (c) re-identification of anonymised information. Related amendments will also be made to the Public Sector (Governance) Act and the Monetary Authority of Singapore Act to align the public and private sector data regimes.

16. While the primary responsibility and liability for breaches of the PDPA rest with organisations, these new offences are aimed at individuals who know that their actions are not authorised or who act recklessly. The clause provides for defences to the new offences, such as independent testing of anonymisation deployed in information security systems. Also, these offences should not apply in situations where the conduct is solely in the nature of a private dispute, which should continue to be resolved through civil suits or other forms of dispute resolution.

(B) Ensuring effectiveness of enforcement

17. Sir, let me now move to the second cluster of amendments, which seeks to enhance the flexibility and effectiveness of the PDPC's enforcement.

Statutory undertakings

18. Clause 23 introduces section 48L, a statutory scheme under which the PDPC may, in lieu of a full investigation, accept written voluntary undertakings from organisations to remedy breaches and prevent their recurrence. For example, such undertakings may be accepted when organisations with effective monitoring and breach management systems notify the PDPC of a data breach, and undertake in writing to implement their breach management plan.

19. Several jurisdictions, like Australia, Canada and the UK, accept voluntary undertakings as part of their enforcement regimes. The PDPC will exercise this option only if it assesses that it will achieve an outcome similar or superior to a full investigation. For transparency, the undertakings, as well as the PDPC's decisions and considerations for accepting them, will be made public. In the event of non-compliance, the PDPC may issue a direction requiring the organisation to comply with its undertakings, or initiate investigations.

Alternative dispute resolution schemes

20. Section 48G of clause 23 empowers the PDPC to establish dispute resolution schemes for the resolution of customer complaints. The PDPC may also direct complainants and organisations to attempt to resolve disputes via mediation, without the need to secure the consent of both parties.

Strengthen the PDPC's enforcement powers

21. Clause 37 empowers the PDPC to require the attendance of an individual or employee to give statements and produce documents that are relevant to its investigations.

Increase financial penalty cap for organisations

22. Clause 24 increases the maximum financial penalty for breaches of Parts III to VI, and the new Parts VIA and VIB, to 10% of an organisation's annual turnover in Singapore or $1 million, whichever is higher. This penalty framework is similar to that in other domestic regulation and legislation, including the Competition Act and the Telecommunications Act.

23. During public consultations, concerns were raised about the higher financial penalties. I would like to assure Members, as well as the broader community, that the PDPC will ensure that financial penalties imposed are proportionate to the severity of the data breach. The Bill also provides for Ministerial discretion to review the effective date for these penalties to commence and we intend for the revised financial penalty cap to take effect no earlier than one year after the Act comes into force.

24. Sir, I also wish to highlight, at this juncture, that I will be moving a Notice of Amendment during the Committee Stage to address a clerical error in clause 24 of the Bill.

Enforce DNC provisions under a civil administrative regime

25. Clause 23 sets out amendments providing for the enforcement of the Do Not Call or DNC provisions under the same civil administrative regime as the data protection provisions. The new Part IXA of clause 22 also prohibits the use of dictionary attacks and address-harvesting software when sending messages to telephone numbers. Under clause 24, the maximum financial penalty that may be imposed on an organisation is 5% of annual turnover in Singapore or $1 million, whichever is higher, and $200,000 for an individual.

26. The new section 48O under clause 23 of the Bill updates the current right of private action by a person who suffers loss or damage directly as a result of a breach of the data protection provisions. The right of private action will be extended to organisations and public agencies that suffer direct loss or damage arising from contraventions of the new business-to-business obligations in the Bill.

(C) Enhancing consumer autonomy

27. Sir, the third set of amendments confers consumers with greater autonomy over data generated by their use of services and more control over how they receive commercial communications.

Data Portability Obligation

28. Under the PDPA, individuals have the right to access their personal data, and request for corrections to be made or a copy to be provided. Clause 14 extends this right by providing for a new Data Portability Obligation, which will enable individuals to request for a copy of their personal data to be transmitted to another organisation. Data portability is expected to spur competition and benefit consumers by encouraging the development of substitute as well as novel services.

29. Sir, though data portability has been introduced in practice in jurisdictions like Australia, California and the EU, it is a relatively new concept in Singapore. The PDPC will therefore work closely with all stakeholders for a phased implementation. Regulations will be issued in the coming months on the categories of data that should be portable and other technical and consumer protection details.

Improved controls for commercial communications

30. Clauses 22 and 41 update both the PDPA and the Spam Control Act to rationalise and harmonise the requirements across all modern digital channels for direct commercial communication with consumers. The options for direct communications have evolved since the enactment of the PDPA's DNC provisions and the Spam Control Act's spam control provisions. For example, instant messaging on mobile devices has become the communication channel of choice for many consumers. With the proposed amendments, organisations can offer consumers a unified experience in managing their subscription to commercial communications. The Bill also recognises the development of an industry of third party DNC checkers, and delineates the responsibilities and obligations of DNC checkers and the organisations that commission them.

(D) Supporting data use for innovation

31. Sir, the final set of amendments aims to provide organisations greater clarity on the use of personal data.

32. Currently, the PDPA recognises organisations' need to use personal data for legitimate purposes, and accommodates them through exceptions to the consent requirement, or as deemed consent. For all other purposes, organisations have to obtain consent from the individual.

33. The proposed amendments update, restructure and clarify the lawful purposes recognised as exceptions under the PDPA, and the deemed consent provisions. Let me elaborate how changes to exceptions and deemed consent accommodate modern commercial arrangements and essential purposes such as security, and support business innovation.

Deemed consent for contractual performance

34. Multiple layers of contracting and outsourcing are common in modern commercial arrangements. Clause 6 therefore expands deemed consent to cater for scenarios where personal data is passed from an organisation to successive layers of contractors for the organisation to fulfil the contract with its customer. Crucially, organisations relying on deemed consent for contractual necessity can only collect, use and disclose personal data where it is reasonably necessary to fulfil the contract with the individual.

Legitimate interests exception

35. Clause 31 introduces the First Schedule to the PDPA, which sets out a new exception to consent for these legitimate uses of personal data. To rely on this

exception, organisations must conduct an assessment to eliminate or reduce risks associated with the collection, use or disclosure of personal data, and must be satisfied that the overall benefit of doing so outweighs any residual adverse effect on an individual. To ensure transparency, organisations must disclose when they rely on this exception. One of many potential use cases is anomaly detection in payment systems to prevent fraud or money-laundering.

36. The next set of enhancements supports innovation and introduction of new services.

Business improvement exception

37. The new First and Second Schedules introduced in clauses 31 and 32 make clear that organisations may use personal data for business improvement purposes including: operational efficiency and service improvements; developing or enhancing products or services; and knowing the organisations' customers. As a safeguard, this exception can be relied upon only for purposes that a reasonable person may consider appropriate in the circumstances and where the purpose cannot be achieved without the use of the personal data.

38. Businesses have asked for this exception to also apply to entities within a group as they may consolidate corporate or administrative functions, or concentrate research and development expertise in a single unit that supports the entire group. Recognising this commercial reality, Part 5 of the new First Schedule in clause 31 allows related corporations to collect and disclose personal data among themselves for the same purposes. The Bill provides for additional safeguards for intra-group sharing by requiring related corporations to be bound by a contract, agreement or binding corporate rules to implement and maintain appropriate safeguards for the personal data.

Research and development exception

39. The current research exception has also been revised in clause 32 to support commercial research and development that is not immediately directed at productisation, in other words, going upstream. This could apply to research institutes carrying out scientific research and development, educational institutes embarking on social sciences research, and organisations conducting market research to identify and understand potential customer segments.

Deemed consent by notification

40. Clause 7 introduces the new section 15A, which expands the consent regime by introducing deemed consent by notification. Under this provision, organisations may notify their customers of the new purpose and provide a reasonable period for them to opt out. Before doing so, organisations must conduct a risk assessment and conclude that the collection, use or disclosure of personal data in this manner will not likely have an adverse effect on the individual.

41. To illustrate, this would be useful for organisations that wish to use the personal data of existing customers for new purposes. For example, a financial institution may want to use voice data as an alternative means to authenticate and verify its customers. With these amendments, the financial institution can notify its customers of the intended use of their voice data, provide a reasonable opt-out period, and a contact number for customers' queries. It should be noted that the individual may still withdraw his deemed consent any time after the opt-out period has lapsed.

42. The PDPC will put in place safeguards to ensure that organisations work with anonymised data as much as possible, clearly assess and address any potential adverse effects on individuals, and continue to seek express consent for sending direct marketing messages.

Conclusion

43. Sir, in summary, the proposed amendments to the PDPA will strengthen consumer trust with greater accountability for the protection of personal data; it will give greater certainty for organisations to use data for legitimate business purposes with the requisite safeguards; and it will ultimately enhance Singapore's status as an important node in the global network of data flows and digital transactions. Sir, I beg to move.

---

[1] Source: IDC.com - 'IDC's Global Data Sphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data', 8 May 2020.