PUBLIC CONSULTATION PAPER ISSUED BY
THE MINISTRY OF COMMUNICATIONS AND INFORMATION AND
THE PERSONAL DATA PROTECTION COMMISSION

DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

14 MAY 2020

PART I:	**INTRODUCTION**	**Pg 2**
PART II:	**STRENGTHENING ACCOUNTABILITY**	**Pg 6**
PART III:	**ENABLING MEANINGFUL CONSENT**	**Pg 12**
PART IV:	**INCREASING CONSUMER AUTONOMY**	**Pg 15**
PART V:	**STRENGTHENING EFFECTIVENESS OF ENFORCEMENT**	**Pg 20**
PART VI:	**OTHERS**	**Pg 23**
PART VII:	**PROCEDURES AND TIMEFRAME FOR SUBMITTING COMMENTS**	**Pg 26**

PUBLIC CONSULTATION PAPER

DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

PART I: INTRODUCTION

Background

1. The Personal Data Protection Act 2012 ("**PDPA**") governs the collection, use and disclosure of personal data by organisations in Singapore. Enacted in 2012, it strikes a balance between the need to protect individuals' personal data against private organisations' need to collect, use and disclose personal data for legitimate and reasonable purposes. The Do Not Call ("**DNC**") Provisions of the PDPA enable individuals to opt-out of receiving specified messages[1] in the form of text messages, fax messages or voice calls, sent to Singapore telephone numbers, by requiring persons to check the relevant DNC Register before sending a specified message to a Singapore telephone number[2]. The DNC Provisions and the Data Protection ("**DP**") Provisions came into effect on 2 January 2014 and 2 July 2014 respectively.

2. Singapore's digital landscape and economy have evolved. Capitalisation of data and cross-border data flows have become increasingly important for business innovation and economic competitiveness. According to the World Economic Forum, the world produces 2.5 quintillion bytes a day, and 90% of all data were produced in just the last two years[3]. With the pervasiveness of sensors and ubiquity of connectivity, modern mobile devices have added exponentially to the data that is generated by digital activities. This is evident with the volume of cross-border data flows growing by 148 times from 2005 to 2017[4].

3. Technology is also changing the way data is collected. The growth of Internet of Things ("**IoT**") devices, machine learning and Artificial Intelligence ("**AI**") is leading to an increased ability to collate and analyse large amounts of data, opening up new possibilities to derive insights that

[1] "Specified message" is defined in section 37 of the PDPA. Exclusions from the definition of specified messages are listed in the Eighth Schedule to the PDPA.
[2] Unless the person has obtained clear and unambiguous consent from the individual or has an ongoing relationship with the individual.
[3] Thirani, Vasudha and Arvind Gupt, "The Value of Data", World Economic Forum (2017). Retrieved from www.weforum.org/agenda/2017/09/the-value-of-data/
[4] McKinsey Global Institute, "Globalisation in transition: The future of trade and value chains" (2019).

can yield enormous benefits for individuals and society. The adoption of new technology across all aspects of life, from e-commerce to remote working and learning tools, has also accelerated in recent years.

4. Technological developments are presenting significant challenges for consent-based approaches to data protection. It is increasingly not feasible for organisations to anticipate the purposes for collecting, using or disclosing personal data at the outset. In addition, with large volumes of data collected seamlessly and instantaneously, it is not always practical for organisations to seek the express consent of individuals in every instance of data collection, or for every new purpose. Reliance on consent for stated purposes has resulted in lengthy or broadly worded notices that do not allow individuals to ascertain the purposes nor provide meaningful consent for the collection of their personal data. Moreover, consent decisions of individuals do not necessarily take into consideration the wider, systemic benefits for the public nor yield the most desirable collective outcomes for society. It is therefore necessary to recalibrate the balance between individual's consent and organisational accountability to harness data for appropriate and legitimate purposes.

5. As more personal data is being collected and generated by businesses for new products and services, the number of data breaches will progressively increase. According to a report by Gemalto, the first half of 2018 saw a 72% increase in data records lost, stolen or compromised worldwide[5] compared to the same period in 2017. Consumers are increasingly aware of the impact of data breaches and the importance of protecting their personal data. Strengthening the accountability of organisations builds consumer confidence in organisations' management and protection of their personal data, which will allow organisations to make better use of data to offer more innovative and competitive products and services for consumers.

6. Globally, data protection laws are also shifting towards a risk-based, accountability approach to ensure organisations meet data protection standards. Over the past few years, the Personal Data Protection Commission ("**PDPC**") has been supporting organisations in making the

[5] The Breach Level Index is a global database that tracks data breaches and measures their severity based on factors such as the number of records compromised, the type of data, and the source of the breach. The Index stated that there were 944 data breaches worldwide in the first half of 2018 that led to 3.3 billion compromised data records. According to Statista, an organisation that tracks market and consumer data, in the US alone, there is a general upward trend of data breaches from 2005 – 2018. Retrieved from https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-3-3-Billion-Records-in-First-Half-of-2018.aspx and https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

shift towards an accountability-based approach to data protection. For instance, PDPC has introduced accountability tools such as data protection by design ("**DPbD**"), Data Protection Impact Assessment ("**DPIA**") and Data Protection Management Programme ("**DPMP**). PDPC has also rolled out Data Protection Trustmark certification as a badge of recognition for organisations that demonstrate accountability in meeting data protection standards.

7. It is thus timely for the Ministry of Communications and Information ("**MCI**") and the PDPC to review the PDPA to ensure it keeps pace with the evolving technological and business landscape, while providing for effective protection of personal data in the Digital Economy. MCI/PDPC proposes four key areas of amendments:

a) First, we intend to amend the PDPA to **strengthen the accountability** of organisations. Accountability will be reflected as a key principle of the PDPA, and accountability practices will be introduced as a requirement to complement new and existing avenues for the collection, use and disclosure of personal data under the PDPA. MCI also intend to amend the PDPA to incorporate relevant recommendations of the Public Sector Data Security Review Committee ("**PSDSRC**")[6] to ensure the accountability of third parties handling Government personal data and introduce offences for egregious mishandling of personal data.

b) Second, we intend to enhance the PDPA's framework for the collection, use and disclosure of personal data to **enable meaningful consent** where necessary. In other circumstances, organisations will be able to collect, use or disclose personal data (as applicable) for legitimate interests and business improvement purposes, especially where there are wider public or systemic benefits.

c) Third, we intend to amend the PDPA to provide for **greater consumer autonomy** over their personal data. The new Data Portability Obligation will give individuals greater choice and control over their personal data, prevent consumer lock-in and enable switching to new services. The DNC Provisions under the PDPA and the Spam Control Act ("**SCA**") will also be amended to provide consumers with more protection and control over unsolicited marketing messages.

d) Fourth, we intend to increase deterrence and **strengthen the effectiveness of PDPC's enforcement efforts**, by providing for

[6] Refer to PSDSRC Report, Recommendation 4.4.

increased financial penalties, and additional enforcement powers for the PDPC, such as requiring a person's attendance for taking statements and referring parties to mediation.

Public consultations

8. Three public consultations[7] on MCI/PDPC's key proposals for the review of the PDPA and SCA were conducted between 2017 and 2019. In these public consultations, MCI/PDPC proposed to introduce, amongst others, (i) deemed consent by notification; (ii) 'legitimate interests' exception to consent for collecting, using and disclosing personal data; (iii) mandatory data breach notification; (iv) Data Portability Obligation; and (v) an exception to consent for the use of personal data for 'business improvement' purposes. MCI/PDPC also proposed to review the DNC Provisions, including enforcing DNC breaches under an administrative regime. The review also considered the SCA, which is a legislation enacted in 2007 to combat spam, with the view to ensuring a technology-neutral approach towards regulating unsolicited commercial electronic (i.e. email and text) messages sent in bulk[8].

9. MCI/PDPC has taken into consideration the feedback received in the previous public consultations for the proposed amendments to the PDPA and the SCA. This public consultation seeks feedback to the draft Personal Data Protection ("**PDP**") (Amendment) Bill (attached as **Annex A**), which includes related amendments to the SCA. This Consultation Paper summarises the proposed amendments to the PDPA and the SCA, and the policy intent of the proposals[9].

[7] The public consultations for these proposals and responses to the feedback received can be found at www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations.
[8] See section 6 of the SCA for the meaning of "sending in bulk".
[9] The policy positions outlined in this Consultation Paper supersedes PDPC's Response Notes to the previous public consultations on the PDPA review.

PART II: STRENGTHENING ACCOUNTABILITY

Accountability principle

10. While the PDPA does not include an explicit reference to the accountability principle, sections 11 and 12 of the PDPA embody it. Organisational accountability will be further strengthened through proposed amendments to the PDPA, including the introduction of mandatory data breach notification (refer to paragraph 13), and requirements to assess the likely adverse effects on individuals as part of the enhanced framework for the collection, use and disclosure of personal data (refer to Part III below).

11. To reflect the increased emphasis on accountability, MCI/PDPC will **insert an explicit reference to accountability at Part III of the PDPA**. This will make it clearer that organisations are accountable for personal data in their possession or under their control, and are expected to be able to demonstrate compliance.

12. Please refer to clause 4 of the draft PDP (Amendment) Bill.

Mandatory data breach notification requirement

13. Presently, there is no requirement under the PDPA to notify any party when a data breach has occurred. Data breach notifications are central to organisational accountability because they encourage organisations to establish risk-based internal monitoring and reporting systems to detect data incidents. When coupled with breach management plans, data breach notifications are integral to organisations' incident response and remediation. Accountable organisations may also couple breach notification and breach management plans in order to apply for a statutory undertaking (see paragraph 64).

14. To strengthen protection for individuals and organisations' accountability for the personal data in their care, MCI/PDPC will introduce a mandatory data breach notification requirement under the PDPA.

15. For the purposes of the mandatory data breach notification requirement, "data breach" refers to any unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data, or loss of any storage medium or device on which personal data is stored[10].

[10] In circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Notification criteria

16. Organisations will be required to **notify PDPC** of a data breach that (i) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates (the "affected individuals"); or (ii) is of a significant scale. Organisations will also be required to **notify affected individuals** if the data breach is likely to result in significant harm to them. Notifying PDPC allows organisations to receive guidance from PDPC on post-breach remedial actions (e.g. implementation of data breach management plans) where necessary, and provides PDPC with a better sense of which sectors might need greater support in holding up data protection standards. Notifying affected individuals allows them to take steps, where possible, to protect themselves (e.g. changing passwords, cancelling credit cards, monitoring and reporting scams or fraudulent transactions, etc.). It also ensures that organisations are accountable to individuals for the proper handling and safekeeping of their personal data.

17. Data breaches of a significant scale could indicate a systemic issue within the organisation, which may require PDPC's further investigation and guidance on appropriate remedial actions that the organisation should implement. To provide clarity for organisations to ascertain whether a data breach meets this notification criteria, MCI/PDPC intends to prescribe in Regulations a numerical threshold on what constitutes "a significant scale" in terms of the number of individuals affected in a data breach. Based on its past enforcement cases, PDPC notes that data breaches affecting **500 or more individuals** would be an appropriate threshold.

18. MCI/PDPC also intends to prescribe in Regulations **categories of personal data** which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. This makes clear the types of data breaches that organisations will be required to notify affected individuals. Several jurisdictions have adopted a similar "whitelist" approach for data breach notification to affected individuals and/or the authorities[11]. Examples of data categories prescribed by other jurisdictions include social security numbers, drivers' licence numbers, state identification numbers, credit/debit card numbers, health insurance information and medical history information.

[11] For instance, various states in the US (such as California and Washington) have prescribed categories of personal data for notification to affected individuals and relevant authorities where a data breach meets the requirements for notification.

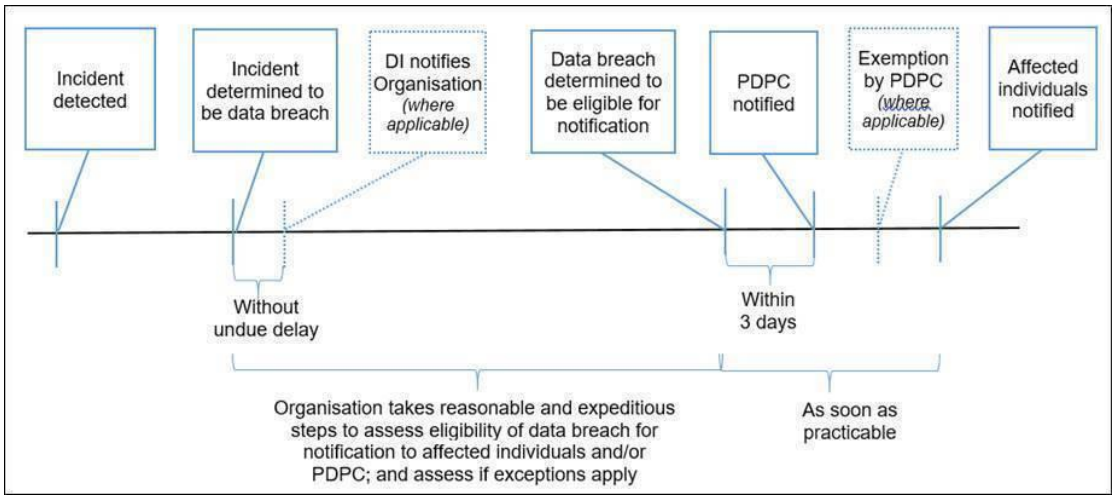
Assessment and notification timeframes

19. Once an organisation has credible grounds to believe that a data breach has occurred, the organisation will be required to take reasonable and expeditious steps to assess whether the data breach meets the criteria for notification to the affected individuals and/or PDPC. The organisation shall document the steps taken to demonstrate that it has acted reasonably and expeditiously, and carried out the assessment in good faith. Unreasonable delay in assessing or notification of data breaches will be a breach of the data breach notification requirement. PDPC will have the powers to assess these matters and to take enforcement action against the organisation for any failure to do so.

20. Upon determining that a data breach meets the criteria for notifying affected individuals, the organisation must **notify all affected individuals as soon as practicable**. Where a data breach meets the criteria for notifying PDPC, the organisation must **notify PDPC as soon as practicable, no later than three calendar days after the day the organisation determines that the data breach meets the notification criteria** (e.g. if the organisation makes the determination on 9 March, it must notify PDPC by 12 March). Prescribing a cap of three calendar days provides clarity for organisations on when they must notify PDPC. As the considerations in determining how expeditiously PDPC can be notified are different from those in determining how expeditiously the affected individuals should be notified, the expectation is not for notifications to PDPC and affected individuals to be made simultaneously. However, PDPC must be notified before or at the same time as affected individuals are notified, to allow PDPC to assist affected individuals who contact PDPC once they are notified.

21. Where a data breach is discovered by a data intermediary ("**DI**") that is processing personal data on behalf of and for the purposes of an organisation, the DI is required to notify the organisation without undue delay from the time it has credible grounds to believe that a data breach has occurred. Please see timeline for data breach notification in Diagram 1 below.

Diagram 1: Timeline for data breach notification



Exceptions to requirement to notify affected individuals

22. MCI/PDPC will provide the following exceptions to the requirement to notify affected individuals:

    a) **Remedial action exception**: where organisations have taken remedial actions to reduce the likely harm or impact to the affected individuals such that the data breach is unlikely to result in significant harm to the affected individuals.

    b) **Technological protection exception**: where the personal data that was compromised by the data breach is subject to technological protection (e.g. encryption) that is of a reasonable security standard, such that the data breach is unlikely to result in significant harm to the affected individuals.

23. In addition, organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. This prohibition is intended to cater to circumstances where notification to affected individuals may compromise any investigations[12] or prejudice any enforcement efforts under the law.

24. Further, to cater to exceptional circumstances where notification to affected individuals may not be desirable, PDPC will have the power to exempt organisations from notifying affected individuals. This includes circumstances where there are overriding national security or national interests.

[12] This includes investigations by public agencies authorised by the law.

25. To be clear, the data breach notification requirements under the amended PDPA do not affect any data breach notification requirements organisations have under any other laws.

26. Please refer to clause 12 of the draft PDP (Amendment) Bill.

Removal of exclusion for organisations acting on behalf of public agencies

27. Currently, under section 4(1)(c) of the PDPA, 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 excluded from the application of the DP Provisions of the PDPA.

28. In line with the PSDSRC recommendations, the PDPA will be amended to remove the exclusion for organisations that act on behalf of a public agency in relation to the collection, use or disclosure of personal data. This will close the legislative gap where non-Government entities acting as agents of Government are not covered under the PDPA or the Public Sector (Governance) Act 2018 ("**PSGA**"), and ensure the accountability of third-parties handling Government data according to the PSDSRC recommendations. It will also provide clarity and consistency in the enforcement of data breaches involving non-Government entities.

29. Please refer to clause 3(a) of the draft PDP (Amendment) Bill.

Offences relating to egregious mishandling of personal data

30. Besides strengthening organisational accountability, MCI/PDPC will also strengthen the accountability of individuals[13] who handle or have access to personal data (e.g. employment or engagement by an organisation). MCI/PDPC will introduce the following new offences under the PDPA to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency:

    a) Knowing or reckless unauthorised disclosure of personal data;

    b) Knowing or reckless unauthorised use of personal data for a wrongful gain or a wrongful loss to any person; and

    c) Knowing or reckless unauthorised re-identification of anonymised data.

[13] Excluding public officers. Public officers are governed under the PSGA.

31. The introduction of these offences do not detract from the policy position to hold organisations primarily accountable for data protection. Organisations remain liable for the actions of their employees in the course of their employment with the organisations.

32. Employees acting in the course of their employment, in accordance with their employer's policies and practices, or whose actions are authorised by their employers, will not run the risk of such criminal sanctions. For instance, cybersecurity specialists, data scientists, AI engineers and statisticians in the information security and encryption industry, who re-identify anonymised data in order to carry out research and development or to test the robustness of their organisations' information security products and service, or their clients' information security systems, will not be held liable for criminal sanctions if their re-identification is authorised by their employers. Other individuals who will not be subject to criminal sanctions include academic researchers who re-identify anonymised data as part of their research work and teaching of topics on anonymisation and encryption; and individuals who independently carry out effectiveness testing of organisations' information security systems either as a white-hat hacker or as part of bug bounty programmes.

33. In addition, MCI/PDPC does not intend for these offences to apply in situations where the conduct is in the nature of a private dispute for which there is recourse under private law (e.g. ex-employee taking an organisation's customer list when joining a competitor). Such private disputes should continue to be settled through civil suits or other forms of dispute resolution.

34. The amendments provide for defences, such as where the information is publicly available; where the conduct is permitted or required under other laws; or where the conduct is authorised or required by an order of the court or in the reasonable belief that the individual has the legal right to do so.

35. In line with the PSDSRC's recommendation for such individuals to be held liable for criminal penalties similar to those under the PSGA, individuals found guilty of each offence will be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years, or both. This ensures that the offences and penalties are aligned for public officers and other individuals.

36. Please refer to clause 20 of the draft PDP (Amendment) Bill.

PART III: ENABLING MEANINGFUL CONSENT

Enhanced framework for collection, use and disclosure of personal data

37. The PDPA provides for consent as the primary basis for collecting, using and disclosing personal data. The Second, Third and Fourth Schedules to the PDPA set out exceptions relating to collection, use and disclosure respectively. The PDPA also provides that an individual is 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 (see section 15 of the PDPA).

38. MCI/PDPC is enhancing the framework for the collection, use and disclosure of personal data under the PDPA to ensure meaningful consent by individuals, complemented by accountability requirements to safeguard individuals' interests. MCI/PDPC will **expand deemed consent** under section 15 of the PDPA to include:

a) **Deemed consent by contractual necessity**: Consent may be deemed to have been given for the disclosure to and use of the personal data by third-party organisations, and the third-party organisations' 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. Please refer to clause 6 of the draft PDP (Amendment) Bill.

b) **Deemed consent by notification**: Consent may be deemed to be given if (i) the organisation provides appropriate notification to inform 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 of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period. In order to rely on deemed consent by notification, organisations are required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual. Organisations also may not rely on this approach to obtain consent to send direct marketing messages to the individuals. Individuals will also be able to withdraw their consent to the collection, use or disclosure of their personal data. Please refer to clause 7 of the draft PDP (Amendment) Bill.

39. These enhancements are broadly similar to approaches under the data protection frameworks in jurisdictions such as Australia, British Columbia, New Zealand and the EU. They will also help reduce compliance costs and facilitate organisations' use and processing of personal data for business purposes.

40. In addition, to cater to situations where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate, **two new exceptions to the consent requirement will be introduced**:

a) **Legitimate interests exception**: This new exception is intended to enable organisations to collect, use or disclose personal data in circumstances where it is in the legitimate interests of the organisation and the benefit to the public (or any section thereof) is greater than any adverse effect on the individual. This could include the purposes of detecting or preventing illegal activities (e.g. fraud and money laundering) or threats to physical safety and security, ensuring IT and network security; and preventing misuse of services. To rely on this exception to collect, use or disclose personal data, organisations must first: (i) assess any likely adverse effect to the individuals and implement measures to eliminate, reduce the likelihood of or mitigate identified adverse effect to the individual; (ii) determine that the benefit to the public (or any section thereof) outweighs any likely residual adverse effect to the individual; and (iii) disclose their reliance on legitimate interests to collect, use or disclose personal data. This exception must also not be used for sending direct marketing messages to individuals. Please refer to clause 31 of the draft PDP (Amendment) Bill.

b) **Business improvement exception**: This new exception is intended to make clear that organisations may use personal data (that was collected in accordance with the DP Provisions) without consent for the following business improvement purposes: (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers. This will provide clarity for organisations to confidently harness personal data for business improvement purposes. The use of personal data for business improvement must be what a reasonable person would consider appropriate in the circumstances[14], and it must not be used to make a decision that is likely to have an adverse effect on an individual. The intent is also for this exception to apply

[14] Section 18(a) of the PDPA.

to a group of companies (e.g. subsidiaries of the organisation). Please refer to clause 32 of the draft PDP (Amendment) Bill.

41. **Revisions will also be made to the research exception**[15] to permit organisations' use and disclosure of personal data without consent for research purposes, while ensuring appropriate accountability measures are in place. The research exception will be revised to introduce conditions such that[16]:

a) The use of personal data or the results of the research will not have an adverse effect on individuals; and

b) Results of the research will not be published in a form which identifies any individual.

42. The revised research exception imposes less stringent restrictions on organisations for the use of personal data for research purposes without consent. This is intended to enable organisations to carry out research beyond the purposes of improving business products or services. For example, the research exception may apply to research institutes carrying out scientific research and development, educational institutes that conduct research into arts and social science, and organisations that carry out market research to understand potential customer segments. Disclosure of personal data for research purposes will continue to be subject to more stringent conditions of impracticality and public interest. Please refer to clause 32 of the draft PDP (Amendment) Bill.

[15] See section 17 of the PDPA, as well as Third Schedule, paragraphs 1(i) and 2, and Fourth Schedule, paragraphs 1(q) and 4.

[16] The revisions will also remove paragraphs 2(b), (c) and (d) from the Third Schedule and paragraphs 4(c), (d) and (e) from the Fourth Schedule to the PDPA.

PART IV: INCREASING CONSUMER AUTONOMY

Data Portability Obligation

43. **A new Data Portability Obligation will be introduced** to provide consumers greater autonomy over their personal data. Data portability allows individuals to request an organisation to transmit a copy of their personal data to another organisation. Similar provisions have been introduced in jurisdictions such as the EU, California and Australia.

44. Under the Data Portability Obligation, an organisation must, at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. This allows individuals to switch to new service providers more easily. Organisations can also have access to more data, thereby spurring the development of innovative data-driven applications that will benefit consumers and support the growth of the Digital Economy.

45. To ensure that the compliance burden is reasonable for organisations, the Data Portability Obligation will be scoped to the following:

    a) **User provided data** (i.e. data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and **user activity data** (i.e. data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) **held in electronic form**, including business contact information;

    b) Requesting individuals who have an **existing, direct relationship with the organisation**; and

    c) Receiving organisations that have a **presence in Singapore**[17]. PDPC may also extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements.

46. User provided and user activity data may include personal data of third parties. Organisations need not obtain consent from the third party whose personal data is to be ported as a result of an individual's data porting request. However, organisations may only port such third party's personal

[17] This refers to organisations that are either formed or recognised under the law of Singapore, or have a place of business in Singapore.

data where the data porting request is made in the requesting individual's personal or domestic capacity. This ensures that the Data Portability Obligation is balanced, reasonable and pragmatic, as it would be impractical for the receiving organisation to obtain consent from every third party and onerous for organisations to redact all personal data of third parties who have not provided their consent. Further, the third party's interests are unlikely to be adversely affected as the requesting individual's porting request is restricted to his/her personal or domestic capacity.

47. To provide greater certainty for compliance, the Data Portability Obligation will only come into effect with the issuance of Regulations. The Regulations will prescribe requirements that apply to the porting of specific datasets. PDPC will work with the industry and relevant sector regulators to develop the requirements to be prescribed in the Regulations. PDPC intends to prescribe the following in the Regulations:

a) A **'whitelist' of data categories** to which the Data Portability Obligation applies. This is intended to reduce compliance costs and provide certainty for individuals and organisations.

b) The **technical and process details** to ensure the correct data is transmitted safely to the right receiving organisation, and in a usable form. The technical details could include data formats, transfer protocol, authentication protocols and cybersecurity standards to enable interoperability between organisations porting and receiving the data. The processes involved could include how customers request for data porting, verification of customers' requests and the expected service level (including timeline for porting) between organisations and consumers.

c) The **relevant data porting request models**. Consumers can either make the data porting request directly to the porting organisations ("**push model**") or through the receiving organisations ("**pull model**"). Data porting between organisations can also happen between two organisations or through an intermediary. These models serve different scenarios or business models, and a preferred model may be specified in each Regulation.

d) **Safeguards for individuals**, tailored to the risks associated with the white-listed dataset. This could include measures to protect consumers (e.g. cooling off periods for certain datasets to provide time for consumers to change their mind and withdraw a porting request) and measures to reduce risks to the ecosystem (e.g.

establishment of a blacklist of organisations that porting organisations may justifiably refuse to port data to). Consumer safeguards, together with the prescribed technical and process details, will make data porting an easy, safe and consistent experience for the consumers.

48. **Exceptions to the Data Portability Obligation will be provided**. The exceptions will mirror those to the Access Obligation under the Fifth Schedule to the PDPA. This is to ensure consistency such that where an organisation is not required to provide access to an individual's personal data under the Access Obligation, it would also not be required to transmit the data to another organisation pursuant to the Data Portability Obligation. One such exception relates to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation. This seeks to protect commercially sensitive information and safeguard the incentive for organisations to innovate, by ensuring "first movers" who bring to market innovative products/services are not prejudiced by the Data Portability Obligation and subject to unfair competition from "fast followers".

49. Further, to protect business innovation and investments by organisations, personal data about an individual that is derived by an organisation in the course of business from other personal data (referred to as "**derived personal data**") will not be covered by the Data Portability Obligation. Derived personal data does not include data that is derived by the organisation using simple sorting nor common mathematical functions like averaging and summation.

50. Similar to the prohibitions for the Access Obligation[18], organisations will also be prohibited from porting data where it is contrary to national interest; threatens the safety or physical or mental health of an individual other than the individual who made the request; or causes immediate or grave harm to the safety or to the physical or mental health of the individual who made the request.

51. Where an organisation refuses a data porting request, the organisation must notify the individual of the reason for the refusal within a reasonable time. PDPC will have the power to review an organisation's refusal to port data, failure to port data within a reasonable time and fees for porting data. Upon completion of its review, among others, PDPC may direct an organisation to port or confirm a refusal to port data; or confirm, reduce or disallow a fee for porting. PDPC may also direct a porting organisation not

[18] Section 21(3) of the PDPA.

to transmit the data in certain circumstances (e.g. where porting of the data is not desirable).

52. Please refer to clauses 13 and 16 of the draft PDP (Amendment) Bill.

Improved controls for unsolicited commercial messages

53. The PDPA's DNC Provisions and the SCA's Spam Control Provisions both aim to address consumer annoyance and provide consumers with greater control over the unsolicited marketing messages they receive. At the same time, they help ensure organisations communicate more effectively with consumers who are interested to receive information on offers of products and services. Technological advancements have fuelled the increased use of marketing tools such as instant messaging ("**IM**") platforms, making it easy to send commercial communications to a large number of recipients.

54. As the PDPA and SCA impose overlapping requirements on unsolicited marketing text messages, MCI/PDPC has reviewed both legislation to make it easier for organisations to comply with their requirements. The proposed amendments also take into account developments in the current landscape. Specifically, MCI/PDPC intend to make the following amendments:

a) **SCA will cover messages sent to IM accounts**: Unsolicited commercial messages sent to IM accounts via platforms such as Telegram and WeChat are currently not covered by the DNC Provisions and the Spam Control Provisions. To address this gap, the SCA will also cover commercial text messages sent to IM accounts and in bulk. Please refer to clause 38 of the draft PDP (Amendment) Bill.

b) **The DNC Provisions will prohibit the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software**: The sending of electronic messages to electronic addresses generated through the use of dictionary attacks and address harvesting software is prohibited under the SCA today. MCI/PDPC will introduce a similar prohibition under the DNC Provisions, in respect of the sending of specified messages to telephone numbers. This aims to deter spammers who use technologies that make it easier to indiscriminately send unsolicited commercial messages (including

robocalls[19]) to a large number of recipients, and helps ensure Singapore does not become a haven for such spammers. Persons who send specified messages to mobile telephone numbers obtained through the use of dictionary attacks or address harvesting software will be dealt with under the amended PDPA. Please refer to clause 27 of the draft PDP (Amendment) Bill.

c) **Introduce obligation and liability on third-party checkers**: Presently, the PDPA does not impose liabilities on third-party checkers engaged by organisations to check the DNC Register(s) on their behalf. The amendments will impose an obligation on third-party checkers to communicate accurate DNC Register results to organisations that they are checking the DNC Register(s) on behalf of, and liability on these checkers for DNC infringements resulting from erroneous information provided by them. The sender would be deemed to have complied with its duty to check the DNC Register(s), if it had been informed by the checker that the number is not listed in the relevant register. This is provided the sender has no reason to believe that, and was not reckless as to whether, the information provided by the checker was false or inaccurate. Please refer to clauses 23 and 24 of the draft PDP (Amendment) Bill.

d) **Incorporate the Personal Data Protection (Exemption from Section 43) Order 2013 into the DNC Provisions**: The intent is to allow organisations to send messages to customers without the need to check the DNC Register(s) when the messages relate to the subject of their ongoing relationship. Please refer to clause 34 of the draft PDP (Amendment) Bill.

[19] Robocalls refer to phone calls that use a computerised auto-dialler to deliver pre-recorded messages. Refer also to section 36 of the PDPA for definition of “voice call”.

PART V: STRENGTHENING EFFECTIVENESS OF ENFORCEMENT

Enforcement of DNC Provisions under administrative regime

55. Currently, breaches of certain DNC Provisions (e.g. duty to check DNC Register, provision of contact information and not to conceal Calling Line Identity under sections 43(2), 44(2) and 45(2) of the PDPA) are enforced as criminal offences.

56. MCI/PDPC intend for PDPC to enforce these DNC Provisions under the same administrative regime as the DP Provisions[20], which will empower PDPC to issue directions (including imposing financial penalties) for infringements. This will enable PDPC to resolve DNC complaints more efficiently and proportionately. Several jurisdictions, such as Australia, Canada, Hong Kong and the United Kingdom ("**UK**"), similarly enforce DNC provisions under administrative regimes.

57. Please refer to clauses 24 to 26 of the draft PDP (Amendment) Bill.

Increased financial penalty cap

58. Under section 29(2)(d) of the PDPA, 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 (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.

59. The higher cap will serve as a stronger deterrent, and provide PDPC with more flexibility in meting out financial penalties based on the circumstances and seriousness of a breach. The higher cap will also be closer to that of other jurisdictions, such as EU and Australia. For example, the EU GDPR provides for a revenue-based maximum financial penalty (€20 million or 4% of the entity's global annual turnover of the previous financial year, whichever is higher). The higher cap is also aligned with other relevant Acts[21].

60. Please refer to clause 17 of the draft PDP (Amendment) Bill.

---

[20] Refer to PDPC's Public Consultation for Managing Unsolicited Messages and the Provision of Guidance to Support Innovation in the Digital Economy and the response to the feedback received.

[21] For example, section 69(4) of the Competition Act states that no financial penalty fixed by the Competition and Consumer Commission of Singapore ("**CCCS**") may exceed 10% or such other percentage of such turnover of the business of the undertaking in Singapore for each year of infringement for each period, up to a maximum of three years, as the Minister may, by order published in the Gazette, prescribe.

Require attendance

61. Presently, PDPC does not have any recourse under the PDPA against organisations which refuse to reply to PDPC's notice to produce information, or give a statement when required.

62. MCI/PDPC will introduce an offence for a person to fail to comply with an order to appear before PDPC/an inspector and provide his/her statement(s) in relation to an investigation under section 50 of the PDPA. It will also be an offence for a person to fail to produce any document specified in a written notice to produce mentioned in paragraph 1(1) of the Ninth Schedule.

63. Please refer to clause 29 of the draft PDP (Amendment) Bill.

Statutory undertakings

64. Statutory undertakings allow a regulator to apply more flexible and individually tailored approaches to enforcement. From PDPC's experience, organisations that have in place a data protection management plan will have an effective system for monitoring, internal reporting, and management of data breaches. The implementation of the data breach management plan can be the subject of a statutory undertaking. When coupled with mandatory breach notification, statutory undertakings will further encourage organisations to adopt accountable practices.

65. Several jurisdictions, such as Australia, Canada and the UK, offer undertakings as part of their enforcement regime. Presently, PDPC accepts undertakings under its Active Enforcement Framework[22]. The amendments will enhance the effectiveness of undertakings as an enforcement mechanism. The statutory undertaking scheme will expand the range of options for enforcing breaches of undertakings.

66. PDPC may investigate the underlying breach if the organisation fails to comply with the statutory undertaking. Alternatively, a breach of a statutory undertaking will be enforceable by PDPC directly through the issuance of directions. If the organisation fails to comply with these directions, PDPC may apply for the directions to be registered by the District Court under section 30 of the PDPA.

67. Please refer to clause 18 of the draft PDP (Amendment) Bill.

[22] Refer to PDPC's Guide to Active Enforcement.

Referrals to mediation

68. To enable PDPC to manage the increase in data protection complaints in a sustainable manner, MCI/PDPC will amend section 27 of the PDPA to provide PDPC with the power to (i) establish or approve one or more mediation schemes; and (ii) direct complainants to resolve disputes via mediation, without the need to secure consent of both parties to the complaint or dispute. This framework would be similar to those enacted in the Medical Registration Act, Private Education Act, Info-communications Media Development Authority ("**IMDA**") Act, and Monetary Authority of Singapore ("**MAS**") Act.

69. Where individuals seek PDPC's assistance on a complaint or dispute under the PDPA, all parties to the complaint or dispute will be required to participate in the mediation scheme when directed by PDPC, and must comply with such terms and conditions of participation in the scheme as may be prescribed. If an individual does not agree to the terms and conditions of the scheme, he/she may attempt to resolve the matter on his/her own, either through exercising his/her right of private action under section 32 of the PDPA, or by other forms of alternate dispute resolution outside of the PDPA.

70. Please refer to clause 15 of the draft PDP (Amendment) Bill.

PART VI: OTHERS

Preservation of personal data requested pursuant to access and porting requests

71. The PDPA provides individuals with the right to request to access their personal data in an organisation's control or possession[23]. However, there is currently no requirement for the organisation to preserve a copy of the individual's requested personal data should the organisation deny the request. This results in situations where the requesting individual is no longer able to obtain access to the requested personal data even if he/she seeks recourse for the rejection of the request, if the organisation deletes the requested personal data.

72. MCI/PDPC will introduce a requirement for organisations to preserve personal data requested pursuant to an access request (or a copy) for a prescribed period of (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later. This will help to preserve the availability of a meaningful remedy should the individual succeed in his/her application. MCI/PDPC will similarly require preservation of personal data requested pursuant to a data porting request.

73. Please refer to clause 19 of the draft PDP (Amendment) Bill.

Prohibitions to providing access

74. Currently, organisations are prohibited from providing access to personal data where it reveals the personal data about another individual or it reveals the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his/her identity[24]. From PDPC's experience, this has resulted in implementation issues for organisations providing access to personal data (e.g. removing third parties' personal data captured in CCTV footage). To ensure alignment with the Data Portability Obligation and for the reasons provided above in paragraph 46, MCI/PDPC will amend section 21 of the PDPA to reduce the scope of prohibitions to access in relation to user provided and user activity data. The amendment will allow organisations to provide access to such data,

[23] Section 21 of the PDPA.
[24] Sections 21(3)(c) and 21(3)(d) of the PDPA.

regardless of whether providing access could (i) reveal personal data about another individual, or (ii) reveal the identity of an individual who has provided personal data about another individual and that individual does not consent to the disclosure of his/her identity.

75. Please refer to clause 10 of the draft PDP (Amendment) Bill.

Excluding "derived personal data" from Correction and Data Portability Obligations

76. For the reasons provided above in paragraphs 48 and 49, MCI/PDPC will provide an exception for "derived personal data" to the Correction Obligation. "Derived personal data" will also be excluded from the Data Portability Obligation. To ensure organisations remain accountable for personal data in their possession or under their control, organisations will still be required to provide individuals with access to derived personal data. Organisations are to also provide the individual with information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request.

77. Please refer to clauses 13 and 33 of the draft PDP (Amendment) Bill.

Revised exceptions to Consent Obligation

78. The PDPA provides for consent as the primary basis for collecting, using and disclosing personal data, with the Second, Third and Fourth Schedules setting out exceptions relating to collection, use and disclosure respectively.

79. The amendments will streamline and consolidate the exceptions to consent, to simplify how organisations may collect, use and disclose personal data without consent. Instead of having three separate Schedules, MCI/PDPC will have (a) a Schedule for all exceptions to the consent requirement which apply collectively to the collection, use and disclosure of personal data; and (b) another Schedule for all exceptions to the consent requirement which apply separately to the collection, use or disclosure of personal data. Minor revisions will be made to align the purposes or conditions when merging the common exceptions into the relevant Schedules. Please refer to clauses 8, 31 and 32 of the draft PDP (Amendment) Bill.

80. MCI/PDPC will amend the business asset transaction exception[25] to extend the scope of applicable personal data under this exception to include that of independent contractors (e.g. Grab drivers), in addition to the personal data of an employee, customer, director, officer or shareholder of the organisation.

81. Please refer to clause 31 of the draft PDP (Amendment) Bill.

[25] See section 17 of the PDPA, as well as Second Schedule, paragraphs 1(p) and 3, and Fourth Schedule, paragraphs 1(p) and 3.

PART VII: PROCEDURES AND TIMEFRAME FOR SUBMITTING COMMENTS

82. MCI/PDPC would like to seek comments on the draft PDP (Amendment) Bill. The draft PDP (Amendment) Bill may be further revised following feedback received from this consultation and MCI/PDPC's further deliberations.

83. Respondents should organise their submissions as follows:
    a) Cover page (including their personal/company particulars and contact information);
    b) Summary of major points;
    c) Statement of interest;
    d) Comments; and
    e) Conclusion.

    Supporting materials may be enclosed as an annex to the submission.

84. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any feedback. Where feasible, please identify the specific provision of the draft PDP (Amendment) Bill which you are commenting on.

85. All submissions should reach MCI/PDPC no later than **5pm on 28 May 2020**. Late submissions will not be considered. Submissions are to be in softcopy only (in Microsoft Word or PDF format). Please send your submissions to **DataRegulation@mci.gov.sg**, with the subject "**Public Consultation for the PDP (Amendment) Bill**".

86. MCI/PDPC reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Respondents may request confidential treatment for any part of the submission that the respondent believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. Respondents are also required to substantiate with reasons any request for confidential treatment. If MCI/PDPC grants confidential treatment, it will consider, but will not publicly disclose, the information. If MCI/PDPC rejects the request for confidential treatment, it will return the information to the respondent, and will not consider this information as part of its review. As far as possible, respondents should limit any request for confidential treatment of information submitted. MCI/PDPC will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.