Submission by Microsoft to the Public Consultation on the Draft Personal Data Protection (Amendment) Bill (the "Draft PDPA Bill")

Sent by email to: DataRegulation@mci.gov.sg

1 Cover page

Microsoft thanks PDPC for the opportunity to provide comments on the Draft PDPA Bill. We would be more than happy to discuss with PDPC any part of this submission. Our contact details are below.

Company particulars	**Microsoft Operations Pte Ltd** 182 Cecil St, #13-01 Frasers Tower, Singapore 069547
Key contact information	Name: Shaun Tan Number: +65 8798 9350 Email: shautan@microsoft.com

2 Summary of major points

2.1 Microsoft welcomes the clarifications on important changes to the PDPA presented in the Draft PDPA Bill. There are a limited set of key refinements to the Draft PDPA which we would like to propose as follows:

(a) Scope of application to data intermediaries (clause 3 of the Draft PDPA Bill): Microsoft recommends that the scope of application of the provisions of the PDPA to data intermediaries be amended to clarify that the only obligation in the new data breach notification regime that applies to data intermediaries is the requirement to notify the controller (i.e. new section 26C(2) of the Draft PDPA Bill). We believe this more accurately reflects the intent of the legislature and reflects the overarching principle throughout the PDPA, which is that the data intermediary's responsibility should be to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations.

(b) Data portability (clause 13 of the Draft PDPA Bill): Microsoft is of the view that an organisation should only be required to transmit an individual's personal data directly to another organisation following that individual's request if it is technically feasible to do so. Data may be held in a format by an organisation that is not directly translatable to another organisation, and in this case the transferring organisation can only provide a copy of the data to the transferee organisation but could not directly "port" it over due to interoperability issues and challenges. The right to data portability should not create an obligation for an organisation to adopt or maintain processing systems which are technically compatible with those of other organisations.

(c) Increased penalties (clauses 17, 35B – 35D of the Draft PDPA Bill): Whilst Microsoft is supportive of a data privacy enforcement regime which adequately protects consumers and dissuades offenders and re-offenders, Microsoft's view is that the maximum financial penalty proposed should only be imposed by PDPC where the offence is a serious breach of the law, it is of a kind likely to cause substantial

damage or substantial harm to data subjects and the breach is deliberate or the result of recklessness. Microsoft is opposed to the imprisonment penalty prescribed for unauthorised disclosure of personal data as this punishment appears disproportionate for data protection law. We note that the Public Sector Data Security Review Committee made certain recommendations to ensure the accountability of third parties handling *Government* personal data but we oppose the extension of this policy position to parties handling *non-Government* personal data.

(d) Request for clarification on amendments to Spam Control Act

3 Statement of interest

3.1 Microsoft is a multi-national technology company which provides cloud and other services, and develops, manufactures, licenses and sells computer software and other technology. Although we do act as a data controller for some of our product offerings, Microsoft often acts as a data processor/ data intermediary on our customers' behalf, and our customers remain the organisation with ultimate control over the processing of their personal data. As such, in these situations Microsoft will only act upon our customers' instructions in processing personal data and they maintain the upmost control. In Singapore, Microsoft has a strong interest in supporting PDPC's innovation and leadership in the data privacy space as the digital economy continues to grow and evolve.

3.2 Microsoft believes that a firm legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship can flourish. As the PDPA has demonstrated in the past, firm data protection laws are also a key means to underpin consumer confidence when operating online and ensures a level playing field between operators. Implementing these practices will instil a level of trust in the local data protection legal regime that is necessary to cement Singapore's position as the digital hub of Asia.

3.3 Microsoft's proposed refinements to the Draft PDPA Bill as set out above seek to ensure that Singapore's data privacy law continues to lead the APAC region in preserving the integrity of individuals' privacy to a standard that is comparable to the privacy laws of other countries, yet without unnecessarily restricting or hampering the operations of businesses in Singapore. Microsoft's suggestions are intended to ensure that the law is both strong and workable and also capture our experience in complying with the EU GDPR and other national privacy regimes across Asia so they reflect what has worked well in practice and what has not.

3.4 As the world becomes increasingly digitised, Microsoft is increasingly seeing a trend of countries working to align their privacy regimes to facilitate a more cohesive and interoperable approach to data management. Microsoft's proposed refinements to the Draft PDPA Bill as set out above have been proposed with this in mind.

4 Comments

4.1 Scope of application to data intermediaries (clause 3 of the Draft PDPA Bill)

(a) The Draft PDPA Bill introduces a mandatory data breach notification regime in Part VIA of the PDPA. However, in the amendments to the scope of application of the PDPA to data intermediaries proposed in clause 3 of the Draft PDPA Bill, Part VIA is not mentioned.

(b) The consultation paper published by the PDPC and the proposed Section 26(C)(2) of Part VIA clearly limits any notification obligations on the data intermediary to notifying the data controller without undue delay from the time it has credible grounds to believe that a data breach has occurred. Accordingly, there should not be any confusion that the requirement to notify an affected individual or the regulator should fall on the data intermediary. A data controller should be primarily responsible for meeting privacy obligations vis a vis the regulator and for providing redress to individuals. This also aligns with accountability principle underlying the PDPA that an entity is subject to the same obligation under the PDPA in respect of personal data processed on its behalf and for its purposes by a data processor as if the personal data were processed by the entity itself.

(c) Microsoft therefore recommends that clause 3 of the Draft PDPA Bill, which sets out the scope of application of the PDPA to data intermediaries, be amended by inserting the words in **bold and underline** below:

"3. Section 4 of the principal Act is amended —

…

(c) by deleting the words "Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data))" in subsection (2) and substituting the words "Parts III, IV, V, VI (except sections 24 and 25)**, VIA (except sections 26A and 26(C)(2))** and VIB";…"

4.2 Data portability (clause 13 of the Draft PDPA Bill)

(a) The Draft PDPA Bill introduces the data portability obligation, which requires an organisation, at the request of an individual, to port 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. Microsoft believes that data portability can lead to numerous benefits to users and providers alike, and is therefore supportive of the introduction of this right in the Draft PDPA Bill.

(b) We understand from the consultation paper that the PDPC intends to prescribe the technical and process details, including data formats, transfer protocol and cybersecurity standards to enable interoperability between organisations porting and receiving the data. Microsoft believes that any data portability requirement that is introduced should not be prescriptive in nature but rather should allow organisations to use a principles-based approach to determine how they enable data portability. This is because more prescriptive and less flexible porting obligations will likely increase compliance costs.

(c) While Microsoft welcomes additional guidance on technical and process details, we believe there still may be circumstances where, despite complying with all the prescribed technical requirements, a receiving organisation may not be able to effectively read and integrate the data. There may be challenges in interoperability given extensive variations in different systems. The right to data portability should not create an obligation for an organisation to adopt or maintain processing systems which are technically compatible with those of other organisations.

(d) For example, the EU GDPR only requires personal data to be ported directly to another organisation where technically feasible. The EU GDPR and Philippines

DPA[1] takes a slightly different approach by giving data subjects the right to obtain a copy of the personal data collected in an electronic or structured format, which is commonly used and allows for further use by the data subject, rather than requiring organisations to transfer data directly to another party.

(e) Microsoft recommends that data should only be required to transmit an individual's personal data directly to another organisation following that individual's request if it is technically feasible to do so.

4.3 Increased penalties (clauses 17, 35B, 35C and 35D of the Draft PDPA Bill)

(a) The Draft PDPA Bill proposes to 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. While the consultation paper uses the EU GDPR and the Australian Privacy Act as examples where penalties based on turnover are imposed, there are many privacy laws regionally that do not impose penalties based on turnover e.g. Japan APPI[2], Hong Kong PDPO[3] and Korea PIPA[4].

(b) Rather than serving as a stronger deterrent, excessive fines may lead to organisations seeking to avoid proactive disclosures, and choosing to keep breaches and other incidents secret, for fear of punishment which would not benefit or protect consumers adequately. Furthermore, higher fines may deter companies from entering or staying in the market.

(c) As the fine can be imposed by PDPC at its discretion to ensure compliance with any part of the PDPA, it is Microsoft's view that the maximum financial penalty proposed should only be imposed by PDPC where the offence is a serious breach of the law, it is of a kind likely to cause substantial damage or substantial harm to data subjects and the breach is deliberate or the result of recklessness.

(d) Microsoft is opposed to the imprisonment penalty prescribed for unauthorised disclosure of personal data as this punishment appears disproportionate for data protection law. To the extent PDPC considers criminal penalties a proportionate remedy for violation of data protection law, we respectfully suggest that an individual should be penalised only if, the "applicable contravention" is done *intentionally* and without authorisation from the organisation or public agency in question.

4.4 Request for clarification on related amendments to Spam Control Act ("SCA"). We are unclear as to whether the expansion of the SCA to cover messages sent to instant messaging accounts would lead to deletion or opt-out requirements for instant messages and would like to request for PDPC's clarification on this point.

5 Conclusion

5.1 Microsoft thanks PDPC for the opportunity to provide feedback on the draft Personal Data Protection (Amendment) Bill. At Microsoft we consider privacy a fundamental right, and we believe stronger data protection through greater transparency and accountability should benefit our customers everywhere and we welcome PDPC's drive to support data innovation

[1] Data Privacy Act 2012

[2] Act on the Protection of Personal Information (Act No. 57 of 2003)

[3] Personal Data (Privacy) Ordinance (Cap. 486)

[4] Personal Information Protection Act 2011

whilst enhancing transparency and accountability on the part of organisations that collect and use personal data.

5.2 We would be very happy to discuss this paper and respond to any questions that PDPC may have at the contact details above.