Response to Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam Issued by the Authority for Info-Communications Technology Industry of Brunei Darussalam dated 20 May 2021

IBM World Trade Corporation (Brunei Branch) ("**IBM**", "**we**", "**us**" or "**our**") welcomes this initiative by the Authority for Info-communications Technology Industry of Brunei Darussalam ("**AITI**") to develop a draft Personal Data Protection Order ("**PDPO**") for the protection of individuals' personal data which is intended to apply to the private sector in Brunei Darussalam (covering both commercial and non-commercial organisations). We are pleased to provide our comments to the Public Consultation Paper on the proposed data protection framework issued by AITI on 20 May 2021.

While we applaud this initiative by the AITI, we are conscious of the potential regulatory and cost-related burdens the proposals may place on businesses. We recognise the need to align data protection framework in Brunei Darussalam with regulatory frameworks in other jurisdictions. The need for the framework must also be balanced with the need to encourage the growth of the Brunei Darussalam economy. In particular, we should be mindful that any new obligation imposed does not: (i) discourage the growth of small and medium enterprises ("**SMEs**"); and (ii) inhibit Brunei Darussalam's ability to drive foreign direct investment ("**FDI**"), whether from new foreign investors which have yet to set up a presence in Brunei Darussalam or from current foreign investors which have existing operations in Brunei Darussalam.

We also note that several proposals potentially overlap with other existing regulatory frameworks. In this regard, we recommend there be standardisation and streamlining of obligations across the various regulatory bodies. Such streamlining will allow the industry to enhance its efforts to achieve "across-the-board" compliance with the existing regulatory framework in Brunei Darussalam.

We also recognise the need for flexibility in cross-border transfers of data as proposed by AITI. In this regard, we urge for participation in government-backed recognised trade systems. In particular, participation in the APEC Cross-Border Privacy Rules (**"CBPR**") System will enable Brunei Darussalam to take advantage of opportunities to conduct dealings with its counterparts throughout the region to facilitate cross-border trade whilst meeting or exceeding recognised privacy standards. Through the CBPR System, certified companies and governments are working together to ensure that when personal information moves across borders, it is protected in accordance with the standards prescribed by the system's program requirements and is enforceable across participating jurisdictions.

No.	Proposal	Comments
3	***Definitions and Key Concepts***	
3.1	**Definition of Personal Data**	We note that the term "personal data" is proposed to mean a natural person, whether living or deceased. We also understand that the PDPO only requires organisations to accord protection to deceased persons' personal data where such persons have been dead for 10 years or fewer. We seek clarification on the purpose of assigning protection over personal data of deceased person and the specific circumstance that it would apply. The EU's General Data Protection Regulations ("**GDPR**") for instance, only consider data to be personal when it is assignable to identified or identifiable living persons.

No.	Proposal	Comments
3.7	**Data Intermediaries / Processors**	➢ We suggest that certain categories of data processors be excluded, such as if the data processor has been engaged under a robust data processing agreement by the data controller. ➢ Secondly, we urge AITI to grant certain exemptions to data processors having regard to the difference in the role of data processors from that of a data controller. For example, we suggest exempting data processors from: (i) Consent Obligation; (ii) Purpose Limitation Obligation; (iii) Notification Obligation; (iv) Access and Correction Obligations; and (v) Accuracy Obligation. Data processors should only be responsible to adopt the necessary security measures to protect data, retain data and inform the public agency of any data breach.
4	***Data Protection Obligations***	
4.5	**The Accountability Obligation**	➢ **Appointment of Data Protection Officer ("DPO")**. In order to ensure that the requirement does not unduly raise the cost of business and discourage the growth of SMEs and FDI in Brunei Darussalam, we suggest that the requirement to appoint a DPO be limited only to organisations which conduct core activities that require regular and systematic monitoring of data subjects on a large scale. ➢ **Location of the DPO**. We understand that the PDPO seeks to regulate all organisations, regardless of where they are established. We suggest that the PDPO allows for DPO to be based outside of Brunei Darussalam for organisations established overseas or those where they have a branch office in Brunei Darussalam. This will encourage FDI into Brunei Darussalam while ensuring that such organisations remain compliant.
4.6	**The Consent Obligation**	We welcome AITI's proposal to provide flexibility to the type of consent (express or deemed) and the standard of consent. ➢ **4.6.1 - Clear Exceptions to Consent Obligations**. We recommend setting out clear provisions on when organisations are permitted to collect, use and disclose personal data without consent. AITI may benchmark these exceptions against the Second, Third and Fourth Schedules of the Singapore Personal Data Protection Act ("**SG PDPA**") which provide, among others, that consent is not required to collect, use or disclose personal data in certain situations (e.g. the collection is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual).

No.	Proposal	Comments
		➢ **4.6.4** - **Deemed Consent.** We recommend benchmarking against Sections 13 to 17 of the SG PDPA and providing further guidance and illustrations on the circumstances in which deemed consent is provided (see Section 15 of the SG PDPA).
4.9	**The Access, Correction and Data Portability Obligations**	Please refer to Section 5 (Data Subject Rights) below.
4.11	**The Protection Obligation**	**4.11.3** - We suggest organisations be given the flexibility to determine the standard of security measures reasonably required, according to the nature of the data and the organization's core activity. For example, higher security standard could be required from organisations which provide direct to consumer goods as their core activities. This is because such organisations require regular and systematic processing of consumer personal data on a large scale.
4.13	**The Transfer Limitation Obligation**	We suggest providing an exception to entities within a group. This will allow related companies to (i) leverage data for business improvement purposes, e.g. by establishing common administrative functions and centralising research and development; and (ii) process data within the organisation in relation to the provision of cloud services. This will reduce the costs of doing business and facilitate the growth of cloud-based computing industry in Brunei Darussalam.
4.14	**The Data Breach Notification Obligation**	We seek clarification on the following: ➢ **4.14.1, 4.14.2, 4.14.4** – **Criteria.** We seek clarity on what AITI considers to be "likely to result in significant harm or impact" to individuals, and what would constitute "significant scale". We also seek further details and guidance on the proposed risk-based approach and threshold for notification. We suggest considering frameworks in other jurisdictions such as Australia and Singapore. Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches scheme that requires organisations covered by the Australian Privacy Act 1988 (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach. The Personal Data Protection Commission of Singapore provided guidance on the types of personal data that is deemed to result in significant harm to affected individuals if compromised in a data breach. ➢ **4.14.1, 4.14.2** - **Notification Format**. We seek clarification on the format of notification. ➢ **4.14.1** - **Time frame.** As the notification is to be made to Responsible Authority, we suggest the timeframe for notification be 3 business days after the organization determines that the breach is eligible for reporting. This is to align with the business hours of Responsible Authority

No.	Proposal	Comments
		who will be receiving the notification. We also suggest providing for an "assessment period" to allow organisations to investigate and assess whether a breach has occurred. For example, Australia's notifiable data breaches scheme allows organisations a 30-day assessment period to determine whether a breach has occurred. ➢ **4.14.2** - **Exceptions.** We seek clarification on the categories of exceptions or waivers. We suggest these exceptions include the exception to the requirement to notify individuals, for instance: (i) where the data subject is the subject of an ongoing or potential investigation (as such notification may compromise the investigations or prejudice enforcement efforts); and (ii) where the data has been encrypted to a reasonable standard whereby such encryption mitigates the risk of unauthorized access or disclosure to the data even if the data may have been misappropriated. ➢ **4.14.3** – **Post Breach Remedies.** We seek clarification on whether post-breach remedial actions from Responsible Authority would be mandatory or whether data controllers would have the discretion to implement the appropriate remedies within their organizations. The latter is preferable, as this allows organizations the discretion to implement the appropriate remedies based on the nature of their business and risks levels. ➢ **Sectoral notifications.** The data breach notification should take into account any sectoral notifications already in place, to avoid multiple reporting obligations to various governmental agencies.
5	***Data Subject Rights***	
5.4	**Right to Request for Access to Personal Data**	➢ **5.4.1 –** We seek clarification on the extent of the disclosure, and in particular, whether a data subject will have the right to know the specific third party to whom the data subject's personal data has been disclosed. Providing a right to know the specific third party (as opposed to the class of third party) will increase the cost of compliance, as organisations will need to record each and every party to whom the personal data is disclosed, according to the specific individual, and such compliance costs may be prohibitive for SMEs. ➢ We suggest the obligation to provide information regarding the ways the personal data has been used or disclosed apply only to organisations that disclose personal data to third parties for direct marketing purposes.
5.6	**Right to Data Portability**	**Scope** ➢ **5.6.9** - We seek clarification on the type of data exempted under 5.6.9(d) and (f).

No.	Proposal	Comments
		➢ We suggest historical data of more than one (1) year prior to the date of request be exempted from the scope of this obligation. ➢ As the purpose of data portability is to provide individual consumers with greater autonomy and control over their personal data in a commercial transaction, a porting organisation should not be required to port personal data collected in reliance on an exception to the consent requirement. This is because such personal data is likely collected in the vital interests of individuals or the public and is not collected for the purpose of providing goods and services. ➢ We suggest limiting the ability to port personal data within Brunei Darussalam, such that personal data may only be ported to a receiving organisation established in Brunei Darussalam so as to mitigate movement of personal data outside of Brunei Darussalam. Limiting the obligation to organisations with a presence in Brunei Darussalam balances the objective of enabling greater consumer data flows from one service provider to another in Brunei Darussalam with the need not to unduly raise compliance costs for organisations. ➢ As the purpose of data portability is to give more control to consumers, we suggest that the data portability obligation apply only to organisations which provide direct to consumer goods as their core activities. **Data of Third-Party Individual** ➢ **5.6.7** - We seek clarification on what constitutes the individual's (P) personal or domestic capacity and P's user activity data or user-provided data. ➢ We suggest that the nature of the goods and services to be provided by receiving organization or nature of business of the receiving organization be clearly specified. ➢ We suggest that the PDPO provides safeguards against any misuse of the third-party (T) personal data. For example, the porting organisation will need to ensure (i) the requested data is under the control of the individual (P); (ii) the data porting request is strictly for the individual's own personal or domestic purposes; and (iii) the third-party's personal data is collected for the purpose of providing the product or service which the third-party individual had given consent (or is deemed to have given consent) for, and not for any other purposes (e.g. direct marketing to the third party). **Limits of Liability** ➢ We recommend that data controllers be absolved of liability in guaranteeing the accuracy of the data. **Fees** ➢ We seek clarification on whether data controllers will be allowed to charge fees for complying with such requests.

No.	Proposal	Comments
6	***Investigations, Enforcement and Appeal***	
6.2	**Powers of Investigation**	➢ **6.2.1(c)** – We suggest that any entry into organisation shall be with a warrant for consistency with sub(d). ➢ **6.2.1 (a)** and **(d)** – We suggest that the taking possession of, or removal of documents be limited to documents which are directly related to the investigation and that the documents shall not be subject to confidentiality or legal privilege.
6.6	**Right of Private Action**	Considering that the PDPO already provides for the setting up of Responsible Authority to administer and enforce the PDPO and the establishment of a Data Protection Appeal Panel, it does not appear to be necessary to provide a standalone right of private action. This will ensure consistency of the direction and finality of decision made by the Responsible Authority and appeal committee.
8	**Do Not Call ("DNC") Regime**	➢ In order to ensure that the DNC regime does not unduly raise the cost of business and discourage the growth of SMEs and FDI in Brunei Darussalam, we suggest that the DNC regime should be limited to organisations which provide direct to consumer goods as their core activities as such organisations require regular and systematic processing of consumer personal data on a large scale. ➢ **8.4** – We suggest defining the nature or category of telemarketing messages. ➢ **8.5** – In order to increase control and oversight on the senders, we suggest that senders be registered with AITI before they are able to apply to check the DNC Register.
10	**Interaction between the PDPO and Other Laws**	We would urge for standardisation and streamlining of obligations across the various regulatory bodies. Such streamlining will allow the industry to enhance its efforts to achieve "across-the-board" compliance with the existing regulatory framework in Brunei Darussalam.