ANNEX 1
Comments on the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam

Section	Paragraph	Comment
4.6 The Consent Obligation	4.6.2 Given that the type of consent could vary depending on the specific context of the collection, the manner in which consent may be given under the PDPO is not specifically prescribed. It is recognised that consent may be explicit or implied through an individual's actions or inaction, depending on circumstances. This gives organisations flexibility as to how they obtain consent.	• What is the reasonable test applicable given that consent is not specifically prescribed and depending on circumstances?
4.7 The Purpose Limitation Obligation	4.7.1 Under the PDPO framework, an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.	• What is reasonable in the context of appropriate person and circumstances?
	4.7.2 In general, organisations must obtain personal data by lawful and fair means and, where appropriate, with the individual's consent. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose from which the individual originally consented. The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and only for purposes that are reasonable. This requirement also seeks to prevent over-collection of personal data by organisations.	• What about general use/purpose of obtaining the data holistically for internal information or credit analysis purposes?
4.8 The Notification Obligation	4.8.1 Under the PDPO framework, the requirement to provide an individual with notice is tied to the Consent Obligation. As part of obtaining valid consent, the organisation must provide the individual with information on: (a) the purposes for the collection, use or disclosure of his personal data, on or before collecting the personal data; and (b) any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data.	• Is application form for a product or service sufficient notice?
4.11 The Protection Obligation	4.11.2 To ensure that organisations are accountable to consumers in relation to the protection of their personal data, the PDPO	• What is considered as reasonable under this provision?

	imposes upon organisations the obligation to make reasonable security arrangements to prevent data breaches. In recent years, there have been several high-profile data breaches internationally, which are usually due to criminal activities like hacking, or organisations failing to impose sufficient or adequate security measures.	• For example, if hacking occurs, etc., or beyond the control of the organisation, what would be the authority's stance?
	4.11.3 The PDPO provides for a reasonable standard for such security measures, and the degree or nature of the measures required may differ depending on factors such as the nature and sensitivity of the data, the form in which the personal data is stored or held, and the impact to the individual if the personal data is subject to 2nauthorized access, disclosure or other risks.	• How do we measure reasonable standard under this provision?
4.12 The Retention Limitation Obligation	4.12.1 Under the PDPO, an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected and is no longer necessary for legal or business purposes.	• Any guidance to be provided in terms of time frame on retention period?
5.4 Right to Request for Access to Personal Data	5.4.3 An organisation must not accede to the individual's access request if the information requested could reasonably be expected to: (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal 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 identity; or (e) be contrary to the national interest.	• How do we measure reasonableness in the circumstances as mentioned?
	5.4.8 If the organisation rejects the individual's access request, it must notify the individual of the rejection within the prescribed time and in the prescribed manner. If the organisation has excluded personal data from the access request, it must notify the individual of the exclusion.	• What would be the prescribed time? • What would be the prescribed manner?
5.6 Right to Data Portability	5.6.2 When an individual submits a data porting request, the porting organisation is required to transmit the applicable data to the receiving organisation in the prescribed manner if certain	• What are the prescribed manner and requirements as mentioned?

	conditions are fulfilled. The data porting request must satisfy the prescribed requirements and there must be an ongoing relationship between the individual and the porting organisation.	
	5.6.7 A porting organisation can disclose personal data about a third party individual (T) to a receiving organisation without T's consent if the data porting request is made in an individual's (P) personal or domestic capacity and relates to P's user activity data or user-provided data. A receiving organisation receiving personal data about T from the porting organisation can use that personal data only for the purposes of providing goods and services to P.	• To seek further clarification and/or elaboration on the process.
	5.6.8 An organisation must not port the applicable data if the transmission of the applicable data can reasonably be expected to: (a) threaten the physical or mental health of another individual; (b) cause immediate or grave harm to the physical or mental safety of the individual related to the data; (c) be contrary to national interests; or (d) if so instructed by the Responsible Authority.	• How do we measure (a), (b) and (c)?
8. Do Not Call ("DNC") Regime	8.3 Generally, organisations in Brunei Darussalam that make marketing calls or send marketing messages by way of text message or fax will be required to check the phone numbers against the DNC Registry and ensure that they do not make calls or send messages to registered numbers, unless an exception or exclusion applies. For example, where the individual had given explicit consent for the company to contact him or her for marketing purposes, or the recipient is in an ongoing relationship with the sender.	• How and/or what are the steps to be taken to check? • Person name? or I.C. no. or phone number? • Confirmation check against number only?
8.5 Duty to Check the DNC Register	8.5.2 A sender may obtain valid confirmation from the Responsible Authority that the Brunei telephone number is not listed on the relevant DNC Register. The sender may do so by making an application to the Responsible Authority in receive this confirmation. This application to the Responsible Authority has to be made within the prescribed duration before sending the specified message.	• What would be the timeframe? From checking to confirmation.
	8.6 Role and Responsibility of Checkers	• What does checkers refer to?

8.6 Role and Responsibility of Checkers	8.6.1 A checker has to ensure information provided is accurate and compliant with requirements under the PDPO. These checkers are persons who, for reward, provide another person (P) with information on whether a Brunei telephone number is listed on the DNC Register for P's compliance with the PDPO.	• How to ensure or what measures are to be taken for accuracy? • What information is referred under this provision?
	8.6.2 Checkers must ensure that the information provided to P about whether the Brunei telephone number is listed on the DNC Register is accurate. Checkers must provide such information to P in accordance with any prescribed requirements.	• How to ensure or what measures are to be taken for accuracy? • What information is referred under this provision?
	8.6.3 Checkers are deemed to have ensured the accuracy of information if it is in accordance with a reply from the Responsible Authority in response to the checker's application for confirmation and this information is provided before the expiry of the prescribed period.	• What does prescribed period refer to?
8.7 Sending of a Specified Message	8.7.1 A sender of a specified message must provide its contact information and other prescribed details in the specified message. When sending a specified message to a Brunei telephone number, the sender must include clear and accurate information on: (a) how to identify the sender; (b) how the recipient can readily contact the sender; and (c) other prescribed information (e.g. if the Responsible Authority prescribes further requirements in subsequent regulations).	• What would be the approach if sending of a specified message is by phone call?
8.9 Prohibition Against Dictionary Attacks and Address-Harvesting Software	8.9.1 An organisation must not send a message to a telephone number that is generated or obtained through a dictionary attack or address-harvesting software. This would be considered an offence under the PDPO.	• What does dictionary attack or address-harvesting refer? Or what actions would be considered as such?