Paragraph no.	Wording	Comment
	General Comments	1. With regards to the penalties, please clarify is there a penalty scale for different types of offence, minor breach, medium breach and major breach. Will the penalties be reduced if company has control measures in place to reduce breach? 2. How would penalty be decided or finalized if data breach is caused by data intermediaries/processors?
3.1 & 3.2	3.1. Definition of Personal Data 3.2. Categories of Personal Data	It would be helpful if AITI would provide guidance on the examples of data that need to be protected and retention controlled.
3.2.4	Accordingly, organisations implementing policies and practices to comply with the PDPO would need to take into account the specific personal data in question (amongst other factors), for instance, how "sensitive" it may be. This may entail an assessment of the category of personal data and how the individual may be impacted should the personal data be subject to unauthorised access, disclosure or other risks.	AITI may wish to consider issuing appropriate guidance on the factors that organisations should consider when making such assessments.
3.7.1 (d)	the duty to notify the organisation or public agency under the Data Breach Notification Obligation as referred to in paragraph 4.2.12 below.	Suggest for AITI to prescribe a time frame within which a data intermediary is to notify the data controller of a breach.
4.5.1	Under the Accountability Obligation in the PDPO, an organisation must appoint a person to be responsible for ensuring that it complies with the PDPO, typically referred to as a data protection officer ("DPO"); and develop and implement policies and practices that are necessary to meet its obligations under the PDPO, including a process to receive complaints. In addition, the organisation is required to communicate to its staff	Please provide more clarity on whether AITI requires the DPO to be: 1.) based in the Brunei; and/or 2.) registered with any public registry.

Paragraph no.	Wording	Comment
	information about such policies and practices and make information available upon request to individuals about such policies and practices.	
4.6.6	Standard of Consent: Furthermore, consent is not valid where: (a) consent is obtained as a condition of providing a product or service, and such consent is beyond what is reasonable to provide the product or service to the individual; or (b) where false or misleading information is provided, or deceptive or misleading practices are used, in order to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.	Suggest for AITI to consider excluding lucky draws/contests.
4.6 & 4.7	4.6.1. Under the PDPO, an individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law or an exception in the PDPO applies 4.7.1. Further 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.	1) In considering the exceptions to the general positions of 4.6.1 & 4.7.1, we suggest that an organisation should be allowed to collect and use personal data without consent if it is in the 'legitimate interests' of the organisation. Legitimate interests may include fraud prevention/detection, for example where an insured's claims history is assessed by an insurance company, or regulatory requirements. 2) Further we suggest that an exception be specifically included in the PDPO to allow commercial organisations to, without consent, use personal data, or share it with a related commercial organisation, for business improvement purposes such as the following:- • Improving, enhancing or developing goods or services • Improving, enhancing or developing operational methods or processes • Learning about and understanding the behaviour and preferences of individuals • Identifying goods or services that may be suitable for individuals, or personalising/customising them 3) We also suggest that the PDPO provides for deemed consent in the following circumstances:- i) Contractual necessity: Where a person provides their data for the purposes of either entering into or performing a contract, the recipient organisation may deem consent to collect, use and disclosure such data as reasonably necessary to enter into or perform that

Paragraph no.	Wording	Comment
		contract. For example, where a person hands over a credit card for payment for services, it is necessary for the recipient to collect, use and disclose personal data to financial services organisations to process the payment. ii) Notification: An organisation may also collect, use or disclose personal data after notifying its intention to do the same and reasons why, provided that (i) the individual does not object within a reasonable period, and (ii) the collection, use or disclosure is unlikely to have an adverse effect on the individual.
4.13.1	Under the Transfer Limitation Obligation, an organisation must not transfer personal data to a country or territory outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO, to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO	1) Transfer of data between related entities is commonplace and in considering whether the recipient of the personal data is bound by legally enforceable obligations before such transfer can be effected, we suggest that such legally enforceable obligations should include obligations imposed on a recipient of personal data under binding corporate rules, where the recipient is an organisation related to the transferring organisation. 2) The recipient can be deemed to be related to the transferring organisation if: (a) the recipient, directly or indirectly, controls the transferring organisation; (b) the recipient is, directly or indirectly, controlled by the transferring organisation; or (c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.
4.14.1	Under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach that: (a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or (b) is or is likely to be, of a significant scale	1) In Singapore, data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Will we be adopting a similar scale for Brunei? 2) Suggest for AITI to provide guidance on the criteria for "significant harm". 3) Please do also consider amending 3 calendar days to 3 working days as there might be instances where incidents occur over the weekends or public holidays. 4) Suggest for AITI be define the period in which organisations are to make such an assessment.

Paragraph no.	Wording	Comment
4.14.2	Unless an exception applies or a waiver is granted, organisations will also be required to notify affected individuals on or after notifying the Responsible Authority, if the data breach results in, or is likely to result in, significant harm to an affected individual.	Suggest for AITI to prescribe, or provide guidance on the exceptions, the criteria for the application of exceptions, and the criteria for when waivers may be requested for.
5.5.3	The organisation must also send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.	1) We seek clarification on what this would be applicable to. Is this only applicable to errors or omission of data due to the fault of the organisation? If an individual was to make correction on his/her personal data due to his/her own omission, will the organisation still be required to send corrected personal data? The ability to send corrected personal data to every organisation might pose huge implications, for example CRS reporting, FATCA reporting, etc. 2) Suggest for AITI to prescribe a time frame in which organisations effect the cessation of use and disclosure of the individual's personal data.
5.5.2	Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall correct the personal data as soon as practicable.	Please confirm if AITI requires the organisation to notify the requesting individual on whether the correction has been made.
5.6	Right to Data Portability	1) Suggest for AITI to enact provisions to address the issue of accountability in the event of a compromise occurring in the process of transmitting the data. 2) Please confirm if the porting or receiving organisation be held accountable, and made responsible for the breach notification obligations. 3) Please confirm if organisations are permitted to charge for carrying out such data porting. If so, also kindly confirm if AITI will prescribe any guidelines or limits on such charges; or require organisations to seek for approval on proposed fee structures.
5.6.3	The Data Portability Obligation will only apply to “applicable data” which is held in electronic form, and that was collected or created by the porting organisation within the prescribed period.	Suggest for AITI to prescribe a form or a collective agreement template or similar for businesses.

Paragraph no.	Wording	Comment
5.6.4	In terms of exceptions, a porting organisation does not need to transmit applicable data that has been specifically excluded by the PDPO or applicable data in specifically excluded circumstances.	Suggest for AITI to prescribe a form or a collective agreement template or similar for businesses.
5.6.6	A porting organisation must preserve any data specified in a data porting request for the prescribed period of time (or longer). This obligation applies regardless of whether the organisation accedes to the porting request. A porting organisation must also ensure that the copy of the data is complete and accurate.	Suggest for AITI to prescribe a maximum period, or some guidance scenarios on determining a maximum period, for such data preservation.
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.	Suggest for AITI to prescribe limitations to how many such third parties (T) can an individual (P) make a request for. What are the scenarios where this might be permitted?
6.2.1 (c)	by giving at least two working days' advance notice of intended entry, entering into an organisation's premises without a warrant;	Kindly clarify if the details of officers intending to enter into premises will be provided in two working days' advance notice.
7.4	As a counterbalance, the PDPO also provides for defences to these offences such that employees acting in the course of their employment, or in accordance with instructions of their employer, will be protected from criminal liability. Notwithstanding the above, the organisation is ultimately accountable for compliance with the PDPO and retains liability for the actions of its employees.	If an organisation is able to demonstrate that all the reasonable protections have been put in place for personal data, please advise if AITI permits organisations to rely on the offences set out in 7.1 as a defence against employees/agents.

Paragraph no.	Wording	Comment
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.	Suggest for AITI to prescribe a list of such checkers, and a limit on the charges that such checkers may impose for performing such checks.
8.8.1	The sender does not need to obtain valid confirmation from the Responsible Authority or checkers of the DNC Registry if the subscriber or user of the Brunei telephone number gives his clear and unambiguous consent to the organisation for the sending of the specified message to that number. This consent from the subscriber or user must be in writing or a form that is accessible for subsequent reference.	Suggest for AITI to prescribe an official format for such confirmation, or such other forms of authentication, so that organisations can be assured of the authenticity of a confirmation.
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.	Suggest for AITI to provide a definition/guidance of what processes may be deemed as dictionary attacks or address-harvesting.
12	Existing Personal Data / Grandfathering Clause	1) It is noted that the PDPO will only apply to personal data collected after commencement of the PDPO. The PDPO is targeted to commence in phases. 2) In the circumstance where the customer took a new policy after commencement, would his previous policies/data collected still be applicable under “grandfather” clause?