PUBLIC CONSULTATION PAPER ON PERSONAL DATA PROTECTION FOR THE PRIVATE SECTOR IN BRUNEI DARUSSALAM

Section reference	Extract from Proposed Regulation	Comment/Query
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 information about such policies and practices and make information available upon request to individuals about such policies and practices.	Please provde more clarity on whether AITI requires the DPO to be: 1.) based in the Brunei; and/or 2.) registered with any public registry.
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.
4.14.1	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:	Suggest for AITI be define the period in which organisations are to make such an assessment.
4.14.1 (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	Suggest for AITI to prescribe, or provide guidance on the criteria for "significant harm".
4.14.1 (b)	is or is likely to be, of a significant scale.	Suggest for AITI to prescribe, or provide guidance on the criteria for "significant scale".
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.
5.3.3	The organisation shall not prohibit an individual from withdrawing his consent. Moreover, upon withdrawal of consent, an organisation must cease (and cause its data intermediaries and agents to cease) to collect, use or disclose the personal data for such purposes.	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	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.
5.6	Right to Data Portability	Please confirm if the porting or receiving organisation be held accountable, and made responsible for the breach notification obligations.
5.6	Right to Data Portability	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.
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.	
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. 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.	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?

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.
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.