BAIDURI				
S/	**Page**	**Para.**	**Relevant Statement**	**Comment / Question**
1	**12-Nov**	**3.5.2**	The term “public agency” is defined in the PDPO to include: (a) the Government, including any ministry, department, agency, or organ of State; (b) any tribunal appointed under any written law; or (c) any prescribed statutory body. The Minister may specify any statutory body established under an Act or Order to be a public agency for the purposes of the PDPO.	Does the PDPO apply to Government-Linked Companies (GLCs)?
2	**12-Nov**	**3.5.2**	The term “public agency” is defined in the PDPO to include: (a) the Government, including any ministry, department, agency, or organ of State; (b) any tribunal appointed under any written law; or (c) any prescribed statutory body. The Minister may specify any statutory body established under an Act or Order to be a public agency for the purposes of the PDPO.	Is Perbadanan Tabung Amanah Islam Brunei (TAIB) excluded from the PDPO? Note that Perbadanan TAIB is a body corporate established under the Perbadanan TAIB Act (source: Perbadanan TAIB website). Please confirm whether data collected from and reported by the Credit Bureau under AMBD fall outside the scope of PDPO as it is a statutory body.
3	**13**	**3.7.2**	In this regard, the PDPO provides for a category of organisations called “data intermediaries/ processors”. A data intermediary / processor is an organisation which processes personal data on behalf of another organisation or public agency. This is in contrast with organisations (sometimes referred to as data controllers) which have direct control over the means and purposes for processing of the personal data.	What types of organisations are considered as data intermediaries / processors in the banking context? Further illustrations and examples would be helpful.
4	**15**	**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.	Further illustrations and examples on what would be regarded as valid consent would be helpful. For e.g., if Baiduri were to conduct a roadshow, would a registration log signed by roadshow participants, constitute a valid consent for future communication by the bank? If a customer provides personal data relating to a third party (for e.g. information of spouse, children, parents or other connected person) by submitting such information to the bank, can the bank consider that it has obtained the consent of the third party?
5	**15**	**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. Such consent must be validly obtained and may be either expressly given or deemed to have been given.	The Brunei Association of Banks (BAB) maintains and compiles a bankruptcy list based on submission by BAB members. Can the BAB continue to collect, use and disclose such information?
6	**15**	**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. Such consent must be validly obtained and may be either expressly given or deemed to have been given.	Can personal data collected by Baiduri Bank be disclosed or shared with its subsidiaries so long as consent is obtained?
7	**15**	**4.6.4**	Deemed Consent: There are circumstances where consent may be deemed under the PDPO, broadly: (b) if the collection, use or disclosure of the personal data is reasonably necessary for the conclusion of the contract between the individual and the organisation;	If a customer approaches a motor vehicle dealer with the intention of purchasing a motor vehicle via bank loan, the motor vehicle dealer makes a referral and provides the customer’s contact number to the bank, and disclosure of such information is considered as necessary for the conclusion of a contract, is this considered as deemed consent? Should the bank receive a complaint from the customer, what safeguard measures are required to protect the bank?
8	**16**	**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.	Can the purpose be defined in a general way? If the purpose must be defined in a specific manner, how specific must it be? Is it required to explicitly request for consent for hosting of data outside of Brunei. (Assuming appropriate measures are in place to protect such data being hosted outside in accordance with the PDPO)
9	**16**	**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	Is marketing considered a relevant and reasonable purpose? It can be argued that marketing promotions is a benefit of a product or service rendered.
			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.	For example, sending a credit card customer a communication of a new benefit / promotion which he/she can benefit from.
				What is considered as unreasonable purpose?
10	**16**	**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.	Clarity required on whether both notification and consent are required at the same time.
11	**16**	**4.9.1**	Under the PDPO framework, individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access, subject to the exceptions in the PDPO.	Clarity required on how general or specific “information about the ways in which that personal data has been or may have been used or disclosed” can be.
12	**16**	**4.9.2**	Individuals may also request for correction of their personal data or that their personal data be transmitted to another organisation, subject to certain exceptions in the PDPO.	Where an individual request for a correction, would it suffice that the bank corrects information contained in its core systems or is it also required to correct information in its back-up systems?

13	**18**	**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.	Can a whitelist of jurisdictions (countries or territories) be provided which is deemed to be having comparable standards with the PDPO.
14	**18**	**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.	Please confirm that 3 calendar days commence from such time that assessment contains substantial evidence beyond doubt that a breach has indeed occurred.
15	**19**	**5.3.1**	On giving reasonable notice to an organisation, an individual may, at any time, withdraw his consent in respect of the collection, use or disclosure of his personal data for any purpose by an organisation. This ability to withdraw consent applies to both express consent and deemed consent.	Requirement may be too excessive, especially where the person has a contractual obligation with the bank. The bank should be able to retain the person's personal data until the person's contractual obligation is completed. It is noted that Banks are obligated to retain records including personal data for no less than 7 years in accordance with the Criminal Asset Recovery Order. Can we further define in what circumstances a bank may decline withdrawal of consent.
16	**20**	**5.4.4**	Sub-paragraphs (c) and (d) above do not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.	This paragraph refers to an exception to an exception. It is difficult to understand. Clarity required.
17	**21**	**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.	Please confirm that Banks will not restricted from charging reasonable fees and will define reasonable timelines to satisfy such requests subject to complexity or scope of the data involved.
18	**21**	**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	Please confirm that the bank may make a reasonable assessment as to whether the other organization (e.g. a vendor which is rendering an outsourced service for the bank) requires the corrected data for business purpose.
19	**22**	**5.6.1**	The PDPO may introduce a data portability obligation which requires a porting organisation to port an individual's data to another organisation under certain circumstances upon receiving a data porting request, unless an exception applies. This is also known as the "Data Portability Obligation".	In what situations will this apply to the banking sector?
20	**23**	**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.	How is "applicable data" defined?
21	**26**	**6.5.4**	Where an appeal is lodged with the DPAP, the Chairman of the DPAP shall nominate a Data Protection Appeal Committee ("Appeal Committee") comprising 3 or more members of the DPAP.	Who will make up the DPAP? Ideally, the DPAP should include representatives from the private sector.
22	**27**	**8.1**	The PDPO may provide for the establishment of a DNC regime. Individuals may request for their telephone numbers to be added to the DNC Registry if they do not wish to receive telemarketing messages via phone call, text message (i.e. SMS, MMS or any electronic communications sent using a telephone number, e.g. WhatsApp, Telegram) or fax. The DNC Registry will be administered by the Responsible Authority.	How is "telemarketing" defined? If the bank obtains a person's telephone number via a referral and sends a message to that person's telephone number, is that considered as telemarketing?
23	**31**	**10.6**	Sectoral regulators may also exempt their licensees from specific requirements under the PDPO where required. This is a more balanced approach which recognises the specific needs and circumstances of different industries.	Would the exemptions be sectorial or industry specific?
24	**32**	**12.2**	For organisations that have control over or possess personal data, the PDPO will have a grandfathering clause which will allow organisations to continue to use that personal data that was collected before the commencement date for the purposes for which the personal data was collected. The exception to this is where the individual withdraws his consent for the use of his personal data.	How are banks expected to evidence the purposes for which the personal data was previously collected?
25	**32**	**12.2**	For organisations that have control over or possess personal data, the PDPO will have a grandfathering clause which will allow organisations to continue to use that personal data that was collected before the commencement date for the purposes for which the personal data was collected. The exception to this is where the individual withdraws his consent for the use of his personal data.	When does the grandfathering clause become effective? Does it become effective on the date the PDPO is enacted or after the sunrise period ends?