Jurisdiction	Brunei Darussalam
Date	31 March 2022
Law Firm	Messrs. Pengiran Izad & Lee
Title, Name	Partner. Pengiran Izad-Ryan Pengiran Haji Bahrin
Contact Information	pgizad@pgizadandlee.com.bn +673-2232945

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

- Yes. Note presently, there is **no** legislation and responses to this questionnaire are based on a public consultation paper issued by Authority for Info-communications Technology Industry of Brunei Darussalam ("**AITI**"). See: https://www.aiti.gov.bn/SiteCollectionDocuments/PDP/RPCP_AITI_03122021_FINAL.pdf.

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

- Not specific.

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.)

- Yes, see Banking Order 2006, particularly Section 58 and the Third Schedule of this Order.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I. (please add a reply column as necessary)

The title of the **draft** law ：**Personal Data Protection Order ("PDPO")**

① The definition of "Personal Information"	Data, whether true or not, about an individual who can be identified (a) from the data; or (b) from that data and other information to which the organization has or likely to access.

②	The scope in which the law applies	All organisations, defined in the PDPO to mean "*any individual, company, association or body of persons, corporate or unincorporated whether or not (a) formed or recognized under the law of Brunei Darussalam; or (b) resident, or having an office or place of business, in Brunei Darussalam".* With the exception of the below: a) individuals acting in a personal or domestic capacity; b) individuals acting as employees or officers of an organization; c) business contact information; and d) personal data of deceased persons. There is also a Public Agency Exclusion.
③	The territorial scope	- All private sector organisations that collect, use or disclose personal data in Brunei Darussalam, regardless of whether they are formed or recognized under Brunei law or whether they are resident or have an office or place in Brunei Darussalam. - Organisations located overseas may still be subject to PDPO as long as they collect, use or disclose personal data (i.e. engage in data processing activities) in Brunei Darussalam.
④	URL	https://www.aiti.gov.bn/SiteCollectionDocuments/PDP/RPCP_AITI_03122021_FINAL.pdf.
⑤	The effective date	- Not yet decided

The title of the law ：**Banking Order 2006**

①	The definition of "Personal Information"	Undefined in the banking Order. Banks have a duty of confidentiality in repect of "Customer Information"which includes but is not limited to customer's name, identity, address, amount of debt outstanding on the customer's credit or charge card, credit facilities. Generally it would be described as any information of the customer obtained duting the course of the banking relationship.
②	The scope in which the law applies	All banking businesses and matters connected thereto. Banking business is defined as *business which consists of or includes the receiving of deposits or other repayable funds from the public and granting of credits for its own account and includes the following activities (a) financial leasing; (b) money transmission services; (c) issuing and administering means of payment, such as credit cards, charge cards, travellers' cheques and bankers' drafts; (d) guarantees and commitments; (e) trading for own account or for account of customers in one or more of money market instruments, foreign exchange, financial futures and options, exchange and interest rate*

		instruments and transferable securities; (f) participation in share issues and the provision of services relating to such issues; (g) advice to undertakings or capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings; (h) money broking; (i) portfolio management and advice; (j) safekeeping and administration of securities; (k) credit reference services; (l) safe custody services; 3 BLUV as at 14th January 2006 (m) bank assurance; and (n) such other business as may be approved in writing by the Authority with the approval of the Minister.
③	The territorial scope	Banking businesses which hold a licence granted under section 4 or 23, and includes all branches and offices in Brunei Darussalam of any such company.
④	URL	https://www.agc.gov.bn/AGC%20Images/LAWS/BLUV/BANKING%20ORDER,%202006.pdf
⑤	The effective date	4th March 2006

ii. If there are any special instructions about the laws, please describe them.

The Authority for Info-communications Technology Industry of Brunei Darussalam ("**AITI**") is designated as the Interim Data Office and was responsible for developing the draft PDPO, setting out the general data protection framework in Brunei Darussalam. AITI has indicated that it shall be designated as the Responsible Authority for the administration and enforcement of the PDPO.
The PDPO is still in its draft form and is intended to be enacted by mid-2022. Enforcement of PDPO shall commence two years from the time PDPO is enacted. PDPO will provide the establishment of a Responsible Authority which will responsible for overseeing the administration and enforcement of the PDPO.
AITI previously issued a Public Consultation Paper and invited the relevant stakeholders and interested parties from various industry groups and companies for their comments and feedback on the draft framework.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

The equivalent is referred to as the **Purpose Limitation Obligation** in the PDPO – 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. Organisations must acquire fresh consent where personal data collected is used for a different purpose from which the originally consented.

(b) Data Quality Principle

The equivalent is referred to as the **Accuracy Obligation** in the PDPO – an organisation must make a reasonable effort to ensure that personal data collected by it is accurate and complete, if it is likely to use such personal data to make a decision that affects the individual concerned, or disclose such personal data to another organisation.

(c) Purpose Specification Principle

Partly covered under the **Retention Limitation Obligation** in 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.

(d) Use Limitation Principle

The equivalent is referred to as the **Consent Obligation** in 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 authorized 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.

(e) Security Safeguards Principle

The equivalent is referred to as the **Protection Obligation** in the PDPO – an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a) unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

(f) Openness Principle

The equivalent is referred to as the **Notification Obligation** and this is linked to

the **Consent Obligation** in the PDPO – 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.

(g) Individual Participation Principle

Partly covered under the **Access, Correction and Data Portability Obligations** in the PDPO – 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 exceptions listed in the PDPO).

(h) Accountability Principle

An organisation will be required to 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.

Additionally, the PDPO sets forth the following obligations that require to be adhered to under the PDPO:

1)	**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.
2)	**The Data Breach Notification Obligation** – an organisation is 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 likely to be, of a significant scale.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle

- N/A

(b) Data Quality Principle

- N/A

(c) Purpose Specification Principle

- N/A

(d) Use Limitation Principle

- N/A

(e) Security Safeguards Principle

- N/A

(f) Openness Principle

- N/A

(g) Individual Participation Principle

- N/A

(h) Accountability Principle

- N/A

Note: AITI is still in the process of considering comments and drafting suggestions. AITI states that it shall include the appropriate exceptions, where applicable, in the finalised PDPO.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

- It is generally understood that public agencies are constrained in their ability to freely request for data or information as the Government's coercive powers are subject to Brunei's statutory provisions. The power to obtain personal data mainly consist of various agency's powers to investigate or to perform regulatory function in accordance with specific laws. To illustrate the scenarios in which such circumstances would apply, the following is a non-exhaustive list of examples of investigative powers exercisable by the responsible authorities of the Government with respect to the relevant legislation:

Legislation	Statutory Powers	Examples of Data that may be accessed
Prevention of Corruption Act (Cap 131)	Investigate and inspect any accounts including but not limited to investment accounts, bank accounts, mutual or trust fund accounts or require the production of any books, documents or other relevant article relevant to the person	Bank books or statement of accounts belonging to an individual under investigation.

		believed to have committed an offence with the approval of the relevant authorities under this Act.	
Immigration Act (Cap 17)		Section 28 – Obtain information as to the identity, nationality, or occupation or information bearing on any of the restrictions contained in this Act and demand all documents in the relevant person's possession relating to the aforementioned.	Passports or identity certificates or any other similar document to that effect for the purposes of entry into the country.
		Section 39 – Summon a witness and request the production of documents for the purposes of an inquiry or appeal under this Act.	
Environmental Protection and Management Order 2016		Section 12 – Require any production of any documents relating or reasonably believed to relate to any duty under provisions of this Order or any regulations made thereunder and take extracts therefrom.	Personal information belonging to an occupier of a premises under investigation, including an employment contract.
Safety, Health and Environment National Authority Order 2018		Schedule 1 – Request information from and collaborate or co-operate with any person on matters related to or connected with workplace safety and health, environmental protection and radiation control.	Personal information belonging to an individual involved in a workplace safety related incident, including an employment contract.
Petroleum Authority Order 2019		Section 47 – Request any person who is a party to a petroleum mining agreement or any person who has an ownership interest to furnish information or documents as the authority may require and produce such information or documents which the Authority consider necessary.	Employment contract of an individual employed in the petroleum industry (other than the authority)
Competition Order 2020		Section 34 – Require the person to produce a specified document or information which is deemed relevant under the Order.	Information belonging to suppliers/consumers under investigation, including an employment contract.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

AITI	**Contact Information**: **Tel**: + (673) 232 3232 **Fax**: + (673) 238 2447 **Email**: info@aiti.gov.bn **Address**: Block B14, Simpang 32-5, Kampung Anggerek Desa, Jalan Berakas BB3713, Brunei Darussalam. https://www.aiti.gov.bn/SitePages/Index.aspx