Authority for Info-communications Technology Industry of Brunei Darussalam

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

ISSUED BY

THE AUTHORITY FOR INFO-COMMUNICATIONS TECHNOLOGY INDUSTRY OF BRUNEI DARUSSALAM (AITI)

20 MAY 2021

NO.	REVISION RECORD	EFFECTIVE DATE	REMARKS
1	Version 1.0	20 May 2021	First date of publication
2	Version 1.1	15 June 2021	Extension of deadline

Contents

PUBLIC CONSULTATION PAPER

PART 1: INTRODUCTION AND BACKGROUND

The Minister of Transport and Infocommunications ("**MTIC**") has designated the Authority for Info-communications Technology Industry of Brunei Darussalam ("**AITI**") as the Interim Data Office to develop a new law for the protection of individuals' personal data (commonly referred to as a "**data protection law**"). This new data protection law, which will be developed taking into consideration various international data protection frameworks and local circumstances, is intended to apply to the **private sector** in Brunei Darussalam (covering both commercial and non-commercial organisations).[1]

A draft Personal Data Protection Order ("**PDPO**") has been developed and prepared to set out a general framework for data protection for the private sector in Brunei Darussalam. As explained in greater detail below, **the draft PDPO sets out the obligations of private sector organisations with respect to the collection, use, disclosure or other processing of individuals' personal data, the rights of individuals in relation to the processing of their personal data, and various matters relating to the administration and enforcement of the PDPO.**

AITI now invites all interested persons to comment and provide feedback on the proposed data protection framework for Brunei Darussalam based on the issues highlighted in **Part 2** of this Public Consultation Paper.

1. Introduction and Background Context

1.1 This Public Consultation Paper seeks views from the public on the proposed data protection framework for the private sector in Brunei Darussalam. This will eventually be incorporated into the PDPO.

1.2 The rationale of introducing this data protection law is two-fold:

1.2.1 to provide for the protection of individuals' personal data by private sector organisations (including both commercial and non-commercial organisations) which seek to collect, use, disclose or otherwise process such personal data for their purposes; and

1.2.2 to facilitate cross-border flows of personal data, which will further the development of the digital economy in Brunei Darussalam.

1.3 Presently, there is no overarching data protection legislation governing the processing of personal data by the private sector in Brunei Darussalam. While there may be sector-specific frameworks which have some form of data protection safeguards, there is currently no data

[1] For the public sector, the Official Secrets Act (Chapter 153) provides for the protection of official secrets, which may include personal information in the possession or control of the government and its officials. Furthermore, other official documents within the government sector such as the Data Protection Policy by the E-Government National Centre which relates to personal data (in electronic or manual form) collected and maintained by government agencies and the Protective Security Manual by the Internal Security Department, Prime Minister's Office, which provides common standards to ensure that information handled by government agencies is protected at all times.

protection law or framework at the national level. Further, while there are some private sector organisations that have designed and put in place policies relating to their processing of personal data, such policies are limited in scope, application and legal effect. Accordingly, the processing of personal data in the private sector is largely unregulated at this point in time.

1.4 Cross-border flows of personal data have also increased in significance in recent times as more businesses both in and outside Brunei Darussalam seek to process personal data for their purposes. Such activities may bring various socio-economic benefits to individuals and organisations in Brunei Darussalam, but also increase the risks to individuals' personal data.

1.5 In response to this, MTIC has given AITI the mandate to develop and implement a framework for the protection of individuals' personal data by the private sector. AITI has developed and prepared the draft PDPO, which sets out a general data protection framework which will apply to the private sector in Brunei Darussalam.

1.6 It is anticipated that the PDPO will operate concurrently with sector-specific frameworks and other legislation relating to data protection, and other laws generally. The PDPO will also provide for the establishment of a responsible authority ("**Responsible Authority**"), which will oversee the administration and enforcement of the PDPO.

1.7 The target date for the enactment of the PDPO is the end of 2021. To provide sufficient time for organisations to implement the necessary measures to comply with the PDPO, enforcement of the PDPO is targeted to commence in phases, starting in early 2022 with the establishment of the Responsible Authority. It is also anticipated that competency and skills development to implement the requirements of the PDPO will be supported by the Responsible Authority.

2. Need for a General Data Protection Regime

Public Interest

2.1 In light of advances in technology, including but not limited to, increased mobile and fixed broadband connectivity, the rise of the Internet and its various applications, together with advancements in the areas of data processing, Artificial Intelligence, machine learning and data analytics, there is an increasing need to protect personal data. This is especially the case given the increasing commodification of data and the growing public concern that consumers' personal data may be used, sold or otherwise processed without their consent or control.

2.2 Currently, there are no safeguards or restrictions placed on private sector organisations as to how they handle personal data. Some examples of the lack of rules governing the processing of personal data include the following:

2.2.1 A business may collect personal data from individuals for a specific purpose (e.g. lucky draws and contests) but subsequently go on to use such personal data for secondary purposes (e.g. to market different products and services to the individual, or sell this personal data to other third parties).

2.2.2 During the COVID-19 pandemic, businesses (e.g. supermarkets, shopping centres) were required to collect personal data about individuals to facilitate contact tracing. Such personal data was collected via the use of physical hardcopy logbooks at the entrance of premises. Many of these logbooks are often left out in the open without

any security measures to safeguard the personal data collected. Any member of public would be able to view the logbook and even take a photograph of all the personal data listed. This personal data can subsequently be used by that business of that third party for purposes not related to contact tracing.

2.2.3 A business may collect the personal data of individuals via online forms and subsequently store such data on publicly available directories online without any technical safeguards put in place. Anyone who does a search, using a search engine, for their name and personal information may be able to locate these publicly available lists / indexes of data.

2.2.4 A business may install CCTV cameras in its offices and collect the personal data of its employees or members of public who enter its premises (including but not limited to the reception area / lobby). These CCTV cameras are collecting personal data of employees and other individuals without anyone being aware or put on notice.

2.3 With respect to the above occurrences, businesses may not be held responsible for the personal data they collect and possess. As a corollary, the recourse which consumers may have against organisations which engage in irresponsible or inappropriate data processing activities that result in a negative impact on individuals is, practically speaking, limited or non-existent.

2.4 As a result, a lack of accountability amongst organisations with respect to their handling of personal data may lead to an erosion of consumer trust and other negative socio-economic consequences (for example, where consumers are reluctant to permit the collection of their personal data even where this may benefit them, the organisations involved, and society as a whole). This may be further exacerbated by instances of misuse of personal data, high-profile data breaches and other incidents. At the same time, organisations increasingly require personal data in order to better serve their customers, develop new and innovative products and services and for many other legitimate purposes. As such, the PDPO will govern the collection, use, disclosure and processing of personal data by private sector organisations in a manner that recognises:

2.4.1 the right of individuals to protect their personal data; and

2.4.2 the need of organisations to collect, use and disclose such personal data.

Economic Benefits

2.5 A strong personal data protection framework will promote the legitimate use of personal data by businesses and cross-border data flows in a sustainable and accountable way. Data protection laws are an increasingly common feature in developed and developing economies, and individuals internationally come to expect such laws to be in place to provide assurance with respect to the processing of their personal data.

2.6 In this regard, major jurisdictions such as the European Union ("**EU**"), Canada and Australia have put in place data protection laws (such as the EU's General Data Protection Regulation ("**GDPR**")) to better protect the personal data of individuals. Regionally, countries such as Singapore, Malaysia and the Philippines have also put in place data protection laws. There are also significant global data protection frameworks which have influenced the development of such domestic laws, such as the OECD Privacy Framework and Guidelines on the Protection of

Privacy and Transborder Flows of Personal Data. At the regional level, there is the APEC Privacy Framework and its frameworks for cross-border data transfers, the Cross-Border Privacy Rules System ("**CBPRs**") and Privacy Recognition for Processors System ("**PRPs**").

2.7 In addition, there are several specific ASEAN initiatives touching on data protection which Brunei has joined and / or affirmed. These initiatives include:

2.7.1 *ASEAN Economic Community (AEC) Blueprint 2025*, which calls for the establishment of a coherent and comprehensive data protection framework;

2.7.2 *ASEAN Digital Masterplan 2025 (ADM2025*), which calls for establishment of a data protection framework to enhance development opportunities across industry verticals; and

2.7.3 *Masterplan on ASEAN Connectivity 2025* and the *ASEAN Digital Data Governance Framework*, the latter of which includes initiatives on harmonising data protection laws and frameworks among ASEAN member states and developing an ASEAN cross-border data flows mechanism.

2.8 These initiatives demonstrate the commitment to propel ASEAN towards a digitally-enabled economy that is secure, sustainable and transformative. Developing and harmonising data protection laws and frameworks is expected to contribute to the promotion and growth of trade and flow of information within and among ASEAN member states, especially in relation to the ASEAN digital economy.

2.9 The lack of a general data protection law could potentially hinder the flow of personal data from Brunei to other countries and *vice versa*. Having such a law in place will strengthen Brunei's economic competitiveness and promote the growth of Bruneian businesses, especially in the area of data management and processing (including businesses that may process personal data as part of other business activities).

Other National Initiatives

2.10 The development of the general data protection law also ties in well with the strategic objectives of national initiatives such as the Digital Economy Masterplan 2025, which seeks to drive and enhance Brunei Darussalam's socio-economic growth through Digital Transformation. A robust data protection law is essential to the strategic outcomes[2] the Digital Economy Masterplan seeks to achieve.

2.11 The new data protection law will also complement the MTIC Strategic Plan 2025, which relates to a vision of a connected smart nation. The MTIC Strategic Plan seeks to utilise technology and connectivity to spur innovation and improve the lives and needs of citizens and businesses for continued national development through Digital Economy, Digital Government and Digital Society initiatives.

[2] The strategic outcomes of the Digital Economy Masterplan 2025 include: (a) a digital and future-ready society; (b) a vibrant and sustainable economy; and (c) a digitally conducive ecosystem. Flagship projects on Digital ID, Digital Payment and People Hub serve as the backbone of the ecosystem.

2.12 Finally, the development of a robust data protection law will support the growth of data processing capabilities and digitisation in industry sectors in Brunei Darussalam, and the establishment of an environment of trust amongst individuals, organisations and society at large.

2.13 We discuss the policy considerations and the key concepts of the draft PDPO below.

[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

PART 2: POLICY POSITIONS IN THE DRAFT PDPO

3. Definitions and Key Concepts

3.1 Definition of Personal Data

3.1.1 Under the PDPO[3], "personal data" is defined to mean "*data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access*".

3.1.2 In general, the term "personal data" (or the similar term, "personal information") is defined in various foreign data protection laws and international data protection frameworks to refer to information relating to an identified or identifiable natural person. The PDPO does not deviate from this approach. Notably, under the PDPO, an "individual" means a natural person, whether living or deceased. Furthermore, the definition of personal data does not differentiate between true or false personal data.

3.1.3 The PDPO will cover all forms of personal data, including both electronic and non-electronic forms of personal data. Although data is increasingly collected, processed and stored electronically, much data is still collected, processed and stored using non-electronic means (for example, lucky draw forms). A homogeneous treatment of all forms of data is thus proposed as it is more effective in achieving the objective of protecting consumer interests.

3.2 Categories of Personal Data

3.2.1 Personal data under the PDPO includes personal data which may be of a more sensitive nature, for example, data concerning the physical or mental health of an individual, financial information, genetic data, biometric data and personal history involving any criminal offence.

3.2.2 However, the PDPO does not expressly recognise a distinction between sensitive and non-sensitive categories of personal data or define a category of "sensitive personal data". It is proposed that the PDPO applies across all types of personal data as a baseline, although sector-specific frameworks may address specific concerns relating to different types of data (e.g. financial data). This approach is consistent with some laws, such as Singapore's Personal Data Protection Act 2012, although it differs from others, such as EU's General Data Protection Regulation.

3.2.3 As personal data which is of a more sensitive nature falls within the definition of personal data in the PDPO, it is subject to all the obligations in the PDPO. Organisations complying with the PDPO are required, as part of acting reasonably, to take into account the sensitivity of the personal data in question where appropriate, for example, in assessing the amount of information to be provided to individuals when collecting their personal data or when determining the security arrangements to be put in place to protect the personal data.

[3] In this Part 2, references to specific extracts of the PDPO are meant to be references to the draft PDPO.

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.

3.3 Organisations

3.3.1 In general (and subject to the specified exceptions noted in paragraph 3.4 below), the PDPO will apply to organisations, which is defined in the PDPO to mean "*any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Brunei Darussalam; or (b) resident, or having an office or place of business, in Brunei Darussalam*".

3.3.2 The PDPO will maintain a baseline regime that applies to all private sector organisations, including small businesses that have low annual turnover, to ensure a minimum data protection standard across the private sector. AITI notes that the exemption of small companies in some jurisdictions has added to the complexities of implementation and such exemptions may encourage larger companies to set up smaller entities to circumvent the law.

3.4 Exceptions from the Scope of Application

3.4.1 The PDPO contains the main data protection obligations (the "**Data Protection Obligations**") (as described and elaborated in Section 4 (Data Protection Obligations) below), which organisations must comply with. These Data Protection Obligations will be set out in the PDPO as the Data Protection Provisions (the "**Data Protection Provisions**").

3.4.2 For certain types of personal data, the PDPO contains exceptions from the application of the Data Protection Provisions.

3.4.3 Individuals acting in a personal or domestic capacity: Under the PDPO, individuals acting in a personal or domestic capacity are excluded from the applicability of the Data Protection Provisions. "Domestic" is defined in the PDPO to mean "related to home or family". An example of this would be an individual keeping an address book or contacts list with names, contact numbers, addresses and birthdates of friends and family for personal use.

3.4.4 Individuals acting as employees or officers of an organisation: Under the PDPO, individuals acting as employees[4] who are acting in the course of their employment with an organisation, and individuals acting in the course of an appointment as an officer of an organisation (e.g. any director, secretary or other similar officer of the corporation) are excluded from the applicability of the Data Protection Provisions[5].

[4] Under the PDPO, an "employee" includes a volunteer, trainee, apprentice or otherwise.

[5] Although we highlight that there are offences in the PDPO which aim to hold individuals (which may include employees and appointed officials of an organisation) accountable for egregious mishandling of personal data in the possession of or under the control of an organisation.

However, the organisation itself still has the responsibility to comply with the Data Protection Obligations. Under the PDPO, the organisation remains primarily responsible for the actions and omissions of its employees and officers, including any breaches of the PDPO caused by its employees and officers acting in the course of their employment. As such, organisations should develop and implement data protection policies and practices to ensure that their employees and officers comply with the Data Protection Obligations.

3.4.5 There may be other categories of individuals who obtain personal data, whether in the course of their own business (e.g. sole proprietors and partners of firms) or in the course of another organisation's business (e.g. independent contractors). Where they do so, the PDPO would apply to them directly (as they would fall within the meaning of the term "organisation" as defined in the PDPO). In other words, an individual may be considered an "organisation" for the purposes of the PDPO. Some examples would be property agents, insurance agents or financial advisors who are independent contractors or sole proprietors.

3.4.6 Business contact information: Except where expressly referred to, business contact information is excluded from the application of the Data Protection Provisions. "Business contact information" is defined in the PDPO to mean an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.

3.4.7 The reasons for the exclusion are largely centered around the difficulties in covering business contact information, and the fundamental question of whether such information belongs to the individual or the organisation (which is not always easily answered). The exclusion also takes into consideration that the transfer of business contact information is often integral to many business processes and that consent for the use of business contact information for certain purposes is often implied in the context where business contact information is exchanged.

3.4.8 Deceased Persons: The PDPO only requires private sector organisations to accord protection to deceased persons' personal data where such persons have been dead for 10 years or fewer. The PDPO does not apply to personal data about an individual that is contained in a record that has been in existence for at least 100 years.

3.4.9 In this regard, the PDPO seeks to obtain a balance between protecting the personal data of deceased individuals from unwarranted disclosure, which may have a negative impact on living relatives, and the ability of organisations to process personal data without requiring consent from parties authorised to act on behalf of deceased persons, which may be administratively difficult in certain situations and especially where the deceased individual passed away many years back.

3.5 Exclusion of the Public Sector

3.5.1 With regard to the scope of application, the PDPO governs the processing of personal data in the private sector, with a specific exclusion for public agencies.

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.

3.5.3 The PDPO is intended primarily to protect consumer data collected by the private sector. For the public sector, in addition to according the necessary levels of protection, the Data Protection Policy is designed to enable agencies to carry out their regulatory and statutory functions in an effective and accountable manner. Personal data is also collected, processed and shared in national emergencies such as the implementation of contact tracing in the event of a disease outbreak. As the means, purposes, and modes by which personal data is collected, processed and shared in the private and public sectors are very different, the Government has its own set of data protection rules which all government agencies would need to comply with, which are based broadly on the principles and obligations as set out in the PDPO, but deviates to take into account the needs of the Government in performing its public function. Applying both these rules and the PDPO may cause confusion amongst government officials where there are differences.

3.6 Territorial Scope

3.6.1 The PDPO applies to all private sector organisations that collect, use or disclose personal data in Brunei Darussalam, regardless of whether they are formed or recognised under Brunei law or whether they are resident or have an office or place of business in Brunei Darussalam.

3.6.2 As such, organisations that are located overseas may still be subject to the PDPO as long as they collect, use or disclose personal data (i.e. engage in data processing activities) in Brunei Darussalam. In addition, organisations that collect personal data overseas and host or otherwise process it in Brunei Darussalam will also be subject to the relevant obligations under the PDPO from the point that such data is brought into Brunei Darussalam.

3.6.3 It is acknowledged that there might be practical difficulties in carrying out investigations and taking enforcement actions against organisations with no presence in Brunei Darussalam, and any complaints against or contraventions made by such organisations may not be adequately addressed. Nonetheless, as a matter of principle, the scope of the PDPO should cover these organisations, and such coverage may act as deterrence for these overseas organisations such that they will process personal data in a responsible and accountable manner that is consistent with the PDPO. The Responsible Authority may, in due course, cooperate with foreign data protection authorities where necessary and appropriate to investigate a matter with cross-border elements.

3.7 Data Intermediaries / Processors

3.7.1 The PDPO contains a partial exception for “data intermediaries” (sometimes referred to as “data processors”) that process personal data on behalf of another organisation or a public agency. Such data intermediaries / processors doing so pursuant to a contract which is evidenced or made in writing are subject to a reduced number of Data Protection Obligations, namely:

(a) the Protection Obligation referred to in paragraph 4.2.9 below;

(b) the Retention Limitation Obligation referred to in paragraph 4.2.10 below;

(c) the Transfer Limitation Obligation referred to in paragraph 4.2.11 below; and

(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.

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.

3.7.3 The term "processing", in relation to personal data, is defined in the PDPO to mean the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: collection; recording; holding or storage; organisation, structuring, adaptation or alteration; retrieval; alignment or combination; use; disclosure by transmission, dissemination or otherwise making available; or erasure or destruction.

3.7.4 Data intermediaries / processors are required to comply with fewer Data Protection Obligations in view of their limited role in connection with the processing of personal data including, in particular, their lack of control over the purposes and other aspects of data processing (e.g. the scope of the data intermediary / processor's activities in relation to such personal data is restricted and subject to the contract between the data controller and the data intermediary / processor).

3.7.5 Subjecting data intermediaries / processors to fewer Data Protection Obligations will also reduce compliance costs for such organisations and potentially transactions costs as between data intermediaries / processors and data controllers.

3.7.6 Nonetheless, the organisations or data controllers engaging these data intermediaries / processors will be subject to the Data Protection Obligations in respect of personal data processed on its behalf and for its purposes by a data intermediary / processor as if the personal data were processed by the organisation or data controller itself.

3.7.7 Such an approach is also consistent with international norms as data protection regimes in most countries similarly require data controllers to be fully compliant with data protection laws and remain liable, even where they outsource the processing of personal data to a third party, regardless of whether there is a formal distinction between data controllers and data processors (as in the EU).

4. Data Protection Obligations

4.1 In general, various data protection principles which are recognised internationally are interwoven into the Data Protection Obligations which organisations are required to comply with. These principles include, for example, accountability; transparency; consent; and reasonableness.

4.2 The specific Data Protection Obligations, and the corresponding provisions of the PDPO, are:

4.2.1 the Accountability Obligation;

4.2.2 the Consent Obligation;

4.2.3 the Purpose Limitation Obligation;

4.2.4 the Notification Obligation;

4.2.5 the Access Obligation;

4.2.6 the Correction Obligation;

4.2.7 the Data Portability Obligation;

4.2.8 the Accuracy Obligation;

4.2.9 the Protection Obligation;

4.2.10 the Retention Limitation Obligation;

4.2.11 the Transfer Limitation Obligation; and

4.2.12 the Data Breach Notification Obligation.

4.3 Some of these Data Protection Obligations are subject to conditions or qualified by exceptions specified in the PDPO. Non-compliance by an organisation with any of the Data Protection Obligations may subject the organisation to administrative sanctions under the PDPO, including financial penalties (as described below).

4.4 Overall, the Data Protection Obligations are largely in line with the 9 main information privacy principles in the APEC Privacy Framework, namely: (a) Preventing Harm; (b) Notice; (c) Choice; (d) Collection Limitation; (e) Use of Personal Information; (f) Integrity of Personal Information; (g) Security Safeguards; (h) Access and Correction; and (i) Accountability.

4.5 <u>The Accountability Obligation</u>

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.

4.5.2 The Accountability Obligation allows consumers to contact the organisation easily in relation to queries about the organisation's data protection policies and issues related to the organisation's compliance with the PDPO. These aspects of data protection are sometimes referred to as transparency and individual participation. The concept of accountability in relation to personal data protection also relates to the undertaking

and demonstration of responsibility for the personal data in the organisation's possession or control. It is one of the key principles highlighted under the APEC Privacy Framework and also one of the obligations in the EU GDPR.

4.6 The Consent Obligation

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.

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.

4.6.3 Generally, organisations should generally look to express consent as the first port of call, and only rely on deemed consent or the exceptions to consent if obtaining consent is impractical, or if they have otherwise failed to obtain express consent.

4.6.4 Deemed Consent: There are circumstances where consent may be deemed under the PDPO, broadly:

(a) if the individual, without giving express consent, voluntarily provides the personal data for that purpose; and it is reasonable that the individual would voluntarily provide the data;

(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; and

(c) if the organisation, after conducting a prescribed assessment for adverse effect on the individual, notify the individual of the new purpose and provide a reasonable period of time for them to opt out (provided that the individual does not opt out or otherwise withdraw their consent).

4.6.5 These grounds for deemed consent (i.e. by conduct, by contractual necessity and by notification respectively), are broadly in line with grounds or legal bases for processing in other jurisdictions (e.g. processing necessary for the performance of contract under the GDPR).

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.

4.6.7 In this regard, organisations may consider some personal data necessary for the provision of good quality products or service, or supply of new products and services.

The requirement to not require individuals, as a condition to providing the product or service, to consent to processing beyond what is reasonable to provide the product or service, is corollary to the principle of data minimisation (i.e. that organisations should not collect more personal data than is reasonable and necessary). Furthermore, organisations should not be entitled to rely on consent obtained through deception or misleading information or practices.

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.

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.

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.

4.8.2 While the PDPO requires that such notice be provided to the individual on or before the collection, use and disclosure of his personal data, there is no prescribed manner or form in which such a notice must be given. This requirement relates to the principle of transparency, specifically, that organisations should be open about the purposes for which personal data is being processed so that individuals are able to make an informed decision as to whether to consent to such processing.

4.9 The Access, Correction and Data Portability Obligations

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.

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.

4.9.3 Individuals may request a porting organisation to port the individual's data to another organisation under certain circumstances, subject to certain exceptions in the PDPO.

4.9.4 Please see Section 5 (Data Subject Rights) below for more information.

4.10 The Accuracy Obligation

4.10.1 Under 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.

4.10.2 To ensure that decisions relating to the individuals are not made with outdated or otherwise erroneous data, it is important for organisations to ensure, to the extent that is practicable, that the personal data they collect and use is accurate. However, it may be overly onerous for it to be an absolute obligation, hence, organisations are required to make a reasonable effort to ensure that such personal data is reasonably accurate and complete if it is likely such personal data will be disclosed or used to make a decision which affects the individual.

4.11 The Protection Obligation

4.11.1 Under the PDPO, an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a) unauthorised 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.

4.11.2 To ensure that organisations are accountable to consumers in relation to the protection of their personal data, the PDPO 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.

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 unauthorised access, disclosure or other risks.

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.

4.12.2 The PDPO seeks to strike a balance between the need for organisations to retain personal data, where there are valid reasons to do so, and the requirement to delete

personal data (or render such data anonymous, such that the data is no longer personally identifiable). This obligation recognises that the longer the organisation retains the personal data, for instance, in perpetuity, the greater the risks of contravening the other Data Protection Obligations of the PDPO (e.g. that such personal data may be subject to a data breach or other unauthorised disclosure).

4.13 The Transfer Limitation Obligation

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.

4.13.2 The Transfer Limitation Obligation is to maintain the level of trust and confidence of consumers in Brunei Darussalam, especially as cross-border data transfers become more commonplace, e.g. in relation to cloud-based computing. It recognises that other jurisdictions may not necessarily have similar laws to protect the personal data transferred.

4.13.3 In this regard, some jurisdictions (e.g. EU) impose stringent and prescriptive conditions in relation to transfer of personal data outside of its territories. In contrast, the PDPO places the onus on the organisation to ensure that appropriate measures are taken to protect personal data transferred out of Brunei through the imposition of contractual obligations or otherwise.

4.14 The Data Breach Notification Obligation

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.

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.

4.14.3 In this regard, this mandatory notification requirement allows organisations to receive guidance from the Responsible Authority on post-breach remedial actions where necessary and informs the Responsible Authority early of any possible systematic issues within the organisation, which Responsible Authority can seek to address. Notifying affected individuals allows them to take steps, where possible, to protect themselves (e.g. changing passwords, cancelling credit cards) in the event of a data breach. This encourages accountability in organisations but also allows the Responsible Authority to have oversight over data breaches at a national level.

4.14.4 With respect to the criteria for notification, the Responsible Authority will take a risk-based approach and impose a threshold for notification. This is because not all data breaches justify notification, especially where the impact of the data breach is

minimal. It is acknowledged that organisations may require time to determine the veracity of suspected breaches. Accordingly, the time frame for notifying the Responsible Authority will thus commence from the time the organisation determines that the breach is eligible for reporting. Unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the Data Breach Notification Obligation.

5. Data Subject Rights

5.1 The PDPO will give individuals four main rights:

5.1.1 Right to withdraw consent;

5.1.2 Right to request access to personal data;

5.1.3 Right to request a correction of an error or omission in the personal data; and

5.1.4 Right to data portability.

5.2 These data subject rights are not unfettered and will be subject to exceptions in the PDPO. When an individual exercises any of these rights, organisations would have a corresponding obligation to give effect to these rights.

5.3 Right to Withdraw Consent

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.

5.3.2 Under the PDPO, the organisation is required to inform the individual of the likely consequences of withdrawing his consent.

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.

5.3.4 Withdrawal of consent does not affect the legal consequences of withdrawal. In other words, if the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out of such withdrawal would not be affected.

5.4 Right to Request for Access to Personal Data

5.4.1 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 exceptions. This is also known as the “Access Obligation”.

5.4.2 An organisation is only required to provide the individual with access to his personal data and the requested information. The organisation is not required to provide the individual with access to excluded information under this Access Obligation (see paragraph 5.4.6 below).

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.

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.

5.4.5 In this regard, “user activity data” is defined as personal data about an individual that is created in the course or as a result of the individual’s use of any product or service provided by the organisation, while “user-provided data” is defined as personal data provided by an individual to the organisation.

5.4.6 Organisations are not required to disclose certain types of information when responding to an individual's access request. Upon receiving an access request, an organisation is not required to provide information that is:

(a) opinion data solely kept for evaluative purposes;

(b) an examination conducted by education institution, examination scripts, results;

(c) personal data of beneficiaries of a private trust kept solely to administer the trust;

(d) personal data kept by an arbitral institution or mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

(e) documents related to prosecution if all proceedings have not been completed;

(f) personal data subject to legal privilege;

(g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

(h) personal data collected, used or disclosed without consent (in accordance with the PDPO) for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; or

(i) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act by agreement between the parties to the mediation or arbitration; under any written law; or by a court, arbitral institution or mediation centre.

5.4.7 An organisation does not have to respond to any access request:

(a) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;

(b) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;

(c) for information that does not exist or cannot be found;

(d) for information that is trivial; or

(e) that is otherwise frivolous or vexatious.

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.

5.4.9 If an organisation refuses to accede to an individual's access request, it must preserve a copy of the personal data for the prescribed period and ensure that that the copy is complete and accurate. This will ensure that the personal data which is subject to the access request is available in the event that the individual submits an application to the Responsible Authority to review the organisation's rejection of the access request.

5.5 Right to Request for a Correction to an Error or Omission in Personal Data

5.5.1 An individual may request an organisation to correct an error or omission in his personal data. This obligation only extends to personal data that is in the organisation's possession or under its control. This is also known as the "Correction Obligation".

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.

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.

5.5.4 When organisation A is notified by another organisation B of a correction of personal data, A shall correct the personal data in its possession or under its control unless organisation A is satisfied on reasonable grounds that the correction should not be made.

5.5.5 If no correction to the personal data is made despite a correction request, the organisation shall annotate the personal data record that the correction that was requested but not made.

5.5.6 An organisation is not required to correct or alter an opinion, including a professional or an expert opinion.

5.5.7 An organisation does not need to accede to an individual's correction request in certain situations. Upon receiving a correction request, an organisation not required to correct personal data that is:

(a) opinion data solely kept for evaluative purposes;

(b) an examination conducted by education institution, examination scripts, results;

(c) personal data of beneficiaries of private trust kept solely to administer the trust;

(d) personal data kept by an arbitral institution or mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

(e) documents related to prosecution if all proceedings have not been completed; or

(f) derived personal data.

5.6 Right to Data Portability

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".

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 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.

5.6.3 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.

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.

5.6.5 A porting organisation which does not transmit data upon receiving a data porting request must notify the individual of the refusal within the prescribed time and in the prescribed manner.

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.

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.

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.

5.6.9 A porting organisation is not required to port certain types of data:

(a) opinion data kept solely for an evaluative purpose;

(b) a document related to a prosecution if all proceedings related to the prosecution have not been completed;

(c) personal data which is subject to legal privilege;

(d) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

(e) personal data which has been collected, used or disclosed without consent (in accordance with the PDPO) for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; or

(f) derived personal data.

5.6.10 A porting organisation is not required to port data in the following circumstances:

(a) transmitting the applicable data will unreasonably interfere with the operations of the porting organisation because of the repetitious or systematic nature of the data porting request;

(b) the burden or expense of transmitting the applicable data is unreasonable to the porting organisation or disproportionate to the individual's interests;

(c) the data porting request relates to applicable data that does not exist or cannot be found or is trivial; or

(d) the data porting request is frivolous or vexatious.

5.7 Data portability, which is tied to data liquidity, ultimately gives more agency and control to the consumers. First, consumers stand to directly benefit when they have the ability to easily switch, at lower or no cost, to different market players, applications and services. Apart from increased flexibility and choices, consumers can also enjoy greater convenience as their data, contacts and / or settings are preserved. Second, the ability of consumers to move their data in response to changes in product or pricing naturally leads to more competition amongst existing players. Third, greater data flows can also reduce the barriers to market entry for potential data holders and open the door to increased innovation in the particular sector. Fourth, data portability will also encourage organisations to develop systems that are technologically compatible and interoperability formats that enable portability.

5.8 In a survey of the international landscape, the right to data portability has been introduced in the Philippines, Australia, and the EU. Moreover, Singapore and Thailand have the right to data portability in their respective data protection legislation, though these provisions have yet to come into force.

6. Investigations, Enforcement and Appeal

6.1 The PDPO provides for the setting up of a Responsible Authority to administer and enforce the PDPO.

6.2 Powers of Investigation

6.2.1 In the course of its investigations, the Responsible Authority may, upon complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation or a person is complying with the PDPO. The Responsible Authority's powers of investigation include:

(a) requiring, by written notice, an organisation to produce any specified document or specified information;

(b) examining orally any person who appears to be acquainted with the facts or circumstances of the matter;

(c) by giving at least two working days' advance notice of intended entry, entering into an organisation's premises without a warrant; and

(d) obtaining a search warrant to enter an organisation's premises and taking possession of, or remove, any document.

6.3 Penalties for Obstruction

6.3.1 An organisation or person who with an intent to evade an access or correction request disposes of, alters, falsifies, conceals or destroys a record containing personal data or other information; who obstructs or hinders the Responsible Authority or an authorised officer in the exercise of their powers or performance of their duties under the PDPO; or knowingly or recklessly makes a false statement to the Responsible Authority, or knowingly misleads or attempts to mislead the Responsible Authority, commits an offence for which that person would be liable upon conviction to a fine of up to B$10,000 and / or to imprisonment for a term of up to 12 months (in the case of an individual), or a fine of up to B$100,000 (in any other case).

6.3.2 Additionally, any person who neglects or refuses to comply with an order to appear before the Responsible Authority, or without reasonable excuse neglects or refuses to furnish any information or produce any document specified in a written notice to produce information, will be guilty of an offence punishable by a fine not exceeding B$10,000 or to imprisonment for a term not exceeding 12 months, or both.

6.4 Power to Issue Directions

6.4.1 The Responsible Authority will be given powers to issue directions to organisations to take specific steps or corrective measures to address non-compliance with the Data Protection Provisions. Some of these directions for non-compliance include:

(a) to stop collecting, using, or disclosing personal data in contravention of the PDPO;

(b) to destroy personal data collected in contravention of the PDPO;

(c) to provide access to or correct personal data; or

(d) if an organisation has intentionally or negligently contravened the Data Protection Provisions, to pay a financial penalty of up to B$1 million or up to 10% of the annual turnover of the organisation in Brunei Darussalam (whichever is higher).

6.4.2 With regard to the quantum of financial penalty, the Responsible Authority will be guided by the degree of harm caused by the breach, the seriousness of the violation and other factors. The amount must provide sufficient deterrence as well as serve to motivate organisations to put in place appropriate measures to safeguard personal data and comply with the PDPO.

6.5 Reconsideration and Appeal Mechanism

6.5.1 The PDPO provides for the establishment of a Data Protection Appeal Panel ("**DPAP**").

6.5.2 An individual or organisation aggrieved by a decision or direction of the Responsible Authority in the exercise of its powers under the PDPO may make a written application

to the Responsible Authority to reconsider its direction or decision. Thereafter, any individual or organisation aggrieved by the Responsible Authority's reconsideration decision may lodge an appeal to the DPAP.

6.5.3 Alternatively, an aggrieved individual or organisation may appeal directly to the DPAP without first submitting a reconsideration request.

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.

6.5.5 The Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal and, in particular, may: (i) remit the matter to the Responsible Authority**;** (ii) impose or revoke, or vary the amount of, a financial penalty; (iii) give any direction, or take any other step, that the Responsible Authority could itself have given or taken; or (iv) make any other direction or decision that the Responsible Authority could itself have made. The direction or decision of the Appeal Committee shall be final.

6.6 Right of Private Action

6.6.1 The PDPO provides for a standalone right of private action. An individual who suffers loss or damage directly as a result of a contravention of certain provisions of the PDPO may also commence a private civil action in court. The court may grant relief by way of injunction, declaration, damages or any other relief as the court thinks fit.

6.6.2 However, if the Responsible Authority has made a decision under the PDPO in respect of a contravention of the PDPO, the right of private action is only exercisable after all avenues of appeal, in respect of the relevant decision issued by the Responsible Authority, have been exhausted.

7. Offences Affecting Personal Data and Anonymised Information

7.1 There are specific offences in the PDPO which aims to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation. There are 3 main offences which the PDPO addresses.

7.1.1 Knowing or reckless unauthorised disclosure of personal data: If an individual discloses, or causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person, which is not authorised, and the individual does so knowingly, or is reckless to the disclosure not being authorised, the individual shall be guilty of an offence.

7.1.2 Improper Use of Personal Data: If an individual makes use of personal data in the possession or under the control of an organisation or a public agency, which is not authorised, and the individual does so knowingly, or is reckless to the use not being authorised, and as a result of the use of the personal data, the individual (a) obtains a gain, (b) causes harm to another individual, or (c) causes loss to another person, that individual shall be guilty of an offence.

7.1.3 Knowing or reckless unauthorised re-identification of anonymised data: If an individual takes any action to re-identify an affected person or cause the re-identification of anonymised information in the possession or under the control of an organisation or a public agency, which is not authorised, and the individual does so knowingly, or is reckless to the re-identification not being authorised, that individual shall be guilty of an offence.

7.2 For all 3 offences, the penalty is a fine not exceeding B$10,000 or imprisonment for a term not exceeding 2 years, or both. Notwithstanding, the PDPO provides for defences in respect of these offences, for example:

7.2.1 where the information is publicly available (or the information was publicly available solely because of an applicable contravention, and the accused did not know, and was not reckless as to whether, that was the case);

7.2.2 where the conduct is permitted or required under other laws;

7.2.3 where the conduct is authorised or required by an order of the court;

7.2.4 where the individual reasonably believes that he had the legal right to do so; or

7.2.5 in the case of the re-identification of anonymised information, the accused reasonably believed that the re-identification was for a specified purpose and notified the Responsible Authority or the organisation or public agency of the re-identification as soon as was practicable.

7.3 The aim of introducing these offences is to reinforce the accountability of individuals who have access to, and process, personal data by punishing the egregious mishandling of personal data (i.e. where the individual acted knowingly or recklessly).

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.

8. Do Not Call ("DNC") Regime

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.

8.2 As part of providing individual consumers with some level of control over the number of unsolicited commercial marketing messages received, the Responsible Authority may establish and administer a national DNC Registry for Brunei Darussalam, which would allow individuals to opt-out of marketing messages sent by way of phone call, text message (including Short Messaging Service and Multimedia Messaging Service) or fax. The registration of phone numbers on the DNC Registry will be free-of-charge.

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.

8.4 Personal messages, messages from charitable organisations soliciting donations and market research surveys are not considered marketing in nature and it is proposed that the DNC Registry will not block such messages. Marketing messages sent by way of email are not covered under the DNC regime.

8.5 Duty to Check the DNC Register

8.5.1 Under the DNC regime, a sender will have a duty to check the relevant DNC Register and obtain valid confirmation that the receiving Brunei telephone number is not on the DNC Register before sending the specified message to that number.

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.

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.

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.

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.

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).

8.7.2 All the information to be included in the specified message must be reasonably likely to be valid for at least 30 days after the specified message is sent.

8.7.3 In addition, the sender of the specified message must not conceal the calling line identity of the sender or perform any operation, or issue any instruction that would conceal or withhold the calling line identity.

8.8 Clear and Unambiguous Consent

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.

8.8.2 With respect to consent, similar rules apply in the context of the sending specified messages. The sender cannot require a subscriber or user of a Brunei telephone number to give consent to the sender to send them a specified message as a condition of contract unless it is reasonable to do so.

8.8.3 Similarly, the sender must not obtain consent to send a subscriber or user of a Brunei telephone number a specified message by providing them false or misleading information or by employing deceptive or misleading practices. Such consent will be deemed to be invalid.

8.8.4 A subscriber or user of a Brunei telephone number can revoke their consent to the sending of a specified message at any time by giving notice to the sender. The sender must stop sending the specified messages to that telephone number after the expiry of the prescribed period. It is proposed that this period be 21 days.

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.

8.9.2 However, there is a defence for an employee acting in good faith who does so in the course of his employment or in accordance with instructions given to him in the course of his employment will not be liable.

8.9.3 These provisions aim to deter spammers who randomly generate telephone numbers and send marketing messages (including robocalls) to those phone numbers. In many cases, spammers employ the use of dictionary attacks or exploit address harvesting software and other similar technologies to indiscriminately send unsolicited marketing messages to a high volume of recipients, causing consumer annoyance, inconvenience, and, in some cases, distress.

8.10 Enforcement of DNC Provisions

8.10.1 The DNC provisions are enforced under the same administrative regime as the Data Protection Provisions. If the Responsible Authority is satisfied that a person is not in compliance with the DNC provisions, the Responsible Authority may issue any direction to ensure compliance.

8.10.2 If a person is found to have intentionally or negligently contravened any of the DNC provisions, the Responsible Authority may require, by written notice, the organisation or person to pay a financial penalty.

(a) For a contravention of the DNC provisions (except the prohibition on use of dictionary attacks and address harvesting software), the financial penalty must not exceed a maximum of B$200,000 in the case of an individual; or B$1 million in any other case.

(b) For a contravention of the prohibition on use of dictionary attacks and address harvesting software, the financial penalty must not exceed a maximum of B$200,000 in the case of an individual; in case of a person whose annual turnover in Brunei Darussalam exceeds B$20 million — 5% of the annual turnover of the organisation in Brunei Darussalam; and B$1 million in any other case.

9. Regulations, Codes of Practice and Advisory Guidelines

9.1 The PDPO empowers the Responsible Authority to, with the approval of the Minister, make such regulations as may be necessary or expedient for carrying out the purposes and provisions of the PDPO and for prescribing anything that may be required or authorised to be prescribed by the PDPO.

9.2 It is anticipated that these regulations would include regulations in respect of the following matters: cross-border data transfer requirements, requirements governing the making of and responding to access and correction requests, rules concerning the assessment and notification of data breaches, and regulations to implement the data portability provisions.

9.3 In addition, the PDPO empowers the Responsible Authority to issue written advisory guidelines indicating the manner in which the Responsible Authority will interpret the provisions of the PDPO.

10. Interaction Between the PDPO and Other Laws

10.1 In terms of the interaction between the PDPO and other laws in Brunei Darussalam, it is envisioned that the PDPO will operate concurrently with other legislative and regulatory frameworks that apply to specific sectors.

10.2 There may be some provisions under existing written laws related to the collection, use, disclosure and processing of personal data. In this regard, the PDPO contains a provision on the subordination of the Data Protection Provisions of the PDPO to other written laws. The PDPO states that unless expressly provided in the PDPO:

10.2.1 nothing in the Data Protection Provisions shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law,

including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPO; and

10.2.2 the provisions of other written law shall prevail to the extent that any provision of Data Protection Provisions is inconsistent with the provisions of that other written law.

10.3 In other words, these exclusions recognise certain rights or privileges conferred under law, e.g. legal privilege, which would supersede the Data Protection Provisions. However, the provision of the other written law will apply only in respect of the matter(s) which is inconsistent between the two provisions. This means that the other provisions in the PDPO which are not inconsistent with the other written law will continue to apply.

10.4 Generally, the PDPO operates as a baseline law for data protection. Sectoral regulators are given the freedom and flexibility to provide higher levels of protection for personal data in their respective legislative and regulatory frameworks on top of the baseline requirements in the PDPO where necessary.

10.5 By way of illustration, certain categories, classes or types of personal data may be considered to be more sensitive in nature and therefore warrant stricter safeguards and standards of protection, e.g. health and medical personal data, or salary and financial information. The relevant sectoral regulators (e.g. Ministry of Health or Autoriti Monetari Brunei Darussalam) may wish to set higher levels of protection for these categories of personal data under the respective legislative or regulatory frameworks.

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.

11. Sunrise Period of Two (2) Years

11.1 AITI is proposing a "sunrise period" of 2 years from the time the PDPO is enacted (which is currently targeted to be Q4 of 2021).

11.2 During this "sunrise period", AITI or the Responsible Authority intends to conduct outreach and awareness-building programmes to educate the wider public about data protection and individual rights available under the PDPO.

11.3 AITI or the Responsible Authority will also engage various industries and associations as part of its outreach efforts to ensure that businesses are familiar with their obligations under the PDPO and will be able to comply with the requirements under the PDPO once the new data protection law takes effect.

11.4 Depending on whether it is necessary and appropriate, the Responsible Authority may issue further advisory guidelines for the public and / or selected industry sectors to provide greater clarity on specific issues at a later date, likely after the PDPO takes effect.

12. Existing Personal Data / Grandfathering Clause

12.1 The PDPO will not have retrospective application and will only apply to personal data that is collected, used and disclosed after the date of commencement.

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.

12.3 This grandfathering clause will only apply to the organisation's *use* and not *collection* or *disclosure* of existing personal data.

12.4 By way of illustration, if Organisation ABC has collected personal data from its customers prior to the commencement date for the purposes of providing after-sales customer support, Organisation ABC can continue to use the existing customer personal data to provide the customers with after-sales customer support after the PDPO comes into effect, even if Organisation ABC did not obtain consent previously.

12.5 However, after the PDPO comes into effect, Organisation ABC cannot use the existing personal data for purposes other than providing after-sales customer support (e.g. to send the customer direct marketing messages advertising new products), or disclose the existing customer personal data to another organisation. If Organisation ABC wishes to do so, it will need to seek fresh consent in accordance with the PDPO.

12.6 Aside from the continued use of existing personal data, the PDPO will not invalidate an organisation's contractual agreements with third parties in relation to the use and processing of existing personal data.

[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

PART 3: SUBMISSION OF COMMENTS

13. Submission of Comments

13.1 We would like to seek views and comments on the issues listed in **Part 2** of this Public Consultation Paper as well as relevant issues that may not have been specifically highlighted above.

13.2 Parties that wish to submit comments on this public consultation paper should organise their submissions as follows:

13.2.1 Cover page (including particulars of the organisation or individual, contact person, valid contact number and e-mail address);

13.2.2 Comments (with reference to specific sections or paragraphs if appropriate) together with relevant justification and analysis, data and information; and

13.2.3 Conclusion.

13.3 Supporting material may be placed in an annex. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any proposed revisions. Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.

13.4 All submissions should be submitted by **Wednesday, ~~16~~23 June 2021 no later than 5:00pm.**

13.4.1 Softcopy submissions should be submitted in both Microsoft Word and PDF formats, with the email subject "Public Consultation Paper on the Personal Data Protection for the Private Sector in Brunei Darussalam", to the following e-mail address: pdp@aiti.gov.bn.

13.4.2 Hardcopy submissions should be addressed and submitted to:

The Chief Executive
Authority for Info-communications Technology Industry for Brunei Darussalam
Block B14, Simpang 32-5,
Kampung Anggerek Desa, Jalan Berakas BB3713
Brunei Darussalam

SUBJECT: Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam

13.5 We reserve the right to make public all or parts of any written submission and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex.

13.6 If we grant confidential treatment, we shall consider, but shall not publicly disclose, the information. If we reject the request for confidential treatment, we shall return the

information to the party that submitted it and shall not consider this information as part of our review.

13.7 As far as possible, parties should limit any request for confidential treatment of information submitted. Any submission that requests confidential treatment of all, or a substantial part, of the submission will not be accepted.

13.8 Enquiries regarding this Public Consultation Paper can be directed to the following e-mail address: pdp@aiti.gov.bn.

[END OF DOCUMENT]