RESPONSE TO FEEDBACK ON 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)

3 DECEMBER 2021

NO.	REVISION RECORD	EFFECTIVE DATE	REMARKS
1	Version 1.0	3 December 2021	First date of publication

Contents

PART 1: INTRODUCTION 4
1. Introduction and Background 4
2. Public Consultation and Response 4
PART 2: FEEDBACK FROM RESPONDENTS AND AITI'S RESPONSE 6
3. Overview 6
3.1 Feedback on the Responsible Authority 6
3.2 Definition of Personal Data 6
3.3 Categories of Personal Data 7
3.4 Organisations 8
3.5 Exceptions from the Scope of Application 8
3.6 Exclusion of the Public Sector and Data Processors acting for Public Sector Organisations 9
3.7 Territorial Scope 10
3.8 Data Processors 11
4. Data Protection Obligations 12
4.1 Query on Penalties for Non-compliance 12
4.2 The Accountability Obligation 13
4.3 The Consent Obligation 14
4.4 The Purpose Limitation Obligation 15
4.5 The Notification Obligation 16
4.6 The Access, Correction and Data Portability Obligations 17
4.7 The Accuracy Obligation 17
4.8 The Protection Obligation 17
4.9 The Retention Limitation Obligation 18
4.10 The Transfer Limitation Obligation 19
4.11 The Data Breach Notification Obligation 20
5. Data Subject Rights 23
5.1 General Feedback 23
5.2 Right to Withdraw Consent 24
5.3 Right to Request for Access to Personal Data 25
5.4 Right to Request for a Correction to an Error or Omission in Personal Data 27
5.5 Right to Data Portability 28
6. Investigations, Enforcement and Appeal 29
6.1 Data Protection Appeal Panel 29
6.2 Powers of Investigation 29
6.3 Power to Issue Directions 30

6.4 Right of Private Action 31
7. Offences Affecting Personal Data and Anonymised Information 32
7.1 Query on Defences to Offences under the PDPO 32
7.2 Feedback on Exclusion of Personal and Criminal Liability 32
8. Do Not Call ("DNC") Regime 33
8.1 General Feedback 33
8.2 Prohibition Against Dictionary Attacks and Address-Harvesting Software 34
9. Regulations, Codes of Practice and Advisory Guidelines 34
9.1 Query on Stakeholder Consultations for Regulations 34
10. Interaction Between the PDPO and Other Laws 34
10.1 Query on Sectoral Regulations 34
11. Sunrise Period of Two (2) Years 35
11.1 Query on length of sunrise period 35
12. Existing Personal Data / Grandfathering Clause 36
12.1 Query on Application of Grandfathering Clause 36
13. General / Miscellaneous Comments 37
13.1 Query on Financial Penalties 37
13.2 Query on Representation for Vulnerable Individuals 37
13.3 Query on Data Custodians 37
PART 3: CONCLUSION 39
14. Concluding Remarks 39
ANNEX A 40

RESPONSE TO FEEDBACK ON PUBLIC CONSULTATION PAPER

PART 1: INTRODUCTION

1. Introduction and Background

1.1 The Minister of Transport and Infocommunications 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**") by private sector organisations (including both commercial and non-commercial organisations) in Brunei Darussalam.

1.2 Presently, there is no overarching legislation governing the processing of personal data by the private sector in Brunei Darussalam. While some private sector organisations may have designed and put in place policies relating to their processing of personal data, such policies may be 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.

1.3 AITI has developed and prepared the draft Personal Data Protection Order ("**PDPO**"), which sets out a general data protection framework which will apply to the private sector in Brunei Darussalam.

1.4 The rationale for introducing the PDPO is two-fold:

1.4.1 to provide for the protection of individuals' personal data by private sector organisations which seek to collect, use, disclose or otherwise process such personal data for their purposes; and

1.4.2 to facilitate cross-border flows of personal data and further the development of the digital economy in Brunei Darussalam.

1.5 Accordingly, the PDPO is intended to set 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.

1.6 The PDPO will operate concurrently with sector-specific frameworks relating to data protection, and other laws in Brunei Darussalam.

1.7 The PDPO is intended to be enacted by mid-2022. To provide sufficient time for organisations to implement the necessary measures to comply with the PDPO, enforcement of the PDPO will only commence two (2) years from the time the PDPO is enacted. It is also anticipated that competency and skills development to implement the requirements of the PDPO will be supported by AITI.

2. Public Consultation and Response

2.1 On 20 May 2021, AITI issued its *Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam* ("**Public Consultation Paper**") and invited interested persons to comment and provide feedback on the proposed data protection framework for Brunei Darussalam.

2.2 In conjunction with the issuance of the Public Consultation Paper, AITI conducted two public consultation sessions with relevant stakeholders and interested parties on 25 May 2021 and 27 May 2021.

2.3 AITI received a total of nineteen (19) responses from various industry groups and companies. The full list of respondents may be found in **Annex A**. Please refer to AITI's website for the full list of respondents and their submissions. AITI thanks all respondents for the comments submitted to the public consultation.

2.4 In terms of topics covered, AITI received feedback on all topics covered in the Public Consultation Paper. Many of the responses included questions as to how the PDPO would be implemented, e.g., questions on how the PDPO would be interpreted and how it would be administered.

2.5 Other respondents raised substantive data protection issues, in some cases, taking guidance from the data protection laws of other jurisdictions (e.g. Singapore's Personal Data Protection Act 2012 ("**Singapore PDPA**"), or the European Union's General Data Protection Regulation ("**EU GDPR**")). A few respondents also proposed suggestions on the drafting of the PDPO.

2.6 AITI will take such comments and drafting suggestions into consideration when finalising the PDPO. In relation to the questions on the interpretation, application and administration of the PDPO, it is envisaged that AITI may make regulations and issue advisory guidelines as appropriate to support the implementation of the PDPO.

2.7 This *Response to Feedback on the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam* ("**Response to Feedback on the PCP**") provides a summary of the key comments and queries raised by respondents to AITI's public consultation on the draft PDPO. It also set out AITI's views on the comments and queries received, taking into consideration the intended policy positions in the PDPO.

[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

PART 2: FEEDBACK FROM RESPONDENTS AND AITI'S RESPONSE

3. Overview

3.1 Feedback on the Responsible Authority

3.1.1 In the Public Consultation Paper, it was provided that the PDPO will also provide for the establishment of a responsible authority ("**Responsible Authority**"), which will oversee the administration and enforcement of the PDPO.

Feedback from Respondents

3.1.2 AITI received feedback from one respondent concerning the agency which would be established or assigned to implement and enforce the data protection framework (i.e. the Responsible Authority). The respondent suggested that the chosen agency should be one that is qualified, experienced, and independent from AITI. The respondent also suggested that the chosen agency should be in the business of facilitating cross-border transfers of data either as a data processor or data owner on a regular basis.

Response from AITI

3.1.3 Implementation and enforcement of a data protection framework under the PDPO is a regulatory function. It would not be suitable or appropriate for a private sector entity, which itself would be subject to the proposed data protection law, to be the chosen agency to implement, administer and enforce such a law. To the contrary, the chosen agency would need to be able to act independently from private sector entities (both data controllers ("**DCs**") and data processors ("**DPs**")) which are subject to the law.

3.1.4 Given the above requirements, it would be more appropriate for a public agency to take on the role of the developing and implementing the data protection framework within Brunei Darussalam. Since AITI has been appointed as the Interim Data Office to develop a new data protection law for Brunei Darussalam, in addition to being the info-communications regulator, it has also studied data protection regimes and considered pertinent data protection issues in great detail in the course of developing the PDPO framework. In this regard, AITI will be designated as the Responsible Authority for the administration and enforcement of the PDPO.

3.2 Definition of Personal Data

3.2.1 Under the proposed PDPO, "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*".

Feedback from Respondents

3.2.2 A large number of respondents asked for more clarification on the definition of "personal data" and requested for examples and illustrations. In particular, respondents asked if the definition of "personal data" needs to differentiate between true or false personal data; if publicly available data will be considered personal data; and if certain categories of personal data will be specified in the PDPO.

3.2.3 There were a number of comments concerning the anonymisation of personal data. Some respondents took the view that data that has been anonymised (i.e. where a data subject cannot be re-identified from that data) should be explicitly excluded from the scope of "personal data" under the PDPO.

Response from AITI

3.2.4 Personal data includes data about an individual that is in electronic or non-electronic form. While personal data primarily relates to the data of living individuals, there are some limited protections conferred on the personal data of deceased individuals. The PDPO does not provide a defined list of personal data or categories of personal data as there are many types of data that may form part of an individual's personal data. For example, an individual's personal data may include biometric data, images or voice recordings, DNA profile, contact information and biographical information (amongst others).

3.2.5 By definition, if a data subject cannot be identified by that data or by that data and other information to which the organisation has or is likely to have access, such data would not constitute personal data under the PDPO, regardless of whether any anonymisation techniques have been applied to the data.

3.2.6 However, there is some complexity surrounding the concept of anonymisation, de-identification and re-identification, particularly in respect of the different types of anonymisation techniques (e.g. data masking, aggregation, pseudonymisation), factors and considerations for anonymising data, and managing the risks of re-identification of anonymised data.

3.2.7 It is not sufficient to simply remove the name of the individual if the presence of other data in the dataset still allows organisations to identify the individual. Accordingly, the Responsible Authority shall provide further guidance on this point of anonymisation in due course.

3.3 Categories of Personal Data

3.3.1 In the Public Consultation Paper, it was stated that 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". However, 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.

Feedback from Respondents

3.3.2 Some respondents asked AITI to expressly clarify what constitutes "sensitive personal data". Respondents also sought clarification as to whether there are additional obligations attached to the processing of such sensitive personal data.

Response from AITI

3.3.3 In view of the comments, AITI clarifies that "sensitive personal data" will not be expressly defined in the PDPO and there will not be a fixed category of sensitive

personal data. This is because whether personal data will be considered "sensitive" in nature depends heavily on the context.

3.3.4 In general, if the potential adverse effects or harm to the individual is high, when such data is misused or subject to unauthorised access or disclosure, such data may be considered to be "sensitive". In such a scenario, to ensure appropriate protection for personal data that is considered to be "sensitive", the organisation may be required to put in place more stringent security measures in accordance with the Protection Obligation. To be clear, this is not dependent on the data being formally categorised or labelled as being "sensitive" but is part of organisations' obligations under the PDPO, in particular, to act in a reasonable manner and put in place reasonable security arrangements.

3.4 **Organisations**

Feedback from Respondents

3.4.1 One respondent asked about the definition of "small businesses" under the PDPO and requested for clarification of application of the PDPO to small businesses.

Response from AITI

3.4.2 The PDPO will apply to all private sector organisations, regardless of size or other characteristics (i.e. including small businesses and even sole proprietors) insofar as they collect, use and disclose personal data. As such, the PDPO will not include a separate definition of what constitutes a "small business".

3.5 **Exceptions from the Scope of Application**

3.5.1 The Public Consultation Paper sets out certain exceptions from the scope of application of data protection provisions of the PDPO, specifically, relating to (a) individuals acting in a personal or domestic capacity; (b) individuals acting as employees or officers of an organisation; (c) business contact information; and (d) personal data of deceased persons.

Feedback from Respondents

3.5.2 Several respondents sought clarification on the exceptions from the scope of application of the PDPO.

3.5.3 In relation to the employee exception (i.e. employees who act in the course of their employment or in accordance with instructions of their employer are excluded from the applicability of the Data Protection Provisions), respondents asked if the exception would still apply where an employee knowingly acts upon the instructions of their employer with a clear intent to use the data for wrongful or unlawful purposes.

3.5.4 With respect to the business contact information exception, one respondent asked if the personal information of connected parties (e.g. directors, shareholders, authorised signatories) may be deemed to be business contact information.

3.5.5 In relation to the exception for personal and domestic affairs and, in particular, the definition of "domestic" in the PDPO, one respondent suggested revising the definition of "domestic" in the PDPO from "related to home or family" to "related to personal affairs, home or family".

Response from AITI

3.5.6 In general, an organisation acts through its employees. If the management of an organisation instructs its employees to act in a manner that contravenes the PDPO, it will be a contravention on the part of the organisation and not the individual employee. Therefore, the onus is on the management of an organisation to put in place appropriate data protection policies and procedures to ensure that the organisation's employees handle personal data that it collects, uses and discloses in a manner that is in accordance with the PDPO. A failure to do so may constitute, or result in, a contravention of the PDPO and enforcement action may be taken against the organisation by the Responsible Authority. It is important to note, however, that there are specific offences in the PDPO which aim to hold individuals accountable for egregious mishandling of personal data which is not authorised by an organisation.

3.5.7 AITI clarifies that "business contact information" will be defined as 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. As such, this exception does not apply to personal data such as signatures of directors, shareholders and authorised signatories, that may be provided in a business context but are not part of the individual's *contact* information.

3.5.8 In relation to the exception for personal and domestic affairs, AITI takes the view that this proposed amendment is not necessary given that the exception from the Data Protection Provisions relates to individuals acting in his "personal or domestic capacity", which naturally includes an individual's personal affairs. As such, AITI intends to retain the original wording in the definition of "domestic".

3.6 Exclusion of the Public Sector and Data Processors acting for Public Sector Organisations

3.6.1 The Public Consultation Paper stated that the PDPO governs the processing of personal data in the private sector, with a specific exclusion for public agencies. 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.

Feedback from Respondents

3.6.2 As the PDPO does not apply to the Government of Brunei Darussalam and public agencies, some respondents inquired about the scope of the exception. In particular, some respondents inquired if the PDPO would apply to the Credit Bureau under the Brunei Darussalam Central Bank (**"BDCB")** previously known as Autoriti Monetari Brunei Darussalam ("**AMBD**"), Government-Linked Companies ("**GLCs**") and Perbadanan Tabung Amanah Islam Brunei ("**TAIB**").

3.6.3 Some respondents suggested that DPs acting on behalf of public agencies should also be excluded from the scope of the PDPO.

Response from AITI

3.6.4 In response to the feedback on the scope of the exception, AITI would like to first clarify that as the Credit Bureau is part of BDCB, a public agency, it would not be governed by the PDPO. However, other credit bureaus which may be operated by the private sector (if any) will not fall within the exception.

3.6.5 In relation to GLCs, as the PDPO is intended to apply generally to the private sector, all commercial entities will be subject to the PDPO in relation to their collection, use, disclosure and other processing of personal data in Brunei Darussalam. In this regard, GLCs will not be exempted from the PDPO.

3.6.6 TAIB is a body corporate established in Brunei Darussalam under the Perbadanan Tabung Amanah Islam Brunei Act (Cap 163) that serves as a financial institution. Since TAIB operates in a manner similar to a private sector entity and does not perform any public functions, it may be subject to the PDPO, however the Responsible Authority will conduct further engagement with TAIB prior to prescribing statutory bodies that will be excluded from the ambit of the PDPO.

3.6.7 In relation to DPs acting on behalf of public agencies, AITI highlights that all DPs have fewer obligations under the PDPO (i.e. Protection Obligation, Retention Limitation Obligation, Transfer Limitation Obligation, and the Data Breach Notification Obligation). These obligations involve aspects of data processing that are within the control of the DPs, and are not dependent on the liability or responsibility of the primary organisation.

3.6.8 Accordingly, the PDPO should not make a distinction between DPs of public agencies and those of private organisations, that is, the DPs of public agencies should be subject to the same obligations as those of private sector organisations.

3.7 Territorial Scope

3.7.1 The Public Consultation Paper stated that 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.

3.7.2 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.

Feedback from Respondents

3.7.3 There were a mix of comments received for this aspect of the PDPO. Some welcomed the extra-territorial scope, although one respondent suggested that the PDPO should only apply to DPs established within Brunei.

3.7.4 One respondent also suggested that the PDPO should target "residents" rather than "citizens" to ensure not only that all residents are treated equally but also that non-resident citizens in Brunei Darussalam are not subjected to conflicting laws.

3.7.5 Several comments in relation to the territorial scope of the PDPO also related to cross-border transfers of personal data. This will be discussed in the section 4.10 on the Transfer Limitation Obligation below.

Response from AITI

3.7.6 In this respect, AITI notes that internationally, countries recognise that there is potential for organisations to engage in data processing activities of residents without having presence in the territory. Accordingly, several other countries' data protection laws have some extraterritorial effect. Although enforcement may be challenging in such circumstances, AITI is aware that many global organisations do respect national laws when engaging in business activities in those countries. While countries may have their own data protection laws, there are often many similarities across different countries' laws, and having to comply with these laws is not a new issue for global organisations to deal with. In this regard, AITI has considered several international frameworks and other countries' laws (as described in the Public Consultation Paper) in developing the PDPO.

3.7.7 AITI also clarifies that that the PDPO does not use the term "citizen". Instead, it applies to "individuals", i.e. natural persons. This includes residents of Brunei Darussalam, e.g. individuals whose personal data is collected by an organisation in Brunei, as well as data of non-residents that may be collected overseas and brought into Brunei for processing.

3.8 Data Processors

3.8.1 The Public Consultation Paper stated that the PDPO contains a partial exception for DPs that process personal data on behalf of another organisation or a public agency. Such DPs 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; (b) the Retention Limitation Obligation; (c) the Transfer Limitation Obligation; and (d) the duty to notify the organisation or public agency under the Data Breach Notification Obligation.

3.8.2 For the avoidance of doubt, as DCs are considered "organisations" under the PDPO (and not this specific class of organisations known as DPs), and they will be subject to the full gamut of the Data Protection Obligations in the PDPO. It is important to note that the same organisation can be a data controller in certain instances (e.g. in respect of its own employees' data) and a data processor in others (e.g. when it is a vendor processing personal data on behalf of another organisation).

Feedback from Respondents

3.8.3 Many respondents sought greater clarification on the concept of DPs. Some respondents requested for examples of DPs, and one respondent asked whether

cloud services providers fall within such a category. Another respondent requested for examples of scenarios in which DPs would not be held liable.

3.8.4 Some respondents proposed that a DP should not be required to comply with the Transfer Limitation Obligation (as is the case in Singapore under the Singapore PDPA) in order to align the PDPO's position with the laws of other jurisdictions.

3.8.5 In relation to the duty of a DP to notify the DC of a data breach relating to personal data processed on behalf of the DC, please note that this point is addressed in section 4.11 on Data Breach Notification Obligation instead.

Response from AITI

3.8.6 In response to these comments, AITI clarifies that a DP is an organisation which processes personal data on behalf of another organisation pursuant to a contract which is evidenced or made in writing. One example of a DP is a cloud or data centre service provider which stores personal data for another organisation (i.e. the DC, which may be an organisation or public agency) pursuant to a written contract.

3.8.7 To the extent that an entity falls within the definition of a DP, it will only need to comply with the Protection Obligation, Retention Limitation Obligation, Transfer Limitation Obligation, and the Data Breach Notification Obligation. In the event of a potential breach of any of the foregoing obligations in relation to personal data that is processed by a DP on behalf of a DC, the Responsible Authority may investigate and consider, based on the evidence, whether the DP, the DC or both may be liable for the breach. If both may be liable, the Responsible Authority shall also consider how to apportion liability and what enforcement action to take against each respective party.

3.8.8 Furthermore, AITI does not intend to amend the PDPO to remove the requirement on DPs to comply with the Transfer Limitation Obligation. AITI notes that there may be situations where a DP which has been engaged by a DC to process personal data wishes to transfers the personal data outside Brunei Darussalam even though the DC does not need the personal data to be transferred overseas.

3.8.9 There are a number of situations where this may arise, typically where the DP will be processing the personal data for the DC outside of Brunei. For example, this may be the case where the DP is providing a cloud-based storage service involving its data centres outside of Brunei. Given that such data transfers are within the DP's control, the DP should be required to comply with the Transfer Limitation Obligation in respect of the personal data.

4. Data Protection Obligations

4.1 Query on Penalties for Non-compliance

Feedback from Respondents

4.1.1 Several respondents raised questions concerning the penalties for contravention of the PDPO.

Response from AITI

4.1.2 In response to this query, AITI clarifies that, in general, the Responsible Authority will have the power to issue directions to organisations which contravene the PDPO to take specific steps or corrective measures to address non-compliance. This may include a direction to pay a financial penalty of up to B$1 million or 10% of the annual turnover of the organisation in Brunei Darussalam (whichever is higher).

4.2 The Accountability Obligation

4.2.1 The Public Consultation Paper stated that the PDPO includes a proposed Accountability Obligation, pursuant to which 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.

Feedback from Respondents

4.2.2 Many respondents had questions about the requirement to appoint a DPO.

4.2.3 One respondent suggested that the Responsible Authority set up a public registry for DPOs.

4.2.4 A respondent raised a question of whether group policies may be implemented for a Brunei office.

Response from AITI

4.2.5 In this regard, AITI clarifies that while the PDPO requires all organisations (including small businesses) to appoint such an individual, AITI does not intend to impose further specific requirements in relation to such person(s). AITI intends to retain the language of the PDPO which leaves it up to the particular organisation to structure this function. As such, the organisation has the freedom to appoint someone from within the organisation to the DPO or outsource the DPO function to a third-party service provider. Depending on the scale of the organisation's data processing, the DPO could be an individual contributor (who may, in appropriate cases, perform the role in addition to other functions or duties) or a manager leading an entire data protection team.

4.2.6 Furthermore, while the DPO does not need to be physically located or based in Brunei Darussalam (the most common scenario is where the DPO is the regional or global head of data protection based in another jurisdiction), it is the intention that the appointed DPO should be available to answer queries from data subjects who are resident in Brunei. Hence, if a telephone number is provided as a means of contacting the DPO, the telephone number should be a Brunei telephone number which is operational during normal business hours in Brunei. AITI may issue advisory guidelines to provide further clarity and guidance on this topic.

4.2.7 In relation to a public registry for DPOs, AITI notes this suggestion and will take it into consideration.

4.2.8 In relation to whether group policies may be implemented for a Brunei office, AITI takes the view that adoption of group data protection policies and practices will be acceptable insofar as such policies and practices are able to adequately address the specific requirements of the PDPO.

4.2.9 AITI acknowledges that the data protection laws of certain jurisdictions may impose a more stringent level of protection for personal data as compared to the PDPO, but reminds all organisations that it is not the case that compliance with such foreign laws would automatically equate to compliance with the PDPO, particularly in relation to personal data that is collected, used, disclosed or processed in Brunei Darussalam. Moving forward, organisations should be mindful of the differences in the data protection requirements under the applicable data protection laws.

4.3 **The Consent Obligation**

4.3.1 The Public Consultation Paper also set out the Consent Obligation, i.e. 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.

Feedback from Respondents

4.3.2 In respect of the Consent Obligation, many respondents provided suggestions relating to exceptions to consent (e.g. concerning legitimate interests and business improvement purposes), and the grounds relating to deemed consent. Several of these suggestions were based on similar provisions in other countries' data protection laws.

4.3.3 Several respondents also asked for clarification on certain specific situations, e.g. lucky draws, roadshows, sale of personal data, deemed consent, and providing consent on behalf of another.

4.3.4 One respondent asked AITI whether, in a scenario where a customer signs the terms and conditions and provides their consent for the disclosure of his or her personal data, such consent would constitute sufficient consent under the PDPO.

4.3.5 A respondent commented that obtaining express consent for each new purpose that may arise throughout the course of an ongoing relationship with a consumer would be burdensome and time consuming, and proposed for consent to be deemed or implied given unless and until individuals submit their objection.

4.3.6 A respondent also asked about the processing of personal data of minors / children.

Response from AITI

4.3.7 In relation to the proposed exceptions to consent, AITI notes the feedback given and will take these comments and suggestions into consideration.

4.3.8 For specific situations, AITI clarifies that there is no specific exclusion in the PDPO for activities such as lucky draws, roadshows and the sale of personal data. In such situations, unless the organisation can avail itself of a specific exception under the PDPO, the collection, use and disclosure of personal data pursuant to such activities would require prior consent (or deemed consent) of the individual in question. AITI may provide further guidance on this at a later stage.

4.3.9 In response to the query relating to the terms and conditions, AITI clarifies that when an individual enters into contract with an organisation and agrees to the terms and conditions, his or her consent would be limited to the scope of that particular contract and the organisation can use his or her personal data only for the purposes which the individual has been notified of. The individual's consent does not extend to purposes that are beyond the scope of the contract, or to purposes that have not been notified to the individual. In other words, the individual's consent is not a blanket consent. Organisations cannot collect an individual's personal data for one purpose and then use or disclose the personal data for another purpose (without the individual's consent or unless otherwise permitted by law). Further, organisations should act reasonably when obtaining consent and should not, for example, use false or misleading practices to do so.

4.3.10 By way of illustration, if an organisation obtains an individual's consent to collect, use and disclose his or her personal data for the purposes of providing him or her goods and services, the organisation cannot rely on the consent to also send the individual marketing or promotional information about other goods and services, as this purpose was not originally notified to the individual at the point of collection. If the organisation wishes to send the individual promotional information, the organisation must notify the individual of this and obtain the individual's express consent.

4.3.11 For the suggestion relating to deemed or implied consent, AITI intends to provide such a ground for deemed consent, subject to certain conditions and safeguards, in the PDPO.

4.3.12 In relation to the processing of the personal data of minors, AITI confirms that the PDPO will apply to the personal data of all individual, including minors. For young children who are unable to give consent to organisations to collect, use and disclose their personal data, organisations will need to obtain consent from the child's parent or legal guardian (i.e. in accordance with the law in Brunei). AITI provide further guidance on data processing activities relating to minors at a later stage.

4.4 **The Purpose Limitation Obligation**

4.4.1 The proposed Purpose Limitation Obligation under the PDPO provides that 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.

Feedback from Respondents

4.4.2 Several respondents had queries on the definition of "reasonable purpose". The respondents asked whether a particular activity would constitute a reasonable purpose or an unreasonable purpose in the circumstances.

Response from AITI

4.4.3 In response to the queries, AITI does not intend to provide a fixed list or category of reasonable purposes in the PDPO. AITI's intention is to provide organisations with the flexibility to determine the purposes for the collection, use or disclosure of personal data in the context of their specific business activities and operations. Notwithstanding, the purposes should be clear and comprehensive enough to cover the intended data processing activities such that individuals are aware as to how their personal data will be collected, used and disclosed.

4.5 The Notification Obligation

4.5.1 The proposed Notification Obligation under the PDPO provides that 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 the individual's 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.

Feedback from Respondents

4.5.2 Several respondents raised questions concerning the application of the Notification Obligation and how it would interact with the Consent Obligation, e.g. whether both notification to the individual and consent are required at the same time.

4.5.3 One respondent suggested that when providing individuals with notice, organisations should be required to specify the "classes of transferee" of personal data within the notice, as is the case under Hong Kong's data protection law.

4.5.4 Another respondent raised the issue of secondary purposes and asked if there will be an exception for such purposes. It asked whether an organisation that obtains consent to use an individual's personal data to process the transaction to deliver goods to an individual needs to obtain the same individual's consent for ancillary purposes such as checking / updating the inventory or for the purpose of preparing the organisation's accounts.

Response from AITI

4.5.5 In response to this feedback, AITI clarifies that for consent to be considered "valid consent" under the PDPO, one of the requirements is that the individual would need to be notified of the purposes for which his or her personal data will be collected, used and/or disclosed, on or prior to the individual providing his/her consent.

4.5.6 In this regard, AITI notes that the purpose of the Notification Obligation is to ensure that the individual is provided with adequate notification when his or her personal data is collected, used or disclosed for a particular purpose. Generally, information on the particular transferee or class of transferees would be considered information that is good-to-have. However, AITI does not intend for this to be a mandatory requirement under the PDPO. For example, if an individual makes an online purchase and consents to use of personal data for delivery of goods, it will not be strictly

necessary to specify to the individual that his or her personal data would be disclosed to delivery companies in order to carry out the delivery. Notwithstanding, organisations should make it clear to the individuals what their personal data may be used for, and to whom will their personal data be disclosed.

4.5.7 In response to this feedback, AITI does not intend to include this specific exception in the PDPO. Notwithstanding, even though this exception may not be expressly stated in the PDPO, such ancillary purposes may be inferred and understood from the primary purpose. Insofar as organisations act reasonably when using personal data for ancillary purposes, separate consent for such specific ancillary purposes is not required.

4.6 The Access, Correction and Data Portability Obligations

4.6.1 Please refer to Section 5 below on Data Subject Rights.

4.7 The Accuracy Obligation

4.7.1 The proposed Accuracy Obligation under the PDPO provides that 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.

Feedback from Respondents

4.7.2 Most of the comments from respondents for this section were requests for clarification as to what constitutes "reasonable effort" to ensure that personal data collected and used is accurate and complete.

4.7.3 A respondent suggested that burden of accuracy should lie with the individual providing the information as opposed to the organisation.

Response from AITI

4.7.4 As to what constitutes "reasonable effort", AITI will address this point in advisory guidelines to be issued in due course. In general, AITI is of the view that where an organisation is collecting personal data directly from an individual, it is reasonable for organisation to rely on that at that juncture in terms of accuracy. However, in other situations, for example, when personal data is provided to the organisation by third parties, or the organisation has reasons to suspect that the personal data provided by the individual may be incorrect or outdated, then the organisation should consider what other reasonable steps it needs to take to ensure accuracy of the data.

4.8 The Protection Obligation

4.8.1 The proposed Protection Obligation under the PDPO provides that 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.

Feedback from Respondents

4.8.2 In general, the respondents appreciated the need for flexibility in the context of security measures, with one respondent supporting the fact that the PDPO did not purport to prescribe security standards or specific security measures. The respondent commented that organisations should be empowered to decide the nature of security measures appropriate to them and the data processing in question based on the given circumstances.

4.8.3 Similarly, another respondent proposed that a higher security standard could be required from organisations which provide direct-to-consumer goods as their core activities as such organisations require regular and systematic processing of consumer personal data on a large scale.

4.8.4 The respondents also requested for clarification as to what would constitute reasonable security measures.

Response from AITI

4.8.5 In relation to the standard required (i.e. reasonable security measures), AITI intends to provide more detailed guidance on the types of security measures, which will include administrative / organisational, physical and technical security measures, in due course.

4.9 The Retention Limitation Obligation

4.9.1 The proposed Retention Limitation Obligation under the PDPO provides that 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.

Feedback from Respondents

4.9.2 Several respondents requested for examples of situations that may result in a breach of the Retention Limitation Obligation. Some respondents asked AITI whether their specific examples of data (e.g. an individual's credit / debt history, investigation conducted by the authorities, retention of credit control information, and internal use of market and segmentation analysis) would constitute valid reasons for data retention.

4.9.3 One respondent proposed introducing an amendment to clarify that DPs should only be subject to the Retention Limitation Obligation in relation to their responsibility to securely delete personal data processed for the primary organisation once their business relationship ends.

Response from AITI

4.9.4 In this regard, AITI takes notes of the queries and intends to issue further guidance on this topic. Nonetheless, AITI wishes to take the opportunity to clarify that there is no

change to existing legal obligations to retain data. Therefore, if an organisation is required to retain a record (which may contain personal data) due to a mandatory obligation under another written law, this would not be in contravention of the PDPO. A common example would be the requirement for organisations to retain certain types of employee-related personal data under employment laws and regulations. For more details, please see Section 10 on Interaction between the PDPO and Other Laws below.

4.9.5 Furthermore, AITI notes that the retention of personal data of the DP to fulfil the purposes of a contract with the DC is a valid business purpose. However, the DP would not be able to retain the personal data for an indefinite or excessively long period of time after the contract is terminated for no valid business or legal reason.

4.9.6 In general, organisations may retain personal data they have collected from an individual for purposes that the individual has consented to, unless an exception applies. If the organisation does not have consent to use the individual's personal data for marketing purposes, the personal data cannot be retained for marketing. A valid business reason would be related to the purposes for which the organisation has consent, e.g. to supply the individual with goods and services. Accordingly, if the organisation needs to hold on to the personal data for a certain period of time (e.g. to satisfy the statutory minimum periods prescribed under law), this would be a valid business reason for organisations to retain personal data.

4.9.7 Organisations should also note that retaining personal data for a longer period than necessary increases risks of contravention of other Data Protection Obligations. For example, in the event that there is data breach and personal data is leaked which had been retained beyond what is permitted under the PDPO, the organisation may contravene the Protection Obligation as well as the Retention Limitation Obligation. Organisations are encouraged to periodically review the personal data that it holds to ensure that personal data is not retained when it is no longer required for any legal or business purpose. This would also prevent the organisation from incurring additional costs of storing and managing the personal data.

4.10 **The Transfer Limitation Obligation**

4.10.1 The proposed Transfer Limitation Obligation under the PDPO provides that 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.

Feedback from Respondents

4.10.2 In this section, most respondents requested for further details on how the Transfer Limitation Obligation would operate under the PDPO. Several respondents offered suggestions as to the kind of cross-border transfer mechanisms that should be included. One respondent suggested for transfer mechanisms (e.g. contractual safeguards) to be aligned with those found in the data protection laws of other jurisdictions such as those in the EU GDPR and the Singapore PDPA.

4.10.3 One respondent proposed that AITI create a whitelist of jurisdictions deemed to have comparable standards with the PDPO in order to facilitate cross-border data flows.

4.10.4 Some respondents proposed for there to be an exception in the PDPO to the Transfer Limitation Obligation for intra-group cross-border data transfers. In general, such an exception is not commonly found in other data protection laws (if at all).

4.10.5 Some respondents commented that the Transfer Limitation Obligation should be positioned more positively to support cross-border data flows.

Response from AITI

4.10.6 AITI notes the feedback and proposed suggestions and will prescribe detailed requirements on the cross-border transfer mechanisms in due course.

4.10.7 With respect to the exception for intra-group data transfers, AITI does not intend to provide for such an exception in the PDPO. Many companies operating globally are already subject to data protection laws which contain requirements relating to cross-border transfers and having an intra-group transfer mechanism is one common approach to ensure that the personal data which is transferred to other jurisdictions within the same group are protected in accordance with the applicable legal requirements.

4.10.8 In relation to supporting cross-border data flows, AITI highlights that the PDPO does not seek to restrict cross-border data flows, as this is diametrically opposed to one of its objectives. Instead, the purpose of the Transfer Limitation Obligation is to ensure that organisations transfer personal data in an accountable manner and ensure that that the transferred personal data is protected to a standard comparable with the laws of Brunei. AITI intends to provide more guidance concerning the specific cross-border data transfer mechanisms at a later date.

4.11 The Data Breach Notification Obligation

4.11.1 The proposed Data Breach Notification Obligation ("**DBN Obligation**") under the PDPO provides that organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the AITI 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.

4.11.2 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.

4.11.3 Many respondents sought clarification on how the DBN Obligation would be implemented, for example, in relation to the notification thresholds, namely what constitutes "significant harm" and "significant scale", the timelines to notify the Responsible Authority, and the format of such a notification. Many of these details will be prescribed in due course in regulations and guidance. In the meantime, AITI

takes the opportunity to address some of the more pertinent comments from the respondents.

Feedback from Respondents

4.11.4 Scope of application: Some of the queries from the respondents related to how the DBN Obligation would apply to DPs.

4.11.5 Definition of data breach: In relation to the definition of "data breach", one respondent suggested that the definition should only pertain to a loss of a storage device that *actually* results in such unauthorised access or disclosure etc., and not where the unauthorised access or disclosure is "likely to occur".

4.11.6 Notification threshold: A data breach is notifiable to the Responsible Authority where the data breach meets the threshold prescribed in the PDPO, i.e. if the data breach:

(a) results, or is likely to result, in significant harm to an affected individual; or
(b) is, or is likely to be, of a significant scale.

4.11.7 In relation to the threshold of significant harm under sub-paragraph (a) above, some respondents suggested that this include a materiality standard, i.e. where there is material risk of harm.

4.11.8 In relation to the threshold of significant scale under sub-paragraph (b) above, one respondent indicated that this would involve assigning an arbitrary number.

4.11.9 Timeframe for notification: With respect to the timeframe to notify the Responsible Authority (i.e. 3 calendar days from determining that the data breach is notifiable), respondents sought clarification as to whether the clock would start running (a) once the organisation's assessment contains substantial evidence or (b) once there is no doubt that a data breach has indeed occurred.

4.11.10 Many respondents voiced concerns about the timeframe being too short, and proposed suggestions to extend the timeframe to 3 business days or 7 calendar days for instance.

4.11.11 Some respondents have suggested setting limits to the duration of the assessment process to determine whether the data breach is notifiable.

4.11.12 Remediation: One respondent sought clarification on whether post-breach remedial actions from the Responsible Authority would be mandatory or whether organisations would have the discretion to implement the appropriate remedies internally.

4.11.13 Exceptions to Requirement to Notify Individuals: Some respondents suggested that the PDPO should include exceptions to the requirement to notify the affected individuals, for instance: (i) where the individual in question is the subject of an ongoing or potential investigation; or (ii) where the personal data has been encrypted to a reasonable standard.

Response from AITI

4.11.14 Scope of application: AITI clarifies that the PDPO will expressly provide that a DP has the obligation to notify the primary organisation (which may include public agencies, if applicable) without undue delay when it has reason to believe that a data breach relating to the personal data they are processing on behalf of primary organisation has occurred.

4.11.15 Definition of data breach: AITI highlights that a data breach is intended to address the situation where there is a *risk* of such unauthorised access, disclosure, etc. occurring. By way of illustration, if a malicious actor breaks into a computer network but no personal data is exfiltrated, it would still be a data breach as the personal data in the organisation's possession or control was put at risk. Further, in many situations, it may not be entirely clear whether some or all of personal data at risk had actually been exfiltrated.

4.11.16 Furthermore, the PDPO will provide an exception for data breaches that occur within an organisation. In other words, a data breach would only extend to the risk of unauthorised access, disclosure, etc. outside the organisation. For example, if an employee were to accidentally send a file containing personal data to another employee within the same organisation, such an incident will not constitute a data breach under the PDPO.

4.11.17 Notification threshold: AITI clarifies that this significant harm threshold similarly seeks to ensure that only data breaches where there is a significant risk of harm are notified to the authorities. As such, a further materiality requirement is not necessary. In this regard, AITI does not intend to amend this threshold.

4.11.18 In relation to the threshold of significant scale, AITI notes that any number chosen may appear arbitrary. However, a threshold is required to address data breaches which are of a scale that is of interest to the Responsible Authority. In prescribing the threshold number, it is expected that the Responsible Authority will take into account international norms. The Responsible Authority will be coming up with guidelines on "significant harm" and "significant scale" in the near future.

4.11.19 Timeframe for notification: With respect to the timeframe to notify the Responsible Authority (i.e. 3 calendar days from determining that the data breach is notifiable), AITI acknowledges that there may be times where there is some uncertainty as to whether the threshold is crossed. As such, the proposed test is whether the data breach is likely to result in significant harm or be of significant scale.

4.11.20 In relation to concerns that the timeframe for notification is too short, AITI highlights that the timeline only starts running when the organisation determines that the data breach is notifiable, and organisations are given a reasonable duration to make the assessment if this is the case.

4.11.21 As stated above, some respondents have suggested setting limits to the duration of this assessment. AITI is aware that organisations may have different requirements regarding the conduct of the assessment (e.g. organisations may need longer or shorter timeframes depending on the type, nature and/or location of the data breach,

or other relevant factors). As such, setting a fixed time for organisations to assess whether a data breach is notifiable may be unduly restrictive and counterproductive.

4.11.22 Remediation: AITI clarifies that in the event of a data breach, the organisation should consider and take the necessary remediation action to rectify and prevent reoccurrence. Such actions would form part of their obligations under the Protection Obligation. If the Responsible Authority investigates and finds the organisation did not have reasonable security measures in place, the Responsible Authority will consider the necessary remediation actions. The Responsible Authority may issue directions requiring organisations to take remediation actions if it considers that the remediation actions taken were insufficient, or take such other enforcement action as provided for under the PDPO.

4.11.23 Exceptions to Requirement to Notify Individuals: AITI will consider the comments further and include the appropriate exceptions to the requirement to notify affected individuals in the PDPO.

5. Data Subject Rights

5.1 General Feedback

5.1.1 AITI had proposed for the PDPO to contain four main data subject rights: (a) the right to withdraw consent; (b) the right to request access to personal data; (c) the right to request a correction of an error or omission in the personal data; and (d) the right to data portability. These data subject rights are subject to exceptions which will be enumerated in the PDPO.

5.1.2 For ease of reference, organisations' obligations in respect of the above-mentioned rights are referred to as the Consent Obligation, the Access Obligation, the Correction Obligation and the Data Portability Obligation respectively.

Feedback from Respondents

5.1.3 Many respondents provided feedback on the proposed data subject rights. Some respondents expressed broad support for the proposed data subject rights. One respondent suggested that additional rights such as the right to be informed be included in the PDPO. Another respondent expressed concern over the inclusion of user activity data and user provided data under the Access Obligation and the Data Portability Obligation as it would be onerous for organisations to comply with. Therefore, the respondent suggested that user activity data and user provided data be excluded from both the Access Obligation and Data Portability Obligation.

5.1.4 Several respondents provided feedback on the operation of the data subject rights. One respondent suggested that a flexible timeframe be adopted for responding to access requests, making reference to the approach adopted in the Singapore PDPA which requires organisations to either respond to and facilitate an access request or reject the access requests for a permitted reason within a specific timeframe, or otherwise notify the individual of the alternative timeframe within which the organisations will respond to the request. It was also suggested that the access, correction and data portability rights be subject to a reasonable trade secrets exception.

5.1.5 Several respondents also raised concerns with the operation of the provisions relating to data portability and the scope of the Data Portability Obligation.

Response from AITI

5.1.6 With respect to the suggestion to include the right to be informed, AITI is of the view that the right to be informed is sufficiently addressed by the Notification Obligation in the PDPO. The two concepts are similar in substance, i.e. both impose an obligation on the organisation to provide individuals with information as to the purposes for which their personal data will be collected, used and disclosed. In the context of the PDPO, which requires organisations to notify and obtain the individual's consent before collecting his or her personal data, it would be unnecessary to also provide for a distinct right to be informed.

5.1.7 AITI notes the suggestions and feedback on the Access Obligation and clarifies that the timeframe for responding to access requests will be prescribed in the relevant regulations to be issued under the PDPO and/or elaborated in further detail in advisory guidelines. AITI also highlights that the PDPO presently provides for a reasonable trade secrets exception to the rights to access and data portability. AITI takes the view that such an exception would not be necessary for the right to correction.

5.1.8 AITI notes that data portability and related concepts such as user activity data and user provided data are relatively new and are found in only some countries' data protection laws. Bearing in mind that the PDPO will be a new law for Brunei Darussalam and after much deliberation on the concerns that respondents have raised, AITI proposes that the Data Portability Obligation be excluded from the PDPO at this point in time. In addition, related concepts such as user activity data and user provided data will also be omitted from the Access Obligation. The Responsible Authority shall monitor international developments in this area and, if appropriate, may propose for a suitable Data Portability Obligation to be added to the PDPO at a later date.

5.2 **Right to Withdraw Consent**

5.2.1 In the Public Consultation Paper, AITI proposed for the right to withdraw consent by individuals in respect of the collection, use or disclosure of their personal data for any purpose by an organisation. This right of withdrawal applies to both express consent and deemed consent.

5.2.2 When individuals withdraw their consent, organisations are not allowed to prohibit such withdrawal and are required to inform the individuals of the likely consequences of withdrawing such consent. Further, upon the withdrawal of consent, organisations must cease to collect, use or disclose the personal data for such purposes. Nevertheless, the withdrawal of consent does not affect the legal consequences of withdrawal.

Feedback from Respondents

5.2.3 Several respondents raised concerns that the requirement imposed on organisations to cease collection, use or disclosure of personal data upon the withdrawal of consent may be too difficult to implement in practice. Some respondents cited examples, e.g. in the banking context, where retention of personal data is necessary for the completion of the individuals' contractual obligations. Other examples involved the credit and debit collection context, and situations in which the retention is necessary for the organisation to provide the individual with services.

5.2.4 Respondents also sought clarification as to how the right to withdraw consent may be applied in practice, e.g. whether offering the individual with an option to opt-out or unsubscribe suffice.

5.2.5 Additionally, one respondent suggested that AITI prescribe a timeframe for organisations to cease the use and disclosure of personal data once a request for withdrawal has been made.

Response from AITI

5.2.6 At the outset, in response to the feedback, AITI makes clear that there is no automatic requirement for organisations to delete personal data upon receipt of the individual's request to withdraw consent. Organisations are permitted to retain personal data subject to the Retention Limitation Obligation, i.e. where it is necessary for legal or business purposes. Nevertheless, organisations cannot prevent individuals from withdrawing consent and the withdrawal of consent does not affect the legal consequences of withdrawal. For instance, a contract may need to be terminated as a result of withdrawal of consent. Further, it is highlighted that the right to withdraw consent does not affect use, collection and disclosure of personal data without consent that is permitted under the PDPO or other written laws.

5.2.7 AITI would like to clarify that the option to unsubscribe or opt out may constitute withdrawal of consent for the purposes of this right to withdraw consent.

5.2.8 With regard to the timeframe for organisations to respond or fulfil a withdrawal of consent, AITI intends to provide further guidance at a later stage.

5.3 Right to Request for Access to Personal Data

5.3.1 Under the PDPO, individuals have the right to request for access to 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.

5.3.2 Mandatory exceptions include situations where the information requested could reasonably be expected to threaten the safety or physical or mental health of another individual amongst others. Amongst such exceptions, the PDPO carves out exceptions to their application. Specifically, where the information requested is the user activity data of the individual making the request, even when it could reasonably be expected that acceding to the request would reveal personal data about another individual, or 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, the organisation may choose to accede to the access request.

5.3.3 Organisations may also refuse to disclose information when responding to access requests for specified categories of information such as opinion data solely kept for evaluative purposes and personal data subject to legal privilege. Further, organisations need not respond to particular types of requests, such as requests for trivial information or otherwise frivolous or vexatious requests.

5.3.4 Where an organisation rejects an 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 also notify the individual of the exclusion. If an organisation refuses to accede to a request, it must nevertheless preserve a copy of the personal data for the prescribed period and ensure that it is complete and accurate.

Feedback from Respondents

5.3.5 One respondent suggested that organisations be allowed to charge reasonable fees and that reasonable timelines for organisations to satisfy their obligations be imposed. Another respondent requested for clarification as to the "prescribed time" and "prescribed manner" in which organisations are to notify individuals of the rejection of their access requests.

5.3.6 Additionally, respondents sought clarification as to the scope of data covered under the right. One respondent had a query as to whether the PDPO would provide guidance on what would constitute a request for "trivial information". Another respondent requested for elaboration on the operation of the exception carved out for user activity data of requesting individuals in relation to third-party individuals' personal data with respect to the exceptions to the Access Obligation. Yet another respondent requested AITI to provide examples where rejection of an access request might take place on grounds of national interest.

5.3.7 Several respondents raised questions as to how organisations may go about fulfilling their obligations under this Access Obligation. One respondent asked whether organisations may require access requests made to be in in original or verified written format only. Another respondent has asked whether organisations are permitted to request individuals to provide their purposes for their access request, such as credit applications. A question was also raised as to whether the reasons that organisations give individuals for the rejection of their access requests will need to be based on the prescribed exceptions set out in the PDPO.

5.3.8 Two respondents expressed concern over the impracticability and burdensome nature of providing personal data used or disclosed within a year before the date of the access request. In this regard, one respondent suggested that the provision of such information be subject to the best of the technical and business process capabilities of organisations.

5.3.9 Many respondents also expressed concerns as to the scope of user activity data (which may be very broad, and may include data e.g. metadata, data relating to the

functioning of the services), and suggested for it to be excluded from both the Access Obligation and the Data Portability Obligation.

Response from AITI

5.3.10 First, AITI notes that "user activity data" refers to data generated as a result of user activity. If such personal data is not collected by the organisation, it is not within the scope of user activity data. Unstructured data such as metadata is not collected by the organisation and hence, does not fall within the scope of the Access Obligation. Nevertheless, as mentioned above, these concepts will be omitted from the PDPO at this point in time.

5.3.11 With respect to the fees which may be imposed by organisations, relevant timelines, and manner in which organisations are to notify individuals of the rejection of their access requests, AITI intends to issue further guidance in the relevant regulations and advisory guidelines at a later stage.

5.3.12 AITI notes the feedback from respondents seeking clarification on the scope of personal data covered under the Access Obligation. AITI clarifies that the right to request access generally covers all personal data (subject to any limits on the scope of personal data, as provided in the PDPO and discussed above). Whether a request is made for trivial information or not is left to be determined by the organisations and they would bear the burden of proving that such requests are so.

5.3.13 Organisations are permitted to provide for reasonable verification measures for access requests and may correspond with individuals to find out the purpose of their access request. In addition, when giving their reasons for rejecting access requests, the organisation's reasons will need to be based on the grounds set out in the PDPO.

5.3.14 AITI has contemplated the respondents' concern over the potential burdensome nature of the Access Obligation. Overall, AITI notes that while organisations are required to establish and implement new internal processes to handle requests for access, they would have the option of charging a fee to recover some of the costs (e.g. those directly relating to the request). Further, the PDPO will provide for various situations where organisations are not required to provide access to personal data. As such, AITI intends to maintain its position that the responsibility falls on organisations to enact measures necessary for complying with the Access Obligation (which also includes the preserving of records). The Responsible Authority will issue guidance in the future to assist organisations in developing and implementing processes to comply with the Access Obligation.

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

5.4.1 Under the PDPO, individuals have the right to request an organisation to correct an error or omission in his or her personal data insofar as the personal data is in the organisation's possession or under its control. The organisation is bound to do so as soon as it is practicable unless it is satisfied on reasonable grounds that a correction should not be made.

5.4.2 Organisations shall 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.

Feedback from Respondents

5.4.3 Multiple respondents asked whether there was a need to send corrected personal data to other organisations to which the personal data was disclosed to, and to notify individuals of correction. One respondent raised the question of whether correction of errors or omission of data that occurred not due the fault of the organisation will also need to be sent to other such organisations. Another respondent asked whether organisations may make a reasonable assessment as to whether another organisation (to which the personal data was disclosed to) requires the corrected data for business purposes.

5.4.4 One respondent suggested that the data subjects should be responsible for communicating corrected data to third parties instead of organisations because it would be fairly onerous to the latter. Another respondent sought clarification regarding the definition of "derived personal data" and how it is distinct from "user activity data".

Response from AITI

5.4.5 At the outset, AITI would like to clarify that organisations are to notify requesting individuals on whether their correction request was acceded to. The obligation to notify other organisations to which the personal data was disclosed to is not a fault-based obligation. Nevertheless, it only extends to requests by individuals for the correction of their personal data. Where appropriate, organisations may wish to put in place mechanisms for individuals to correct their personal data by themselves. In ascertaining whether another organisation requires the corrected data for business purposes, organisations are allowed to make such an assessment.

5.4.6 In relation to the respondents' concern over the onerous nature of the obligation on organisations to communicate the corrected data to third parties, AITI maintains its view that it would be easier for organisations to send corrected data to the third parties rather than leaving this up to the individual. If the responsibility falls to the individual, the organisation would need to provide a list of the names and addresses of all the other third-party organisations that will need to receive the corrected personal data. Further, such third parties may not have a direct relationship with the individual and subjecting them to the Access and Correction Obligations would result in a significant compliance burden and potentially affect their relationship with the first organisation (e.g. if the third party is a subcontractor of the first organisation). On balance, AITI believes that the organisation which received the correction request would be best placed to communicate the corrected data to the third parties and address any issues that may arise.

5.5 Right to Data Portability

5.5.1 In this Public Consultation Paper, AITI proposed for the introduction of the right to data portability in the PDPO. The right to data portability would require 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

obligation will only apply to "applicable data" as defined under the PDPO. The general purpose of this relatively new right is to give individuals greater agency and control over their personal data.

5.5.2 Many respondents raised concerns relating to the right to data portability, specifically the regulatory burden placed on organisations, and the lack of clarity concerning the scope of "applicable data".

5.5.3 Given the foregoing and the fact that data portability is a relatively new concept in many data protection laws worldwide, AITI will be excluding the right to data portability from the PDPO at this juncture. Nonetheless, AITI will be monitoring the situation and consider whether to introduce the right to data portability into the PDPO in the future.

6. Investigations, Enforcement and Appeal

6.1 Data Protection Appeal Panel

6.1.1 Two respondents provided feedback regarding the Data Protection Appeal Panel ("**DPAP**"). One suggested that DPAP should comprise of respectable independent personalities and that DPAP should publish its list of panels in excess of 3 to be readily available to hear appeals. Another respondent sought clarification as to the composition of DPAP and suggested that it should include representatives from the private sector. In this regard, AITI notes the suggestions from the respondents and will take them into consideration.

6.2 Powers of Investigation

6.2.1 In the Public Consultation Paper, AITI proposed that the Responsible Authority may, upon complaint or on its own motion, conduct an investigation to determine whether an organisation or person is complying with the PDPO. The Responsible Authority's range of powers of investigation include, amongst others: requiring, by written notice, an organisation to produce any specified document or specified information; by giving at least two (2) working days' advance notice of intended entry, entering into an organisations' premises without a warrant; and obtaining a search warrant to enter an organisation's premises and taking possession of, or removing, any document.

Feedback from Respondents

6.2.2 One respondent sought to clarify whether the details of officers intending to enter into the premises of an organisation would be provided.

6.2.3 Another respondent suggested that the taking possession of or removal of documents be limited to specific categories of documents, specifically, documents which are directly related to the particular investigation, and documents which are not subject to rules of confidentiality or legal privilege.

Response from AITI

6.2.4 In response to the query, AITI clarifies that there is no legal requirement to disclose the identity of officers insofar as they are able to be identifiable as officers belonging to the Responsible Authority.

6.2.5 With regard to the suggestion that limitations be imposed on the categories of documents which the Responsible Authority may take possession of or remove under its powers of investigation, in general, the PDPO does not affect the operation of other laws, including in relation to the confidentiality of documents or operation of legal privilege. Nevertheless, AITI will take the comments into consideration and consider the scope of such powers.

6.3 **Power to Issue Directions**

6.3.1 The Responsible Authority will also be given powers to issue directions to organisations which have contravened the PDPO, for example, to delete or destroy personal data collected in contravention of the PDPO. In the event an organisation has intentionally or negligently contravened the Data Protection Provisions, the Responsible Authority may also issue a direction requiring payment of a financial penalty which must not exceed the maximum prescribed, which in no case may be more than the following:

(a) in the case of a contravention by an organisation whose annual turnover in Brunei Darussalam exceeds BND10 million – 10% of the annual turnover of the organisation in Brunei Darussalam;

(b) in any other case – BND1 million.

6.3.2 In deciding the quantum of financial penalty imposed on offending organisations, the Responsible Authority will be guided by the degree of harm caused by the breach, the seriousness of the violation and other factors.

Feedback from Respondents

6.3.3 One respondent commented that rather than pegging the quantum of financial penalties to the organisation's annual turnover, an alternative approach would be ensuring that the quantum is proportionate to the harm caused to the affected individuals and whether there was any aggravating or mitigating factors. The reason for this arises from the concern that civil penalties would impose undue hardships on the responsible entity.

6.3.4 Another respondent commented that a direction for the destruction of personal data collected in contravention of PDPO would lead to deactivation of person's active subscriptions.

AITI's response

6.3.5 AITI clarifies that the limit to financial penalties provided in the PDPO only represents the *maximum* quantum that may be imposed by the Responsible Authority. When a

financial penalty is imposed, relevant factors such as the harm caused, and other aggravating and mitigating factors would be taken into account.

6.3.6 AITI notes that a direction to destroy personal data may be issued if the personal data had been collected in contravention of the PDPO. Further, organisations will be prohibited from requiring an individual to consent to the collection, use and/or disclosure of his or her personal data beyond what is reasonable to provide a service to the individual. In such circumstances, destruction of personal data collected in contravention of the PDPO should not lead to consequences such as termination of services or subscriptions which an individual wishes to obtain.

6.4 **Right of Private Action**

6.4.1 The PDPO seeks to provide 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 commence a private civil action in court. However, if the Responsible Authority has made a decision under the PDPO in respect of a contravention, 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.

Feedback from Respondents

6.4.2 Two respondents expressed doubts over the need for a right of private action. A respondent stated that it does not appear that such a right would be necessary given that the PDPO already provides for the setting up of Responsible Authority to administer and enforce the PDPO and the establishment of DPAP. Therefore, in the interests of ensuring consistency and finality of decisions made by the Responsible Authority and DPAP, the right of private action should not be included. The other respondent raised concerns over risks of unnecessary litigation and significant costs imposed on businesses. The right of private action should be an instrument of last resort.

6.4.3 On the other hand, a different respondent expressed the view that the right of private action should not be conditioned upon the exhaustion of all avenues of appeal in the interests of justice. AITI also received feedback to clarify whether organisations have a right of private action.

AITI's response

6.4.4 AITI clarifies that the Responsible Authority does not have the power to require an organisation to pay compensation to an individual who has suffered a loss or harm as a result of the organisation's contravention of the PDPO. As it is not proposed that the Responsible Authority take on such a function, the right of private action would enable individuals to seek an appropriate remedy before the courts. Such a remedy would be in addition to any directions or penalties which may be imposed on an organisation by the Responsible Authority. Whether organisations would have a right of private action would be left for the courts to determine based on the facts of the case.

7. Offences Affecting Personal Data and Anonymised Information

7.1 Query on Defences to Offences under the PDPO

7.1.1 In the Public Consultation Paper, AITI proposed that the PDPO would contain three main offences: (a) the knowing or reckless unauthorised disclosure of personal data, (b) improper use of personal data, and (c) the knowing or reckless unauthorised re-identification of anonymised data. For all three offences, the penalty will be a fine not exceeding B$10,000 or imprisonment for a term not exceeding 2 years, or both.

7.1.2 As a counterbalance, the PDPO provides for defences to these three offences. These include the defence that 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), and where the conduct is permitted or required under other laws. Notwithstanding the above, organisations are ultimately responsible for complying with the PDPO and are liable for the actions of its employees.

Feedback from Respondents

7.1.3 Several respondents sought clarification regarding the defences. A respondent asked if the defences applied to organisations or were limited to individuals. Two other respondents asked if organisations are entitled to rely on the three main offences as a defence against employees or agents.

Response from AITI

7.1.4 In consideration of the queries and feedback, AITI clarifies that whether an offence may be committed by an organisation, and also whether an organisation may avail itself of a defence provided in the PDPO, depends on the application of general criminal law. Based on the scope of the three main offences, they are likely to apply mainly to individuals.

7.1.5 Notwithstanding the foregoing, an organisation is responsible for complying with the PDPO's Data Protection Provisions. If an organisation does not have reasonable security arrangements put in place and thereby contravenes the PDPO, even if its employees are found to have committed an offence under the PDPO or another law, the organisation may be separately liable for its contravention of the PDPO.

7.2 Feedback on Exclusion of Personal and Criminal Liability

Feedback from Respondents

7.2.1 Some respondents provided feedback that the personal and criminal liability for breaches of the PDPO should be excluded from the PDPO. In this regard, civil enforcement of personal data protection laws should adhere to international standards and requirements such as the APEC Privacy Framework.

Response from AITI

7.2.2 In response, AITI clarifies that the offences under the PDPO do not relate to contravention of the PDPO's Data Protection Provisions and that employees are excluded from the requirement to comply with such provisions (when acting in the course of their employment). Some of the offences in the PDPO relate to situations where an employee has, in some manner, misused personal data in the possession or under the control of an organisation. Other offences relate to situations involving administration of the PDPO, such as if an employee provides false information to the Responsible Authority in the course of an investigation by the Responsible Authority. Nevertheless, AITI notes the and shall consider the feedback raised.

8. Do Not Call ("DNC") Regime

8.1 General Feedback

8.1.1 In the Public Consultation Paper, it was proposed that a DNC regime be introduced into Brunei Darussalam. Under the proposed DNC regime, which is to be administered by the Responsible Authority, individuals who do not wish to receive telemarketing messages via phone call, text message or fax may request for their telephone numbers to be added to the DNC Registry. The registration of telephone numbers will be free-of-charge.

Feedback from Respondents

8.1.2 A number of respondents raised concerns over the scope and definition of "telemarketing". Several respondents also expressed concern over the high establishment costs of a DNC Register and business compliance costs with the DNC regime. One respondent raised the issue that there may be confusion amongst customers seeking to only receive certain marketing materials.

8.1.3 One respondent suggested that instead of on opt-in regime, all individuals in Brunei Darussalam be added to the DNC Register by default, unless an exception or exclusion applies or individuals have given express consent directly to the sender that they may receive unsolicited marketing communications. Another respondent suggested that senders should be registered with AITI before they are able to apply to check the DNC Register.

Response from AITI

8.1.4 Having considered the concerns, views and suggestions regarding the operation of the DNC regime and its associated costs, AITI has decided to exclude the DNC provisions from the PDPO. In this regard, organisations would still be required to obtain individuals' express consent before collecting or using their personal data for the purpose of sending a telemarketing message and individuals may withdraw any such consent they have given (or be deemed to have given) under the PDPO. While having a DNC regime may provide some benefits to individuals who do not wish to receive such messages, AITI notes that other individuals may wish to receive such messages. Further there would be additional costs imposed on organisations that wish to use telemarketing as a means of advertising or promoting their goods and/or services.

8.1.5 The Responsible Authority may review this area in future and may propose a suitable regime to be implemented, whether as part of the PDPO or another legislation which addresses marketing by electronic means (telephone, email, etc.).

8.2 Prohibition Against Dictionary Attacks and Address-Harvesting Software

8.2.1 The PDPO provides that 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 is subject to a defence for employees acting in good faith who does so in the course of their employment or in accordance with instructions given to them in the course of their employment.

Feedback from Respondents

8.2.2 Two respondents sought clarification regarding the definition of dictionary attacks or address-harvesting.

Response from AITI

8.2.3 As this provision would have operated in conjunction with the provisions relating to the DNC Regime, they will be removed from the PDPO. The Responsible Authority may review this area in future, if appropriate, and may include such provisions as part of the PDPO or another legislation which addresses marketing by electronic means (telephone, email, etc.).

9. Regulations, Codes of Practice and Advisory Guidelines

9.1 Query on Stakeholder Consultations for Regulations

9.1.1 Generally, the Responsible Authority shall be empowered 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.

Feedback from Respondents

9.1.2 One respondent queried whether stakeholder consultations for regulations issued under the PDPO would be held.

Response from AITI

9.1.3 AITI may conduct stakeholder consultations, however this would depend on the type of regulations developed.

10. Interaction Between the PDPO and Other Laws

10.1 Query on Sectoral Regulations

10.1.1 In the Public Consultation Paper, AITI proposed that the PDPO operate as a baseline law for data protection that would run concurrently with other sectoral legislative and regulatory frameworks. Where there are inconsistent provisions with other written

laws, the provisions under those written laws will supersede the provisions of the PDPO. Sectoral regulators may also exempt their licensees from specific requirements under the PDPO where required.

Feedback from Respondents

10.1.2 A respondent expressed its general support for the PDPO operating as a baseline law for data protection whilst leaving room for sectoral regulators to impose higher levels of protection where appropriate. On the other hand, another respondent was not in favour of the approach proposed in the Public Consultation Paper, instead calling for the data protection obligations to be standardised across various regulatory bodies. As a point of clarification, one respondent queried as to whether exemptions would be sector-specific.

Response from AITI

10.1.3 Having considered the feedback received on the interaction between the PDPO and other laws, AITI maintains its position that the PDPO ought to operate as the baseline data protection laws, while sectoral regulators are given the flexibility to stipulate higher levels of protection for the industry that it regulates. This would be a more balanced approach which recognises that different industries and sectors may have their own specific needs and circumstances. AITI also does not intend to change its approach with regard to how inconsistencies between the provisions of the PDPO and other written laws should be resolved (i.e. with the provisions of other written laws taking precedence).

11. Sunrise Period of Two (2) Years

11.1 Query on length of sunrise period

11.1.1 In the Public Consultation Paper, AITI proposed that there be a "sunrise period" of two (2) years from the time the PDPO is enacted to allow organisations time to secure compliance. During this sunrise period, AITI or the Responsible Authority, intends to conduct outreach and awareness-building programmes for the wider public as well as actively engage various industries and associations on data protection issues. The ultimate objective to help businesses familiarise themselves with their obligations under the PDPO and prepare for compliance once the PDPO takes effect.

Feedback from Respondents

11.1.2 Two respondents expressed concerns that a sunrise period of two (2) years may be insufficient as organisations would require time to understand their obligations under the PDPO and effect changes (e.g. organisation may need to review their processes and invest or upgrade their customer management systems to ensure compliance).

Response from AITI

11.1.3 In view of this feedback, AITI will take such concerns into consideration and will monitor the matter and consider whether the sunrise period of two (2) years should be extended.

12. Existing Personal Data / Grandfathering Clause

12.1 Query on Application of Grandfathering Clause

12.1.1 The PDPO will contain a grandfathering clause which provides that organisations may continue to use personal data that was collected before the commencement date of the PDPO for the purposes for which the personal data had been collected. However, organisations must cease to use such data if the individual concerned withdraws consent for such a use of his or her personal data. This grandfathering clause only applies to an organisation's use of existing personal data, and not the collection of further personal data or disclosure of personal data that had already been collected.

Feedback from Respondents

12.1.2 One respondent expressed support for the introduction of the grandfathering clause in the PDPO. Many respondents had questions on the operation of the grandfathering clause. One respondent asked whether in the circumstance where a customer takes up a new insurance policy after commencement, would his previous policies or personal data collected be covered under the grandfathering clause. Another respondent sought clarification as to how organisations are expected to evidence the purposes for which the personal data was previously collected. Two respondents asked when the grandfathering clause would become effective.

Response from AITI

12.1.3 AITI notes that the purposes for which personal data had been collected prior to the commencement of the PDPO might not have been communicated to the individuals concerned. Where the organisation is able to demonstrate that the previously-collected personal data was used for such purposes, for example, in providing services to an individual, it may rely on the grandfathering clause and continue to use the personal data for that purpose.

12.1.4 Where an organisation is in a longer-term relationship with the individual (for example, under an existing insurance policy or contract), the organisation would nonetheless have to establish policies covering the purposes for the processing of personal data in order to comply with the PDPO (specifically, the Accountability Obligation). Notification of purposes and obtaining consent would be required for any new collection of personal data after the commencement data of the PDPO. For personal data already collected under existing policies / contracts, it would nonetheless be good practice to give individuals notice of the purposes of such use of their personal data. In the event of any changes to the purposes of use after the PDPO comes into force, the organisation would be required to obtain consent for any new purposes.

12.1.5 In view of this responses and feedback, AITI intends to provide guidance on the operation of the grandfathering clause in due course.

13. General / Miscellaneous Comments

13.1 Query on Financial Penalties

13.1.1 Several respondents also raised specific questions which broadly touched on the data protection issues discussed in the Public Consultation Paper. One respondent sought clarification on whether AITI would be introducing a penalty scale for different types of offences, specifically, whether the Responsible Authority would classify data breaches into categories of minor, medium, and major breaches, and whether financial penalties would be reduced if the offending organisation had implemented control measures.

Response from AITI

13.1.2 In response to this feedback, AITI clarifies that the general approach to the decision to impose financial penalties on organisations for the non-compliance of the PDPO is that the penalties would generally be commensurate with the severity of the offence and would take into account relevant aggravating and mitigating factors. AITI may provide further guidance on the enforcement of the PDPO and imposition of financial penalties at a later stage.

13.2 Query on Representation for Vulnerable Individuals

13.2.1 Another respondent suggested that AITI should provide for a class of individuals who may represent vulnerable individuals so that the former may exercise their rights under the PDPO.

Response from AITI

13.2.2 With respect to a class of representatives for vulnerable individuals, AITI takes the position that it is generally for other laws to determine who may legally act for vulnerable individuals in relation to exercising their rights under the PDPO.

13.3 Query on Data Custodians

13.3.1 Finally, there were several issues that respondents raised in their feedback that did not neatly fall within any of the above categories of topics and were not expressly dealt with in the PDPO. Examples of these issues included the concepts of data custodianship and ownership. As a general rule, with respect to the issues that respondents raised which were not specifically dealt with in the PDPO, AITI may take them on board for further study in due course.

13.3.2 One respondent asked whether the Data Protection Obligations under the PDPO would cover personal data that is transferred from companies to data custodians. This arises in situations where personal data is exchanged between companies by virtue of their business or for the purpose of supporting certain business functions such as Human Resources departments sending staff salary particulars to banks or financial institutions for processing.

Response from AITI

13.3.3 In general, the PDPO will apply to situations where personal data is transferred from organisations to data custodians unless an exception applies. One issue that may arise is whether the data custodian is a DP that would be subject to fewer Data Protection Obligations under the PDPO. Otherwise, both the organisation and data custodian would be required to comply with the full suite of Data Protection Obligations under the PDPO.

[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

PART 3: CONCLUSION

14. Concluding Remarks

14.1 AITI intends to issue advisory guidelines and other resources which will assist organisations in their compliance with the PDPO once the law is introduced.

14.2 AITI thanks all respondents for their comments, proposed suggestions and feedback to the Public Consultation Paper.

[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

ANNEX A

List of Respondents

1. Amazon Web Services
2. Brunei Insurance and Takaful Association
3. Brunei Association of Banks
    a. Baiduri Bank Berhad
    b. Bank Islam Brunei Darussalam
    c. Bank of China (Hong Kong)
    d. Maybank
    e. Standard Chartered Bank
    f. United Overseas Bank
    g. Perbadanan Tabung Amanah Islam Brunei
4. Brunei Shell Petroleum Co Sdn Bhd
5. Datastream Digital Sdn Bhd
6. Great Eastern Life
7. IBM World Trade Corporation
8. Imagine Sdn Bhd
9. LBC Mabuhay Remittance Sdn Bhd
10. Progresif Sdn Bhd
11. Royal Brunei Airlines Sdn Bhd
12. Unified National Networks Sdn Bhd
13. US-ASEAN Business Council

[END OF DOCUMENT]