DETAILED RESPONSE TO PUBLIC CONSULTATION DOCUMENT

1. **The Transfer Limitation Obligation: Cross-border data transfers should be explicitly permitted, and the Transfer Limitation Obligation should not apply to data intermediaries/processors**

a. **The Transfer Limitation Obligation should facilitate cross-border data flows by explicitly permitting the transfer of data** where the data controller takes reasonable steps to ensure that personal data transferred overseas continues to be protected to a comparable standard to that which would apply in Brunei Darussalam.

Additionally, we recommend that the draft Personal Data Protection Order (PDPO) should set out a non-exhaustive, but clear, list of measures that an entity can take to demonstrate that it has taken such reasonable steps, such as where: (1) the data controller assesses that the recipient is bound by comparable data protection obligations under applicable laws in the destination jurisdiction; (2) the recipient is bound by binding corporate rules; (3) the data controller enters into contractual terms imposing data protection obligations on the recipient that are appropriate for the nature of the relationship between the parties and the data involved; (4) the recipient has established systems and processes that comply to internationally recognized standards, such as requisite ISO certifications (e.g. ISO 27001 and ISO 270018); or (5) or express consent has been obtained from the data subject for the transfer.

b. **The Transfer Limitation Obligation should not apply to data intermediaries/processors**. Data intermediaries/processors merely act on behalf of data controllers, and their primary responsibility is to follow data controllers' lawful directions. Data Intermediaries/processors, and cloud service providers (CSP) in particular, typically do not have visibility into the data they are processing and therefore typically will not be able to distinguish whether the data they are processing even includes personal data at all. Therefore, it should ultimately be the data controller's responsibility to determine whether to transfer personal data offshore, to which destinations it is appropriate to transfer that personal data, and what appropriate protection measures should be implemented when transferring personal data offshore.

The requirement set out in the draft PDPO that the Transfer Limitation Obligation should apply to data intermediaries/processors is inconsistent with other international personal data protection frameworks, including Singapore's Personal Data Protection Act (PDPA). For example, Singapore's Personal Data Protection Commission has clarified that where an organization (data controller) engages a data intermediary to process personal data on its behalf and for its purposes, the organization is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organization to an overseas data intermediary or is transferred overseas by a data intermediary in Singapore as part of its processing on behalf and for the purposes of the organization. Furthermore, Singapore's PDPA's Transfer Limitation Obligation requires the organization to ensure that personal data transferred overseas is protected to a standard comparable to that under the PDPA. The onus is on the transferring organization to undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure that the intermediary can provide a comparable level of protection. In undertaking its due diligence, transferring organizations may rely on data intermediaries' extant protection policies and practices, including their relevant industry standards or certification.

- **Recommendation:** We therefore recommend that Section 4.13 of the PDPO, which sets out the obligations for the Transfer Limitation Obligation, should be amended to: (a) explicitly permit the transfer of personal data where transferred personal data is protected to a comparable standard; (b) provide a list of clear but non-exhaustive transfer measures that can demonstrate that such transfers are made to a comparable standard; and (c) is amended so that it does not apply to data intermediaries/processors.

2. **Further clarification should be provided on how the Retention Limitation Obligation (Section 4.12) should apply to data intermediaries/processors.**

The PDPO should make clear that in circumstances where a data processor/intermediary (for example, a CSP) could not reasonably know: (1) the purpose for which personal data is processed; and/or (2) whether the personal data is still necessary for that purpose, then the data controller should remain primarily responsible for the Retention Limitation Obligation. This is because the data intermediary/processor ordinarily would not know the purpose for which the data was collected, and whether it is necessary to retain the data for that purpose. Only the organization (or data controller) can determine this.

Therefore, a data intermediary/processor should primarily be held responsible for complying with the lawful instructions of a data controller and should only be subject to the Retention Limitation Obligation insofar as a data intermediary/processor is required to securely delete personal data processed for a data controller once the data intermediary/processor's relationship with the data controller ends.

- **Recommendation:** For the reasons stated above, we recommend that Section 4.12 of the PDPO be amended to clarify that data intermediaries/processors should only be subject to the Retention Limitation Obligation in relation to their responsibility to securely delete personal data processed for a data controller once the data intermediary/processor's relationship with the data controller ends.

3. **The Data Breach Notification (DBN) Obligation should not apply to data processors/intermediaries but should more clearly define when the DBN is triggered.**

AWS recognizes that the DBN obligation will strengthen protection of individuals and accountability of organizations for the personal data in their care. We note that Section 4.14.4 of the PDPO states that the Responsible Authority will take a risk-based approach and impose a threshold for notification. To achieve this, we recommend that the law provides further clarity on the materiality threshold for triggering the DBN obligation. The consultation document suggests that data processors will need to notify the Responsible Authority of personal data breaches, but this is inconsistent with the DBN regimes elsewhere in the world. Other frameworks such as the European Union (EU)'s General Data Protection Regulation (GDPR), Singapore's PDPA, and Australia's Privacy Act uniformly place the obligation on the data controller to notify the regulator and individuals of any personal data breaches. We recommend **that only data controllers are required to notify the Responsible Authority or individuals of a "notifiable data breach."** Our specific responses below on both these issues are below:

- **Recommendation: Revise Section 4.14 of the PDPO to make clear that data intermediaries are not required to notify the Commission or individuals of a "notifiable data breach."** Instead, the data controller should remain responsible for assessing whether a personal data breach constitutes a "notifiable data breach" and notify the Responsible Authority and/or individuals, as the case may be. This is because data intermediaries/processors may not have visibility over the content of data controllers. This means that such processors would not be able to distinguish between an intentional movement of data or a security incident, let alone whether a data breach involves personal data. Finally, data intermediaries/processors do not have direct relationships with the data subject and would therefore not be able to meaningfully or effectively communicate matters relating to a personal data breach with them. Instead, data intermediaries/processors should instead have the responsibility to notify controllers of confirmed data breaches, in a reasonable timeframe, given the specific circumstances, and in accordance with their contractual agreements. Therefore, we recommend that the Section 3.7.1(d) of the PDPO should be deleted in order to remove the DBN obligation from the list of obligations applicable to data processors/intermediaries.

- **Recommendation: Revise the definition of "data breach" to link it clearly to when a security incident has actually occurred.** Under the current formulation of the definition of a "data breach", the requirement to notify the Responsible Authority of a data breach is not tied to a security incident. Rather, the phrases "likely to result" and "likely to be" in limbs (a) and (b) of the obligation could be interpreted to capture *potential* data breaches which have not transpired. This is inconsistent with other DBN regimes such as the EU GDPR, which defines a

personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Linking a data breach to a security incident means that organizations can create effective mechanisms to constantly monitor threats, detect security failures, and trigger investigations. By requiring organizations, to notify the Responsible Authority of potential data incidents, the current formulation will likely require organizations to divert resources away from investigating an incident and curtailing its impact while also potentially leading to over-notification, causing "notification fatigue." This issue is addressed in the GDPR definition, which captures only actual unauthorized or unlawful processing. We recommend that the definition of "data breach" should be revised to be more consistent with international practices. AITI could also consider further clarifying organizations' obligations by adopting the EU GDPR definition.

- **Recommendation: Incorporate a "materiality" standard of "significant harm" before a DBN is required under Section 4.14.1 of the PDPO and exempt notification when the risk of harm has been effectively mitigated.** We recommend that the threshold for notifying data subjects and/or data protection authorities should be tied to unauthorized disclosure of, or access to, personal data that may cause material risk of harm (e.g., a material risk of identity theft or economic loss to the data subjects). Providing more clarity around "a risk-based approach" by incorporating a "materiality" standard is necessary, as it will ensure that notifications, made to regulators or data subjects only pertain to breaches that require their greatest attention and expedient mitigation. Without such a threshold, numerous immaterial notices will be issued resulting in "notification fatigue." This would in turn lead to inconvenience for data subjects, increase in administrative costs and burden for the regulator, and most importantly result in a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm.

  Additionally, the GDPR and other DBN regimes around the world recognize that there should be reasonable exceptions where a notification obligation would not be triggered by a personal data breach, because the risk of harm has been effectively mitigated. We recommend that the PDPO also includes such exceptions. Article 34 of the GDPR also recognizes that notification to individuals should not be required if organizations have taken subsequent measures to address the risk.

  Therefore, a "materiality" standard is necessary to ensure that regulators or data subjects are notified of breaches that require their greatest attention and expedient mitigation. Additionally, the PDPO should also explicitly exempt the obligation to notify the data subject and/or the data protection authority in scenarios where the risk of harm arising from a personal data breach has been effectively mitigated.

  We also recommend that reporting the breach should only occur after the organization has had a reasonable period of time to investigate and confirm a breach.

- **Recommendation: Clarify the requirement for organizations to notify affected individuals "on or after notifying the Responsible Authority."** We recommend that the requirements should be amended to state that the "organization is required to notify affected individuals **without undue delay** after notifying the Responsible Authority."

4. **<u>The Access and Portability Rights: Access and Portability Rights should be streamlined and should exclude user-activity data.</u>**

In general, the right to access personal data is an important consumer right as it plays a central role in enabling individuals to exercise further rights, such as correction and portability. The information covered by the right to access could include the personal data collected itself, information about the processing purposes, and the way in which the data may be disclosed.

The PDPO recognizes that there may be circumstances under which a data controller can "reject" a data access request of an individual. In other jurisdictions such as Singapore, the data protection authorities have clarified that "(Organizations) are not required to provide access if the burden or expense of providing access would be unreasonable to the organization or disproportionate to the individual's interest or if the request is otherwise frivolous or vexatious."[1]

In order for Brunei to balance (1) the need to allow individuals to exercise their right to access data effectively and (2) the costs to companies of complying with over-broad or frivolous access requests, we recommend that the right to access should be clearly scoped and should not extend to cover vague categories of data, such as user-activity data. User activity data could include extremely broad categories of data and metadata, including information related to the functioning of services, data about an individual's interaction with e-services, among others. Many of these types of data would not be meaningful or valuable to individuals with regard to exercise of further rights. However, if individuals requested such data, such requests would be very costly for data controllers to collate and provide as they would cover very broad data sets, including all user-activity data related to transactions made with the organization.

Additionally, as user-activity data is often unstructured data, there could be significant privacy risks to other individuals whose data may incidentally be reflected in that "user-activity" data. We therefore recommend that user-activity data should excluded from the Access Obligation.

Furthermore, user-activity data could be generated from the use of proprietary tools or features. Therefore, requiring organizations to release this data to individuals could present risks for confidentiality of commercially-sensitive information or trade secrets. Such requirements could, in turn, chill innovation and render Brunei a less attractive location for data processing if a data access request could inevitably result in a disclosure of commercially sensitive information.

If Brunei intends to continue including "user-activity" data in the data access requirements, we recommend that the following categories of data should be excluded:

(a) data that provide no clear value to individuals' ability to switch providers, and/or take time for organizations to process, including (1) user activity data generated from the use of proprietary tools or features, (2) user-generated content (such as voice recordings, videos, images, customer reviews and feedback), and (3) unstructured data;

(b) data that identifies another individual, unless the other individual has provided their consent for the data to be shared for such purpose.

[1] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en

Separately, Section 5.6 of the PDPO repeatedly uses the term "applicable data" without clearly defining this term. We recommend that the PDPO should provide a clear definition of "applicable data," and that for the reasons articulated above, this definition should exclude "user activity."

Section 5.6.7 of the PDPO also states that a porting organization can disclose personal data about a third-party individual (T) to a receiving organization without T's consent if the data porting request is made in an individual's (P) personal or domestic capacity and relates to P's user activity data or user-provided data.

It is extremely onerous for the porting organization to review applicable data to determine whether transmitting applicable data about an individual (P) would transmit personal data about another individual (T), and if so, whether the data porting request is made in P's personal or domestic capacity. It is also not clear why there is a separate concept of "user activity data or "user-provided data" to qualify this request.

Instead, we propose that a porting organization may disclose personal data about T to a receiving organization without T's consent only if the data porting request from P satisfies any requirements prescribed. The proposed changes require porting organizations to only verify that the data porting request from P satisfies prescribed requirements. The prescribed requirements for the data porting request can include statements that the request is being made in P's personal or domestic capacity.

5. **Definition of Personal Data: Anonymized data should be explicitly excluded from the scope of the PDPO.**

We generally support the proposed definition of "personal data." However, for clarity, we recommend that personal data that has been anonymized, such that a data subject cannot be re-identified from that data, should be explicitly excluded from the scope of "personal data" so that it does not fall within the scope of data protection legislation.

6. **Exceptions from the Scope of Application: Data processors acting on behalf of public agencies should also be excluded from the scope of the PDPO.**

Section 3.5.1 of the PDPO specifically excludes public agencies, even as data controllers. If public agencies as data controllers are not subject to the PDPO, then data processers acting on behalf of such public agencies should also should not be not subject to the PDPO is because data processors do not have the same relationship with data subjects as data controller have. Data intermediaries/processors are therefore not typically in a position to make meaningful or independent decisions about the processing of personal data – rather, they implement decisions of the public agencies which are the data controllers. It is therefore inappropriate for processors to be held accountable to data subjects.

7. **Territorial scope should extend only to data processors established within Brunei Darussalam**

Section 3.6 of the PDPO provides that PDPO applies to all private sector organizations that process personal data in Brunei Darussalam, regardless of whether they are formed or recognized under Brunei law or whether they are resident or have an office or place of business in Brunei Darussalam i.e. that the PDPO is extra-territorial.

Data protection laws should not be extra-territorial, as enforceability on foreign organizations will be challenging. In addition to enforceability challenges, extra-territorial privacy laws could create conflicting and overlapping data protection obligations that could make compliance both overly complicated and costly for these foreign organizations and would ultimately detract from privacy laws' aim of protecting personal data.

We recommend that the PDPO should only apply to data processing where: (1) the data subject is a resident of Brunei Darussalam when his/her/its personal data is processed (including when the data is collected, used, or disclosed); and (2) the data controller and/or entity processing the personal data is established within Brunei Darussalam. We suggest 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 on Brunei Darussalam are not subjected to conflicting laws.