Annex: Recommendations and Inputs on the Public Consultation Paper
(Paragraph references below are to those in the Consultation Paper)

1. **Paragraph 3.1, 3.4.6-7, 3.4.8 re. Definitions of Personal Data.**

    - We recommend that anonymized personal data where a data subject cannot be re-identified should be explicitly excluded from the scope of the term "personal data" and clearly excluded from data protection legislation.

2. **Paragraph 3.2 re. Categories of Personal Data.**

    - US-ABC broadly supports the approach of not carving out a separate category for "sensitive personal data" to allow for flexibility in implementing data protection measures that are appropriate for different circumstances.

    - However, should there be types of data that the Government of Brunei Darussalam is likely to recognize as "sensitive personal data" regardless of sector (e.g., an individual's national identification number) and for which additional obligations would apply, we encourage AITI to expressly clarify within the proposed PDPO or advisory guidelines what constitutes 'sensitive personal data' and what those additional obligations are. Otherwise, we support the flexible nature of this obligation and note that there are no prescriptive security standards and/or measures imposed for any specific types of data. We support that organizations themselves are empowered to decide the nature of security measures based on the circumstances.

3. **Paragraph 3.5.1 re. Exclusion of the Public Sector.**

    - This paragraph specifically excludes public agencies from the PDPO, even as data controllers. Since public agencies as data controllers are not subject to the PDPO, data processors acting on behalf of public agencies should also be excluded from the scope of the PDPO. This is because data processors do not have the same relationship with data subjects as data controllers do and typically are unable to make meaningful or independent decisions about the processing of personal data on behalf of such public agencies, as their focus is on implementing decisions of the public agencies, acting as the data controllers.

4. **Section 3.7.1 re. Written Agreements between Data Controllers and Data Intermediaries/Processors.**

    - US-ABC is supportive of AITI's distinction between data controllers and data intermediaries/processors and attendant obligations. We also note that data processors are subject to a reduced set of obligations under the PDPO provided they have a written processing agreement in place.

    - However, we are concerned about smaller enterprises who may not have put in place good business practices such as documented agreements with their data processors. Such a requirement may result in data processors being unfairly penalized and subject to a broader range of obligations and cost of compliance. Whether a data processing arrangement exists between companies should be a matter of substance in its content, rather than any particular form.

    - Therefore, we recommend that AITI extend the set of reduced obligations to data processors without needing a written agreement in place, while simultaneously promoting the wider adoption of good business practices and ASEAN Model Contractual Clauses to small and medium-sized enterprises as these companies require more time and support to move towards compliance.

5. **Paragraph 4.11 re. The Protection Obligation.**

    - We support the flexible nature of this obligation and note that there are no prescriptive security standards and/or measures imposed. Organizations should be empowered to decide the nature of

security measures appropriate to them and the data processing in question based on the given circumstances.

6. Paragraph 4.12 re. The Retention Limitation Obligation.

- As mentioned above, data intermediaries/processors act on behalf of data controllers, and their primary responsibility is to follow their lawful directions, generally without having visibility over whether the data they are processing includes personal data. They are therefore unable to meaningfully assess whether the personal data they are processing is no longer necessary for legal or business purposes. Only the organization (or data controller) can determine this. If data intermediaries are responsible for assessing and implementing the data retention obligation, there is a much higher risk that they would make inaccurate decisions about whether to retain or delete data because they do not have insight into the purpose for collecting the personal data and the reasonable uses for which it could be used by the organization in the future.

- We therefore recommend that paragraph 3.7 on the obligations that apply to data intermediaries/processors does not include the Retention Limitation Obligation, as they cannot meaningfully comply with this obligation.

7. Paragraph 4.13 re. The Transfer Limitation Obligation and Extra-Territorial Scope

- US-ABC is of the opinion that this obligation be positioned more positively to support cross-border data flows by explicitly stating that transfer of data is permitted where the data controller takes reasonable steps to ensure that personal data transferred overseas continues to be protected to a comparable standard, as it were in Brunei Darussalam.

- US-ABC understands that the onus is placed on organizations to ensure appropriate measures are taken to protect personal data transferred out of Brunei Darussalam, but we seek greater clarification on what the prescribed requirement for these transfers are.

- To the extent that AITI intends to rely on prescriptive mechanisms to regulate these transfers, we urge AITI to adopt regulations that are compatible with other personal data protection regimes internationally, such as GDPR or Singapore's Personal Data Protection Act ("PDPA"), and to set out, in the PDPO, a non-exhaustive, but clear, list of measures that an entity can take to demonstrate that it has taken such reasonable steps to permit the transfer of data to provide regulatory certainty to data controllers and help data controllers demonstrate that comparable standards have been met. These measures would include:

  (i) Where the data controller assesses that the recipient is bound by comparable obligations under their applicable laws;

  (ii) The recipient is bound by binding corporate rules;

  (iii) The data controller and/or the recipient is bound by a code of conduct;

  (iv) 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 (e.g., standard/model contractual clauses such as the ASEAN Model Contractual Clauses); and

  (v) That the recipient has established systems and processes that comply to internationally recognized standards or certification schemes (e.g., ISO certifications and the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors systems).

- We also recommend the recognition of consent as a legitimate basis for the transfer of data.

- Additionally, while we acknowledge AITI's intention for the PDPO to serve as a "deterrent" to overseas organizations from misusing or using data irresponsibly, we recommend that the PDPO's territorial scope be more limited to within Brunei Darussalam.

- Data protection laws should not be extra-territorial as enforceability of regulations on foreign organizations based outside of Brunei Darussalam will be a challenge. In addition, extra-territorial privacy laws could create a web of overlapping or even conflicting data protection obligations that could make regulatory compliance overly complicated and costly for these international organizations. This may ultimately detract from the aim of privacy laws to protect personal data and result in reduced benefit to end users as foreign entities, who likely are already subject to data protection obligations in their home countries, may decide to geo-block or otherwise restrict their services in Brunei Darussalam to avoid additional compliance burden.

- To this end, we recommend that the PDPO's territorial scope be limited to data controllers and processors established within Brunei Darussalam. We further suggest conditions for coverage on data processing performed by a data subject or legal entity and suggest that the legislation targets "residents" of a jurisdiction rather than "citizens" to ensure equal treatment of all residents and to ensure that non-resident citizens are not unintentionally covered by conflicting laws:

  (i) The scope of the legislation extends only to residents who are within Brunei Darussalam at the time their personal data is processed (including collected, used or disclosed);

  (ii) The data subject or entity processing the personal data is established within Brunei Darussalam; and

  (iii) The residents of Brunei Darussalam are specifically targeted.

- We also recommend the exclusion of data processors/intermediaries from the Transfer Limitation Obligation. As previously mentioned, these companies do not have visibility over whether the data they are processing contains personal data.

  (i) By excluding this obligation from data intermediaries/processors, the PDPO would be consistent with other international PDP frameworks, including Singapore's PDPA.

  (ii) For reference, 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, it is the organization that 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 transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organization.

  (iii) Furthermore, the PDPA's Transfer Limitation Obligation requires that an organization ensures that personal data transferred overseas is protected to a standard comparable with the Data Protection Provisions, and that onus is on the transferring organization to undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure that it can do so. In undertaking its due diligence, transferring organizations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification.

8. Paragraph 4.14 re. The Data Breach Notification Obligation.

- The need for minimum thresholds to be met before notification is appropriate, but we seek clarification on the scope of "significant harm" and "significant scale." These should be defined clearly so that

companies are aware of when to notify and to prevent the regulator from being inundated with notifications that may result in a greater administrative burden.

- Further, we recommend that the meaning of "significant harm" include a materiality standard. That is, the Notification Obligation should be clearly scoped to cover unauthorized disclosure of, or access to, personal data that may cause *material* risk of harm, wherein there is *material* risk of identity theft or economic loss to the data subjects. Incorporating a materiality standard 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 inconveniences for data subjects, an increase in administrative costs and burden for the regulator, and data subjects and regulators potentially failing to take appropriate action in response to notifications that indicate a real risk of harm.

- In relation to "significant scale," an arbitrary number assigned to this may again result in notice fatigue (since notification would be required for technical data breaches that affect many users but have only trivial privacy impacts) and stretch the resources of the regulator since it may not be obvious which of the many reported breaches require specific attention and investigation. Moreover, this would also result in individuals being inundated with numerous immaterial notices such that they may not be able to take appropriate action and distinguish between inconsequential and material data breaches. This would result in the abovementioned "notification fatigue," extra costs and greater risk to all parties. Therefore, an arbitrary number should hence not be prescribed in this case.

- In addition, if data breach notification frameworks are introduced, we recommend that authorities provide guidelines around when a data controller becomes "aware" of a breach and has to report it. Data controllers should be provided a reasonable period of time to investigate and confirm a breach before requiring notification to regulators or data subjects. The language of paragraph 4.14.2 may also be amended to state that the "organization is required to notify affected individuals without due delay after notifying the Responsible Authority."

- We ask for clarification regarding what the exceptions to notifying affected individuals of a data breach are, because if steps have already been taken to mitigate the impact to the affected individuals, notice to individuals should not be required. This will balance the interests of the individuals against the administrative costs to the organization.

    (i) For example, the Singapore Advisory Guidelines on Key Concepts in the PDPA provides that an organization may rely on the remedial action exception if timely remedial actions have been taken such that it is unlikely that the data breach will result in significant harm to the affected individual. Similarly, where there are appropriate technological measures applied to the personal data (e.g., encryption, password-protection etc.) which renders the personal data inaccessible or unintelligible to an authorized party, the technological protection exception applies. The Australia Privacy Act also includes such remedial actions as exceptions.

- We seek greater elaboration on the definition of "data breach." The definition should be aligned with the Protection Obligation (paragraph 4.11) and limited to *actual* occurrences of unauthorized access, collection, use, modification, disclosure, copying or disposal, and a loss of a storage device that *actually* results in such unauthorized risks. This would ensure internal consistency within the PDPO.

- We also recommend that data intermediaries/processors be excluded from the duty to notify in event of a data breach, except for notification to the main organization who contracted the data intermediary/processor.

    (i) This obligation to notify should be borne by the data controller (i.e., the original organization that contracted the intermediary). As mentioned above, the intermediary's responsibility is only to the data controller.

(ii) Applying the duty to notify on data intermediaries/processors would be inconsistent with other data breach notification regimes elsewhere, including Singapore's PDPA and Australia's Privacy Act that places this obligation to inform regulators and individuals on data controllers instead.

(iii) It should remain the responsibility of the data controller to assess whether a personal data breach constitutes a "notifiable data breach" and notify the Responsible Authority and/or individuals.

9. Paragraph 4.2.8 re. The Accuracy Obligation.

- We enquire if self-service settings that allow individuals to update and correct their personal data are sufficient to comply with this obligation.

10. Paragraph 4.5 re. The Accountability Obligation and Data Protection Officer.

- US-ABC is supportive of appointing a DPO to ensure regulatory compliance and data protection in Brunei Darussalam. It should, however, be clarified in either the guidelines or the PDPO itself that the DPO does not need to be a citizen or resident of Brunei Darussalam and can reside anywhere in the world.

11. Paragraph 4.6 re. The Consent Obligation.

- US-ABC notes that it appears that AITI's intent is for consent to be the primary basis for processing personal data. Additionally, AITI's intent of having less prescriptive standards of consent is consistent with Singapore's PDPA and provides flexibility for organizations. However, while the draft PDPO suggests that there will be exceptions to consent, these are not further elaborated upon. Therefore, we seek to clarify the exceptions to consent.

- Additionally, we encourage AITI to consider other legal bases for processing of user data beyond the stated consent model. Examples would include the GDPR's recognition of "legitimate interest."

  (i) GDPR Article 6(f) allows for legitimate interest as a legal basis for processing personal data where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

  (ii) This will help cover a range of other scenarios and uses such as security and fraud activities, as well as basic internal business analytics which are challenging to subject to a consent standard and lack a significant negative impact on privacy. Business benefits from this, and individuals are protected in case of fraud/security concerns as well.

  (iii) GDPR Article 6 also includes other, equal bases for processing personal data, including where processing is necessary for: (a) the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (b) compliance with a legal obligation to which the data controller is subject; (c) protecting the vital interests of the data subject or of another natural person; and (d) performing a task carried out in the public interest or in the exercise of official authority vested in the data controller.

- Other exceptions that can be considered include processing of personal data in the context of vital interests of individuals, publicly available data, business asset transactions, for business improvement purposes and for law enforcement purposes. These exceptions are also recognized in Singapore's PDPA.

12. Paragraph 4.7 re. The Purpose Limitation Obligation

- US-ABC broadly supports this provision, but we would recommend that the consent standards and requirements should remain flexible so that where organizations require fresh consent for new purposes, this is not overly burdensome for both the organization and the individual.

- Repeated requests for active, opt-in, express consent may result in 'consent fatigue' in consumers and result in less, not more, data protection awareness.

13. Paragraph 4.8 re. The Notification Obligation.

- We recommend creating an exemption to the notice and consent obligations if the use or disclosure is related to the primary purpose of collection, contractual necessity, and the individual would reasonably expect the organization to use or disclose the information for that secondary purpose.

- This exemption would help to balance the need for transparency with the need to encourage data use to facilitate economic development and cost savings for companies.

14. Paragraph 4.9.3 re. Individuals Porting Data.

- We recommend that the ability to port user data be consistent with data portability obligations as outlined under the EU's GDPR.

15. Paragraph 5 re. Data Subject Rights to Access Personal Data and Data Portability.

- US-ABC recognizes the right to access personal data as an important consumer right as it plays a central role in enabling individuals to exercise further rights (i.e., 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 draft PDPO also 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".

- There is a need to balance between providing individuals the ability to exercise their right to access data effectively and the cost of compliance to companies if over-broad or frivolous access requests are made. Therefore, we recommend that the access and portability rights be streamlined, and that "user-activity" data be excluded from the access obligations.

    (i) "User activity" data could include extremely broad categories of data and metadata, including information that is related to the functioning of services, data about an individual's interaction with e-services, etc. Many of these types of data would not be meaningful or valuable to individuals exercising further rights – however if individuals were to make such requests, they would likely ask for broad data sets (e.g., all data related to transactions made with the organization), which would be very costly for data controllers to collate and provide.

    (ii) 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. "User-activity" data could also be generated from the use of proprietary tools or features resulting in risks for confidentiality of commercially sensitive elements or trade secrets. Inclusion of such data could therefore chill innovation and render Brunei Darussalam a less attractive location for data processing if there is a risk that a data access request could result in a disclosure of commercially sensitive information.

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

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

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

- On a related note to accessing data, we urge AITI to adopt a flexible timeline with regards to processing, receiving and responding to data subject requests. The draft PDPO currently mentions that requests must be responded to within the "prescribed time and in the prescribed manner."

  (i) Flexible timelines would be more appropriate as the range of organizations that will need to comply with the PDPO is very broad and can include sophisticated data processing companies as well as local retailers that only keep hardcopy records. Flexibility is therefore important to allow each an appropriate time to respond.

  (ii) An example of flexible response time is seen in Singapore's PDPA, which requires that within 30 days of the request that a response be provided: (a) either giving effect to or rejecting the request for permitted reasons; or (b) notifying the individual of the alternative timeframe within which the organization will respond to the request.

- We recommend against the inclusion of paragraph 5.4.8 where organizations are required to notify users of a rejection or exclusion of their requests and the requirement to retain copies of data where an access request has been rejected.

- Paragraph 5.5.3 states that organizations must send corrected personal data to every other organization that has received it unless the other organization does not need it for any legal or business purpose.

  (i) We recommend against requiring organizations to send corrected data to third parties as it is fairly onerous for an organization to be responsible for updating third parties and also to independently assess if these third-party organizations require the data for their own legal or business purposes.

  (ii) Instead, the data subject should be responsible for communicating this and is equipped to do so as the right of access would allow him/her to obtain the list of organizations to whom the data is disclosed.

- Additionally, paragraph 5.6 uses the term "applicable data" throughout the section. However, there is no clear definition of "applicable data." We recommend that there be a clear definition of "applicable data," and that this definition should exclude "user activity" data, for the reasons articulated above.

- Paragraph 5.6.7 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.

  (i) It is 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.

  (ii) Instead, we recommend 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 including statements that the request is being made in P's personal or domestic capacity.

- With regards to the Access, Correction and Data Portability Rights, we recommend that these rights be subject to a reasonable trade secrets exemption.

16. Paragraph 6.4 re. Power to Issue Directions.

- We recognize that while the potential fines are high, the fact that the annual turnover calculation is restricted to Brunei Darussalam limits the potential exposure significantly and is much less than the GDPR's cap of 4% of annual global turnover.

- However, we recommend removing the peg to the annual turnover as civil penalties should not be tied to a regulated entity's turnover. Instead, it should be proportionate to the harm caused to the affected individuals and whether there is any aggravating or mitigating factors. Civil penalties should also not impose undue hardship on an otherwise responsible entity.

17. Paragraph 6.6 re. The Right of Private Action.

- Having a right of private action may encourage wasteful and unnecessary litigation and impose significant costs on businesses.

- Instead, we recommend for all rights and obligations created under the draft PDPO to be administered and enforced solely by the Responsible Authority, in conjunction with the reconsideration and appeal mechanism contemplated under paragraph 6.5 of the Consultation Paper.

- We are of the opinion that private action should be an instrument of last resort not easily taken. If a right of private action is to be included in the PDPO, we recommend that the right be clearly targeted for events like a data breach, and where the data breach was caused by a willful or reckless action or omission of the organization in question. Damages should have a direct causal relationship to the claimed infringement of rights.

18. Paragraph 7 re. Offences Affecting Personal Data and Anonymized Information.

- US-ABC recommends against the inclusion of personal liability and criminal liability for breaches, obstructions or other offences. Civil enforcement of privacy laws and related legislation should be in line with international standards and requirements such as the APEC Privacy Framework, which Brunei Darussalam participates in.

19. Paragraph 9.2 & 9.3 re. Further Regulations and Guidelines.

- The scope and detail of the regulations are presently unclear. We note that this draft is reassuring in its emphasis on a flexible and business-friendly regime, yet there is still a possibility of prescriptive regulations being introduced via the regulations, which would undermine this.

- We urge AITI to avoid regulations that are unduly prescriptive, and that they should align with the general principles and philosophy of the Consultation Paper. A balance should be struck between protecting individuals and ensuring innovation is not stifled.

20. Paragraph 10 re. Interaction between PDPO and Other Laws.

- US-ABC is generally supportive of the PDPO being used as the baseline data protection law in Brunei Darussalam, with sectoral regulators continuing to have freedom to provide higher levels of protection where appropriate.

- Furthermore, unless expressly provided in the PDPO, in the event of any inconsistency the other written laws will take precedence over the PDPO.

21. Paragraph 11 re. The Sunrise Period.

- US-ABC supports this transition period as laid out in the draft PDPO. This transition period is key for organizations to understand their obligations under the PDPO and implement the necessary processes and policies for compliance. If possible, we hope for an extended sunrise period before high financial penalties come into effect as the PDPO is a new data protection regime in Brunei Darussalam, which businesses may be still unfamiliar with.

22. Paragraph 12 re. Grandfathering Clause.

- US-ABC supports how the PDPO will only be applied to personal data used, collected and disclosed on or after the date of commencement and not applied retrospectively. This allows organizations to better focus on the future and better prepare for the full commencement of the PDPO during the transition period.