

1. INTRODUCTION

- 1.1 Datastream Digital Sdn Bhd (“DST”) would like to express its appreciation for the opportunity to participate and providing its feedback to the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam (“The Public Consultation Paper”).
- 1.2 DST applauds the Ministry of Transport and Infocommunications (“MTIC”) leadership and drive for the introduction of the proposed data protection framework for Brunei Darussalam and for the appointment of the Authority for Infocommunications Technology Industry of Brunei Darussalam (“AITI”) as the Interim Data Office for this purpose vis a vis to develop a new law for the protection of individual’s personal data.
- 1.3 The Public Consultation Paper represent trial and tested methodology by adopting Singapore’s model based on the 2011 / 2012 consultation paper. It is noted that there are certain degree of certainty in this Public Consultation Paper, the benefit of learning from Singapore. The Singapore’s Personal Data Protection Act (“PDPA”) has evolved and developed since its debut in 2012. There are recent amendments to the PDPA. Considering that Brunei Darussalam is commencing its journey into the PDPO it is important to know at the earliest opportunity which version of the PDPA that Brunei Darussalam will choose. To follow the pre-amendment PDPA or the recent PDPA with the benefit of learning and minimise chances of repeating certain pitfalls.
- 1.4 The draft PDPO should not hinder any innovation development especially when strict practices impose in regulating personal data as organisation such as DST utilise our customer data for improvement to our customer service and experience in using our product and services.
- 1.5 The telecommunications market in Brunei Darussalam have undergone a monumental and first of its kind market transformation spearheaded by Darussalam Assets Sdn Bhd (“DA”). The transformation brought about market reform with the end result of equal access to all the three salescos. The most tangible result from the transformation is the divestiture of network infrastructure / carveout of Brunei Darussalam’s telecommunication industry.
- 1.6 DST has a 25 years’ of foundation and roots in Brunei Darussalam. In the wake of the market reform and infrastructure carveout of Brunei’s telco industry transformation, the new DST was born which followed through with DST’s own major digital transformation exercise. Formally a full-service Mobile Network

Operator and a full Mobile Service Provider to now, an asset light, customer focused digital first operator, in triple play mobile, fixed and all things digitally horizontal.

Now expanding from a mobile service provider to a fixed service provider, both Residential and Enterprise and mobile and fixed convergence play, DST remains the major telco player in Brunei. With the expansion of services to fixed, this is a developing area for growth.

Backed by its 25 years of traditional telco experience, and always transforming mindset, DST continues to build on its digital platform and will continue to build its ecosystem to provide digital services, providing value and convenience as a priority to its customers in Brunei, with a set vision to grow into the region as a digital service provider.

- 1.7 Protecting its customers data is at the paramount in DST's business operation by having systems and processes in place to prevent unlawful and unjustified disclosure.
- 1.8 Given the effect of this transformation, Brunei Darussalam witnessing intense competition amongst the salescos and visible drive for salescos' towards innovation of their products and services. The competition at the salescos level propelled for more consumers' centric campaign and marketing taking shape and form from lucky draw, referral programs for subscribers to invite new subscribers, porting offers and enhance digital platform customer interface such as mobile applications, website, online order portal and the likes.
- 1.9 It is noted that the justification from the public interest for the need to have a legal framework on personal data protection based on the technological advances fuelled by increased mobile and fixed broadband connectivity, rise of the internet and its various applications, advancements in data processing, data analytics, advancements in Artificial Intelligence and machine learning. The personal data protection framework is essential as it sits strategically from economic benefits aligned with ASEAN – commitment to propel ASEAN towards a digitally-enabled economy, Digital Economy Masterplan 2025 and MTIC Strategic Plan for Connected Smart Nation.
- 1.10 Factually, currently there is no specific legislation governing personal data protection by the private sector in Brunei Darussalam. The AITI submitted that the lack of accountability on the handling of personal data may lead to an erosion of consumer trust. DST does not disagree with these proponents' reasons. However, in the same premise, DST as a SeTi license are bound by the provisions of the

Telecommunications Order, its SeTi license's provision and the Code of Practice for Competition in the Telecommunications Sector (Competition Code) pertaining to the protection of subscriber information and End User Service Information.

- 1.11 In light of the vibrancy of the new telecommunication market in Brunei Darussalam and technological advancement, it is commendable and timely for the introduction of the personal data protection framework and eventual Personal Data Protection Order ("PDPO") in Brunei Darussalam. DST wishes to reach out to the AITI for a balancing act to be at the backdrop of this framework i.e., balancing the interest of the public and businesses in respect to the collection, handling, management and the usage of personal. It is worthy to stress that the telecommunications sector need to have a light touch regulation and to avoid over regulation, considering the market size and its economy.

2. DST'S COMMENTS TO PART 2: POLICY POSITIONS IN THE DRAFT

2.1 Definition of Personal Data – Paragraph 3.1

- 2.1.1 Personal data definition is very subjective and require proper definition on what is construed as personal data which is accessible by the owner and what is not such as technical information, IP configuration etc which can be useful to the organisation for true purpose of process its customer data and information.

The definition is too general and wide. The Public Consultation Paper seek to regulate any form of data from individual to be classified as "personal data" as long as the organisation is able to identify the individual from that data or based on the combination of that data with other information that the organisation has or likely to have access.

In the wake of artificial intelligent and machine learning capability, the suggested definition or personal data will encapsulate information produced by this independent processing power of great computing using artificial intelligent and machine learning to identify customers behaviours in respect of usage of DST's products and services and such information will be considered as "personal data" under the PDPO. It is submitted that this independent data should be available for the organisation to harness and utilise in promotion of suggestion of other services of the organisation.

DST propose that “personal data” should be defined as:

- (a) data relating to an individual provided for commercial purposes and/or to manage current business relationship between the organisation and the customer; and
- (b) Data that directly identifies an individual without the need for any other data.

2.1.2 The definition of “personal data” does not differentiate between true or false personal data. This could create certain degree of unfairness to the organisation, for example that an individual provides erroneous information about him/herself to the organisation by stating, deliberately, misleading information pertaining to the individual. In the event that the individual as a customer / subscriber procuring products and/or services from the organisation it is accepted that the organisation, as mandated by The Accuracy Obligation – Policy 4.10, must make a reasonable effort to ensure the accuracy and completeness of the personal data collected. By taking the reasonable effort the organisation ascertains accurate information about the individual and the individual eventually become a customer / subscriber, it is agreeable for that personal data to be protected under the PDPO.

On the other hand, if having taken the necessary reasonable effort to ascertain the accuracy and completeness of the personal data the individual does not become the customer/subscriber to the organisation then the personal data should not be considered personal data under the PDPO.

2.1.3 Another caveat from having a very wide definition of personal data is that the cost of compliance to the organisations in retention of the personal data and providing access to the customers.

2.1.4 It will be ideal for the personal data collected in electronic forms to be covered under the PDPO. This is consistent with the current development in light of electronic forms and e-KYC approach. This will encourage digitalisation to the organisations.

2.2 Categories of Personal Data – Paragraph 3.2

The PDPO includes sensitive personal data such as mental health, financial information, genetic data, biometric data and personal history – criminal records. This expand to more sensitive personal data and the PDPO requires the organisation to act reasonably in considering the sensitivity of the personal data in regard to the amount of information to be provided to individuals when collecting their personal data. The practical test will be the level of comfort or apprehension for an organisation to inquire sensitive information of such nature from individuals in assessing their eligibility in applying for the organisation products and/or services.

DST welcome AITI’s guidance and look forward for the sunrise period to be used as the barometer for PDPO implementation.

2.3 Territorial Scope – Paragraph 3.6

DST welcome that the PDPO will apply to all private sector organisations that collect, use or disclose personal data in Brunei Darussalam regardless of the organisations are resident or have an office or place of business in Brunei Darussalam. In other words, foreign organisations such as Zalora, e-bay, Google, Youtube, Netflix will be bound by the PDPO.

Similarly, foreign organisations that does collect foreign personal data but uses Brunei Darussalam as their “port of call” to store and/or process such data will also be subject to the PDPO.

Despite the nobility of this provision, the PDPO acknowledged the weaknesses of this policy in respect of its potential adequacy pertaining to investigations and complaints against foreign organisations under the PDPO.

The PDPO insisting that this policy should be stated as a matter of principle and hopefully act as a deterrence for foreign organisations not to be running foul against the PDPO.

In any event, the PDPO should provide protection to any individuals in Brunei Darussalam conducting business with foreign organisations as it would to providing protection to individuals dealing with organisations in Brunei Darussalam. This will ensure that the individuals in Brunei Darussalam will not be prejudiced, discriminated and disadvantaged in enforcing their rights against foreign organisations by having to conduct any legal action abroad.

It is expected that in parallel, there should be an ongoing discussion with foreign data protection authorities to establish process and procedures for PDPO compliance in terms of cross border enforcement.

The PDPO should not be allowed to have different standards between local organisations and foreign organisations standard of compliance of the PDPO.

2.4 Data Intermediaries / Processors – paragraph 3.7

The Data Intermediaries / Processors should be liable for their own non-compliance and/or breach of the PDPO and not the organisations engaging them provided that the organisations have not issued any instructions that caused the Data Intermediaries / Processors to contravene the PDPO.

2.5 Data Protection Obligation – Paragraph 4

2.5.1 Data Protection Officer (“DPO”):

Under the PDPO it is a requirement for an organisation to appoint a DPO. The challenge will be on the availability of DPO in Brunei Darussalam. The Personal Data Protection Commission (“PDPC”) Singapore stated that there are 9 competencies for a DPO. The AITI should present the initiatives, incentives or scheme for DPO training regime once the PDPO is enforced.

Perhaps it can be suggested that during the sunrise period, a special pioneer scheme for pioneer DPO can be set up in key organisations such as telecommunications, ICT, health care, retail where these pioneer DPO are nominated by the organisations and to undergo on the job training with guidance and sponsored fully funded trainings provided by the AITI with the objective of achieving the relevant competencies as DPO.

It is expected for the DPO to handle and liaise with individuals in respect to any queries on PDPO related policies and practices. On the outset this should be agreeable and provide transparency to the organisations. Similarly, this methodology and handling process should be one of the items to be covered by the special pioneer scheme training. The decision-making process of the DPO in respect to the granting or rejecting any request must be clearly established and best to draw from regional experience.

2.5.2 The Consent Obligation – paragraph 4.6

DST noted that the PDPO is flexible in respect of as how consent is obtained. However, DST is keen to share practicality of obtaining fresh consent for new purpose as this will be burdensome and time consuming. As an example, in the event that DST provides a new location-based service and requires the usage of personal data relating to the historical movements of the individuals and there is no specific consent for this purpose at that time, as a matter of flexibility, DST believed that fresh consent will not be necessary. DST will be guided and responsible in ensuring any future services will only collect and process data reasonably and necessary it required.

DST propose that deemed or implied consent to be accommodated in the PDPO where consent is deemed or implied given unless and until individuals submit their objection. This is more practical given that human behaviour suggested that in business as usual transactions, individuals' customers expect to be provided / access new services without requiring them to provide active and express consent. This is very relevant in telecommunications especially ongoing relationship.

2.5.3 The Purpose Limitation Obligation – paragraph 4.7

DST agrees for a new consent is required for a totally different purpose not relating to the deployment of services of the organisation. DST's reiterate its preceding position. Consent can be considered granted, in the event that the key purposes and uses or generically described purposes have been described in the terms and conditions of services / contract signed by customers or any update of such terms and conditions.

2.5.4 The Access, Correction and Data Portability Obligations – paragraph 4.9

Please see our comments for Data Subject Rights below.

2.5.5 The Retention Limitation Obligation – paragraph 4.12

In DST's nature of business personal data including credit / debt history are retain and kept continuously despite such debts maybe written off due to financial policy. The retention is to ensure that credit control information records such information for credit control. DST opined that this constitute one of the valid reasons for retention of personal data.

2.5.6 The Transfer Limitation Obligation – paragraph 4.13

DST agreed with the general principles stated under this obligation. In practice, it will be difficult to ascertain that the same standard and requirements are accorded to the data protection transferred to outside Brunei Darussalam. It is suggested that as long as DST have conveyed to the foreign organisation that they need to provide same standard of protection comparable to PDPO and received affirmative reply for such organisation then DST should be considered as having taken the appropriate measures to protect the personal data under the PDPO.

2.5.7 Right to Withdraw Consent - paragraph 5.3

Consent cannot be withdrawn in case where the personal data provided to the organisation is necessary for the provision of the services utilised by the individual and/or for the purpose of credit and debt collection.

2.5.8 Right to Request for Access to Personal Data – paragraph 5.4

DST find it technically impractical and burdensome to provide to the individual on information on how the personal data have been used or disclosed within a year before the date of request for access. Unless the PDPO take into consideration that such information may be provided by DST subject to the best of its technical and business process capability.

DST seek AITI's indulgence in explaining and illustrating rejection on the ground of contrary to the national interest.

DST generally agrees where in the draft PDPO, an organisation may allow to reject the individual or customer access request by notifying the individual or customer accordingly. A reasonable fee should be applied to cover the cost of the individual/customer accessing their data and/or organisation attending to the individuals request for access.

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

DST generally agrees where the customer data held by an organisation can be access and corrected by the customer if the data is inaccurate or needed to be updated.

2.5.10 Right to Data Portability – paragraph 5.6

DST welcome the right to data portability as well as its exception. DST seek to suggest for additional exception as to when data porting maybe rejected i.e. personal data contained third parties personal data which inclusive of other individual personal data and there is no evidence of consent from such third party.

2.5.11 Investigations, Enforcement and Appeal – paragraph 6

Data Protection Appeal Panel (“DPAP”):

The membership should comprise of respectable independent personalities. It is suggested that the DPAP publish its list of panels in excess of 3 to be readily available to hear the appeals.

Right of Private Action:

Perhaps the right of private action should not be conditioned upon exhaustion of all avenues of appeal as justice delayed is justice denied.

2.5.12 Do Not Call Regime – paragraph 8

DST has few concerns regarding the implementation of Do Not Call (“DNS”) regime. As part of our business operations to keep our customer updated with our latest product and/or service offering, including our engagement with our merchants and other business partners, DST believes that part of the organisation obligation is to reasonably use the personal details in accordance with draft PDPO, hence the DNC registry may seem to be redundant. The establishment cost for DNC can be utilise on bridging the digital divides in Brunei Darussalam. In addition, if the Responsible Authority decided to implement the DNC regime, amongst few, who will bear the cost and responsible in maintain this registry, how will the

database made available to organisations and if theirs is any update or changes in the database, how the organisation will be notified, etc.

It is possible for a confusion resulting from customers registering in DNC Registry but still expect to receive certain marketing materials but seek to exclude others.

2.5.13 Sunrise Period of Two (2) years – paragraph 11

The sunrise period of two (2) years may be not enough to implement compliance to the draft PDPO requirements as organisations may need to invest or upgrade their customer management system to comply with the new regulations. In such event, it is acceptable for an initial sunrise period of 2 years to be proposed but with an open mind for additional period beyond the initial 2 years judging from readiness level as assessed by the stakeholders.

-END OF SUBMISSION-