Stakeholder Briefing Details		
Subject:	UNN Input to PDPO – Post Stakeholder Briefing	
Venue:	MTIC Hall	
Meeting Date:	27th May 2021	
Attendees	**Initials**	**Institute / Company**
~~##########~~		UNN
~~##########~~		UNN
~~##########~~		UNN
~~##########~~		UNN

No.	Subject
1.	PDPO Introduction and Stakeholder Sharing Session – Live
2.	Queries put forward to PDPO Committee

No.	Discussion Points	Action Owner	Action Date
1.	While the proposed data protection law appears general, as it should be, it is understood from the Q&A segment that a supplementary framework would further define certain scopes of the law's application (e.g. reasonableness, relevance of the purpose). It is therefore proposed that the agency assigned to develop this said framework be one that is qualified, experienced and most importantly independent from AITI. The agency should also have the competencies in data protection management and should at the very least be habitually in the business of transborder data as a processor or owner. This also prevents any overlaps in functions of "sectoral regulations" (Section 10.6) and to preserve balance as stated. This also should be taken into consideration when establishing the Responsibility Authority (Section 1.6).	AITI	No Date
2.	Concept of data ownership, custodianship, stewardship etc and how the respective obligations would be compared to each other?	AITI	No Date
3.	How does this support data brokering and monetization initiatives, especially in case it involves elements of personal data being traded?	AITI	No Date
4.	How about personal data that are being exchanged between companies, by virtue of their business or to support certain functions? e.g. HR send staff salary particulars to Banks for processing.	AITI	No Date

No.	Discussion Points	Action Owner	Action Date
5.	Does the same obligation applies to data custodians above, as it would be applicable for the data owners (first party who captured the data)?	AITI	No Date
6.	What are the expectations for companies to treat individual's right to opt out from the sale of personal information etc. What sort of process/policies should be in place? Or is this entirely dependant on the organization choice, so long as it is justifiable?	AITI	No Date

Next Meeting Details	Discussion Points
Subject:	No Meeting
Venue:	
Meeting Date:	
Time:	

END OF DOCUMENT

Response on Public Consultation Paper on Personal Data Protection Order

Unified National Networks Sdn Bhd

23 August 2021

Confidential

Table of Contents

Glossary of terms

DCMS	Department for Digital, Culture Media and Sport, UK
DPA	Data Protection Agency (the Responsible Authority)
DPIA	Data Protection Impact Assessment
DPAP	Data Protection Appeal Panel
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
GSMA	GSM Association (Mobile Industry Trade Association)
IoT	Internet of things
NPC	National Privacy Commission, Philippines
OECD	Organisation for Economic Co-operation and Development
PCP	Public Consultation Paper, Brunei
PDPA	Singapore Personal Data Protection Act 2012
PDPC	Singapore Personal Data Protection Commission
PDPO	Personal Data Protection Order, Brunei
UK ICO	Information Commissioner's Office, UK

1 Response to the Public Consultation Paper

1.1 General comments

1.1.1 Responsible data governance

Data protection laws should have the effect of incentivising responsible data governance and provide a comprehensive way to address privacy concerns.

The PDPO aims to be non-prescriptive. This is good practice; data protection laws should not be too prescriptive. Instead, they should operate on the basis of principles, so as to ensure flexibility and accommodate future changes in business practices and technology.

However, we need to consider and better understand how the PDPO will be administered and enforced. This is essential given the magnitude of the financial penalties that could be meted out by the new data protection agency.

1.1.2 Availability of Draft PDPO

It is important for stakeholders to see the actual draft Personal Data Protection Order (PDPO), rather than extracts via the Public Consultation Paper (PCP)

There is usually a standard set of background information, including a draft of the regulatory proposal, discussion of policy objectives and the problem being addressed and, often an impact assessment of the proposal and, perhaps, of alternative solutions.[1]

Information … such as … drafts of legislation … should, wherever possible and appropriate, be made available to stakeholders to enable them to make informed comments on proposals and proposed legislation.[2]

1.1.3 Timeline

The timeline to December is too tight and does not allow for productive and informed development of the PDPO. This will inevitably store problems for the future.

The example of Singapore is useful to benchmark against. An extensive review of the Personal Data Protection Act (PDPA 2012) was undertaken by Personal Data Protection Commission (PDPC) with a multi-year process beginning in 2017. There were three public consultations on various aspects of data protection, as this is a highly fluid subject matter area, in 2017, 2018 and 2019. Input from interested stakeholders was used in a public consultation in May 2020, with the Amendment Act enacted six months later in November 2020. This Act came into effect in February 2021. Note that this was only a review of an existing data protection act, not the introduction of a new act.

“One important lesson from Singapore’s experience is the need for stakeholder input in updating laws. Among citizens and policymakers alike, awareness of the risks associated with data has risen.”[3]

---

[1] https://www.oecd.org/mena/governance/36785341.pdf
[2] https://www.pmc.gov.au/sites/default/files/publications/best-practice-consultation.pdf
[3] https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/August-20/Singapores-Review-of-the-PDPA-and-its-Opportunity-for-Leadership-in-the-Region

1.1.4 Clarity of process

Clarity is needed on the process that will be adopted with regards to the responses received during the consultation process. This is especially important with regards to the transparency of the decision-making process behind which comments will be incorporated and which will not.

For example, comments could be recorded, analysed and then accepted or rejected against an agreed and standardised set of criteria.

1.2 Specific comments

1.2.1 Independent Responsible Authority

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

The European Commission defines Data Protection Authorities as follows: "DPAs are **independent** public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They **provide expert advice** on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State."[4] (Emphasis added).

The data protection authority (DPA) for Brunei (para 6.1) should be established to raise awareness, encourage good practice, deal with complaints, investigate and take appropriate enforcement action.

The DPA should be independent in terms of its position and reporting structure within Government, it should have sufficient powers and be correctly resourced in terms of expertise as well as being adequately funded in order to execute its duties.

In UK, the DPA is the ICO is an independent public body and the Department for Digital, Culture Media and Sport (DCMS) is the ICO's sponsoring department within Government. The ICO is primarily funded by organisations paying the data protection fee, which accounts for around 85% to 90% of the ICO's annual budget. This is supplemented by grant-in-aid from the government to fund the ICO's regulation of various other laws.[5]

In Singapore, the DPA is the Personal Data Protection Commission (PDPC), which serves as Singapore's main authority in matters relating to personal data protection and will represent the Singapore Government internationally on data protection related issues.[6]

1.2.2 Penalties

The financial penalties (paras 6.4 & 7) are extremely onerous. At 10% of turnover they are significantly higher than those set out in the GDPR which has already been criticised for setting penalty amounts at too high a level.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en
[5] https://ico.org.uk/about-the-ico/
[6] https://www.pdpc.gov.sg/Who-We-Are

It is essential that financial penalties are imposed as a means of providing **effective, proportionate and dissuasive punishment**, and are not utilised as a means for revenue generation. An independent, properly resourced (i.e., skill sets) and adequately funded DPA should be less inclined to adopt this approach.

Funding could come from central government and would depend on how the DPA is set up.

For example, in UK the ICO is 85%-90% funded by the data protection fee. **This fee is around** £40-£60 **(B$75-B$112)** for most organisations, including charities and small and medium-sized businesses. The fee can be up to £2,900 for businesses who employ many people and have a high annual turnover.[7] Failure to pay the fee can result in a fine.

In the Philippines, the National Privacy Commission (NPC) has yet to determine a schedule of reasonable fees for registration, renewal, and other purposes to **recover administrative costs**.[8]

1.2.3 Appeals process

The PDPO provides for the establishment of a Data Protection Appeal Panel (DPAP). Where an appeal is lodged with the DPAP, the Chairman of the DPAP shall nominate a Data Protection Appeal Committee. The Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal

The DPAP will need to be independent and suitably qualified in order to be able to consider appeals in an effective and equitable manner. The detail behind how the PDPO provides for the establishment of the DPAP is not stated and clarity should be provided.

1.2.4 Horizontal / neutral regime

The data protection regime should be neutral across technologies and sectors.

General data protection laws should apply to any processing of personal data, regardless of sector or technology. This represents a positive for the consumer, as they do not need to consider specific rules for the technology they are using or the activity they are doing. It is positive for stakeholders in the digital ecosystem as it sets a consistent standard across many of the traditional segments which are now dynamic and breaking down.

Therefore, a horizontal data protection regime could reduce consumer confusion and potentially reduce costs for organisations. Unfortunately, the PCP refers to sector-specific frameworks (paras 1.6 & 3.2.2) and that the PDPO will operate concurrently with other legislative and regulatory frameworks that apply to specific sectors (para 10.1).

1.2.5 Data breach notification

The PCP states that, under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach.

The PDPO (para 4.14) is more prescriptive than elsewhere in this instance, stating a fixed duration of time for notification (3 calendar days) rather than establishing a principle, such

[7] https://www.gov.uk/data-protection-register-notify-ico-personal-data
[8] https://www.privacy.gov.ph/faqs-registration-for-individuals-and-organizations/

as notification of a data breach “promptly”. However, it is in line with GDPR on the notification period.

1.2.6 Categories of Personal Data

There is no category for “sensitive personal data” in the PCP (para 3.2). The burden is placed on organisations to decide how sensitive the data may be. Inevitably, this will lead to differing interpretations and thus different standards of protection between organisations. This is not ideal for consumers.

However, the PDPO (para 4.11, make reasonable security arrangements) is in line with the GDPR (implement appropriate technical and organisational measures) with the level of security taking into account the sensitivity of the data and, therefore, the attendant risk of harm.

1.2.7 Purpose Limitation

The PDPO (para 4.7) states that the purpose limitation requirement “seeks to prevent over-collection of personal data” based on a “reasonableness” approach.

The GDPR approach is more specific, with a clearer definition:

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (‘purpose limitation’).

However, the new Responsible Authority (DPA) is expected to prepare a supplementary framework that would further define certain scopes of the law’s application, including “reasonableness”.

1.2.8 Transfer Limitation

The PDPO (para 4.13) places the onus on organisations to ensure that appropriate measures are taken to protect personal data transferred out of Brunei. However, it is not clear what process will be adopted to determine how these measures will be certified as appropriate.

1.2.9 Right to Data Portability

As well as the GDPR, regional data protection frameworks in the Philippines and Singapore have introduced the right to data portability. The PDPO “may” introduce such an obligation (para 5.6). Further clarity on this potential obligation would be welcomed.

1.3 Questions from UNN

1.3.1 Fees

The PCP does not state what administrative fees or annual fees will be payable under the PDPO. Other jurisdictions, such as UK ICO, levy modest annual fees on organisations to cover the administrative costs of the Responsible Authority (i.e., the DPA). What fees will be payable under the PDPO?

1.3.2 Data Controllers

There is a specific section on Data Processors (para 3.7) but there is no explicit section to discuss the requirements for Data Controllers. The obligations of Data Controllers as they pertain to Data Processors is covered in para 3.7, but we would seek clarity as to whether there are further obligations in the PDPO for Data Controllers.

References:

Public Consultation Paper on "Personal Data Protection for the Private Sector" issued by AITI, dated 20 May 2021

UNN First submission: E-mail with subject: UNN Input to PDPO – Post Stakeholder Briefing, dated 23 June 2021

UNN Second submission: Letter (Ref: RC20003699), dated 23 August 2021

AITI Letter in reply to UNN submissions, dated 13 September 2021

Table: Consideration of the AITI letter dated 13 September 2021 replying to UNN's response to the PCR

Ref AITI Letter	Response from AITI	Further comment and analysis
3.1. Responsible data governance	The PDPO provides for the setting up of a Responsible Authority (hereinafter referred to as the "RA") who will administer and enforce the PDPO.	The response does not address the concerns UNN raised i.e., how the PDPO will be administered and enforced given the magnitude of potential financial penalties.
3.2. Availability of draft PDPO	The Authority has been advised by the Attorney General's Chambers against publishing the draft PDPO in its entirety as part of the public consultation.	The response does not address the concerns UNN raised i.e., to see the actual draft PDPO, rather than extracts via the Public Consultation Paper (PCP). In addition, AITI has made references to **written advisory guidelines (paras 9.3 & 11.4)** to be developed under the PDPO indicating the manner in which the RA will interpret the provisions of the PDPO. During the consultation, AITI indicated that while PDPO has been developed by their external counsels and supporting Attorney General Chambers (AGC) counterparts, the written advisory guidelines may be developed by AITI. If we cannot yet be privy to the PDPO, these proposed guidelines or outline of the **guidelines should be made available during the development stage as it would be the directive to define thresholds, base cases, formulas, penalties, cross-border data transfer requirements, notification of data breaches, and regulations to implement the data portability provisions.**

Ref AITI Letter	Response from AITI	Further comment and analysis
3.3 Timeline	Considering that Brunei has a much smaller number of organisations compared to Singapore and the EU, the Authority is confident that this form of active and open engagement will enable stakeholders to grasp the concepts under the PDPO and voice out their views and concerns, thus allowing for a productive and informed development of the PDPO.	AITI is proposing a 2 year sunrise period from the date the PDPO is enacted (current target is Q4 2021). So, the PDPO will be in force and it is expected that the sunrise period will be a "soft launch" during which time industry should be able to expect light touch enforcement.
3.4. Clarity of process	At this juncture, we would like to seek clarification from UNN on whether UNN is requesting confidential treatment for their first and second submissions as both are marked as confidential.	Our submission is not confidential in the context of the PCP and should be used/published as required in the PCP.
4.1 Independent Responsible Authority	AITI would like to clarify if this response supersedes UNN first response where UNN mentioned that the Responsible Authority should be habitually in the business as a processor or owner seeing as the two responses are contradicting.	The preliminary feedback is interrelated with our subsequent review and requires elaboration. The intention behind the preliminary comment was to emphasize that representatives of the Responsible Authority should have the essential prerequisites including **track records of the required expertise and experience** in data protection processes. We are not implying that the RA should be a data processor/owner, but its representatives should be subject matter experts. The issues are competencies (per first response) and reporting structure (per second response) with both relating to the constituents of the RA.
4.2 Penalties	Since the maximum fine under the PDPO is based on an organisation's annual turnover in Brunei, it can be said that the GDPR imposes a higher maximum level than the PDPO.	Under GDPR, the maximum penalty is 4% of worldwide turnover. Under PDPO the maximum penalty is 10% of turnover. The point about global and Brunei turnover is moot for UNN. The PDPO proposed penalty is 2.5 times the maximum penalty of GDPR, which has already been criticised for setting penalty amounts at too high a level.
4.3 Appeals process	The Data Protection Appeal Panel will be an independent structure comprising of individuals appointed by the Minister.	Noted, no further comment.
4.4 Horizontal / neutral regime	While the PDPO will operate concurrently with other legislative frameworks that apply to specific sectors, it generally operates as a baseline law for data protection.	Noted, no further comment.

Ref AITI Letter	Response from AITI	Further comment and analysis
4.5. Data breach notification	… the timeline only starts running after an assessment is conducted, when the organisation determines that a particular data breach is considered as notifiable	Noted, no further comment.
4.6. Categories of personal data	In general, the **Authority** considers that 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.	No formal categorisation of data, the organisation must act in a reasonable manner and put in place reasonable security measures. At this stage the definition of "reasonable" has not yet been provided. We expect the guidelines would provide for such definitions. For clarification, is the "Authority" referred to in para 4.6 the RA as opposed the AITI?
4.7. Purpose limitation	To clarify this point, the PDPO intends 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.	We would seek confirmation on **how this flexibility would be formally provisioned** whether it would be included in the final PDPO or that reasonableness tests would fall under the guidelines.
4.8. Transfer limitation	The Responsible Authority intends to provide more guidance concerning the specific cross-border data transfer mechanisms at a later date.	No comment at this stage, await further information.
4.9. Right to data portability	The Authority proposes to exclude the concept of the right to data portability from the PDPO at this stage.	Noted, no further comment.