11 March 2020

Personal Data Protection Department
Ministry of Communications and Multimedia Malaysia
Lot 4G9, Persiaran Perdana, Precint 4,
Central Administration of The Federal Government,
62100 Putrajaya, Malaysia.

Subject: Response to the Public Consultation Paper No. 01/2020: Review of Personal Data Protection Act 2010 (Act 709) [Updated submission with additional recommendations]

On behalf of the Asia Internet Coalition (AIC) and its members, we would like to thank Malaysia's Department for Data Protection ("**JPDP**") for giving AIC the opportunity to provide our feedback on the Public Consultation Paper No. 01/2020 ("**Consultation**") in relation to the Review of the Personal Data Protection Act 2010 ("**PDPA**"). As an introduction, AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com. AIC as an industry association has been actively contributing to privacy and security legislations in Asia, and we therefore support the government's objective of revising the PDPA to strengthen its implementation and align to international standards.

In our digital era, a growing array of organizations use personal data to provide a growing range of services. Responsible data use can unlock benefits for people, companies, and other organizations around the world. Regulation can protect individuals and communities from harm and misuse of data, and help maintain the trust that enables innovation and change. Given this, we understand the government's motivation and believe that this is a timely initiative to review the PDPA and bring it in line with global standards and requirements on personal data protection.

As responsible stakeholders in this policy formulation process, we appreciate the ability to participate in this public consultation and submit our views. As such, please find appended to this letter, a detailed comments and recommendations which we would like to respectfully request you to consider when reviewing the PDPA.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue for data protection in Malaysia. We stand ready to engage with the Personal Data Protection Department's committees who have been tasked to look into possible amendments to the act which would strengthen personal data protection and expand the existing personal data privacy system.

Thank you.

Sincerely,
Jeff Paine

Managing Director, Asia Internet Coalition (AIC)

DETAILED COMMENTS AND RECOMMENDATIONS

A. Section 1: Recommendation to align the role of data processors to international best practices and avoid imposing registration requirements on data processors

Comments: We are in favor of clarifying the primary responsibilities of data users, vis-à-vis data processors. Some direct regulation of data processors, where appropriate, would be consistent with international best practices. However, based on the Consultation's proposal, it is unclear what the JPDP aims to achieve by intending to impose "direct obligations" on data processors under the PDPA. The law should be explicit in the division of obligations between the data user and the data processor, in a manner which reflects the realities of each parties' control and role over the processing of personal data. Few of the obligations that apply to a data controller should apply to a data processor. For example, data processors have no direct relationships with end users and should not be responsible for consent-type obligations or fulfilling subject access requests.

A data processor should be obligated to: (a) follow instructions of a data user, and (b) implement reasonable and appropriate security measures for the systems it controls. It does not have visibility into the data sets, the sensitivity of the data, and the impact on the individuals and therefore it is not appropriate for it to have obligations beyond this. For example, data processors like cloud services providers - often have no visibility on the data being processed by them (including lacking an ability to distinguish personal data from other types of data) and it would therefore be inappropriate for them to have the same or similar obligations as a data user. However, it may be appropriate for a data processor to be liable for acts which are not authorised by the data user.

In contrast, the data user should bear the primary obligations for compliance with the law. Accordingly, the legislation should explicitly identify the data user (not the data processor) as being accountable to data subjects and the regulator. Data processors do not have the same relationship with data subjects and typically are not in a position to make meaningful or independent decisions about the processing of personal data – rather they implement decisions of a data user. It is therefore inappropriate to hold data processors accountable to data subjects. Instead, a data user should contractually be free to impose consequences for a data processor failing to comply with its obligations to the data user. The handling of privacy incidents and the determination of appropriate actions must be determined by the data user.

International best practices do not obligate data processors to report a breach to a regulator or a data subject directly. All actions are funnelled through the data controller, as they are the controller and owner of the data from the perspective of the data processor. Not all data processors have insights into a breach. Data processors wouldn't have insights into what specific data may have been breached, nor can they see how many data subjects are affected, nor their residence, nor can they judge the impact of the data breach on data subjects. For example, enterprise cloud users (the data controller) often encrypt the data stored/processed in the cloud as a best practice security measure; such encryption prevents the cloud services provider (the data processor) from reading and defining the data and determining whether it is PII-related. Additionally, depending on the configuration of the data controller, cloud services providers (CSPs) may not be able to judge what is an appropriate or inappropriate instance of data access or detect/identify a breach.

The obligation of a CSP is to inform the customer of relevant security events (via a mechanism such as logging alerts). The parsing of CSP security events and their materiality to a potential data

breach relies solely on the Customer. Even if the CSP (the data processor) is able to read the data in the breach, reporting it beyond the data controller could violate confidentiality agreements or the privacy of the data subject. We propose following the GDPR, under which the role of a processor should be to report the breach (if the processor is aware of it) to the data controller and let the data controller proceed with appropriate actions.

We therefore recommend that the JPDP consider alignment to the EU General Data Protection Regulation (GDPR), Article 28, or the Singapore Personal Data Protection Act (PDPA), Section 4(2), to allocate appropriately the responsibilities between data users and processors. In addition, we request that the JPDP avoid imposing requirements on data processors for registration. As indicated above, data processors often do not have sight of their customer's data, and hence will not be able to establish whether personal data is processed, and therefore cannot reasonably be expected to know when and whether it should register with the JPDP.

Furthermore, while the law should clearly distinguish between the rights and obligations relating to 'access, storage, security, disclosure, deletion, security breach notification etc.' (various stages of handling of data) as between a data user and processor, the law should not dictate terms/clauses that must be included in the contracts between controllers and processors. The nature of the relationship between such entities could vary considerably and a set of inflexible standards could lead to inappropriate or impossible obligations being placed on these entities in the context and nature of their relationship.

B. Section 2: Recommendation on Data Portability

Comments: We recognize that data portability can provide people with control over their information, and we support giving individuals the ability to access, correct, delete and download personal information about them. Individuals should have access to personal information they have provided to a data user, and where practical, have that information corrected, deleted, and made available for export in a machine-readable format.

Making it easier for individuals to choose among services facilitates competition and innovation, empowers individuals to try new services, and enables them to choose the offering that best suits their needs. Data portability can benefit consumers by lowering barriers to entry in the market for digital services for competitors who provide comparable services and can enable new business models and innovative services through easier access to data. Competition and innovation are important for the Internet economy—and for creating services people want.

We encourage JPDP to continue to review international data protection regimes and developments as it looks to create Malaysia's own framework. Interoperability and consistency are the key to facilitate cross-border data flows, and therefore it is important to ensure alignment with other existing data portability provisions, such as the European Union's General Data Protection Regulation ("GDPR") and Australia's Consumer Data Rights ("CDR"). Most jurisdictions that have adopted or are adopting data portability rights either require a data user to provide the data directly to the individual (e.g. California Consumer Privacy Act or "CCPA") or, if organizations are expected to exchange data without the data subject playing a direct role, to make sure not to put an additional burden on organizations to maintain processing systems which are technically compatible (e.g. GDPR Recital 68 and Article 20).

We also wish to emphasize that this right does not work under the GDPR at the moment. While we at least know under the GDPR what to provide, the format is totally unclear. Concerns on data portability rights: (i) applicability , (ii) scope (what needs to be provided, can the information reasonably be collected, and would we not have to release sensitive business information?); and (iii) format (what exactly would be an appropriate format?) must all be given due consideration.

We also suggest referring to the global standard ISO Cloud Standard ISO/IEC 19941:2017, which addresses cloud computing interoperability and portability requirements. Standardized means of transferring data between services are essential for scalable, secure forms of data portability. Data portability can pose many cybersecurity challenges, even when implemented correctly, as it may increase the likelihood of attack by enlarging the number of sources of vulnerabilities for attackers to siphon user data. We encourage JPDP to further build upon this obligation. This would include specifying to what extent porting and receiving organizations would be responsible for ensuring security, particularly during data in transit.

One means of addressing concerns over data security and privacy in the context of a data portability request could be a system of accreditation or certification, based on existing global standards. To avoid introducing burdensome additional reporting requirements or double certification with this system, there should be a carve-out for entities which adhere to certain global standards (e.g. ISO, NIST, etc.).

While developing measures around right to data portability, we suggest JPDP to consider key policy and technical questions with respect to data protection and security in the context of data portability, many of which are sector-specific. Key questions include:

1. Who is responsible for providing data portability? Best practices dictate the burden should solely be on the data user.
2. What data should be freely portable?
    - Individuals should have the ability to transmit their data to different organisations. But what exactly is their data? What happens when one person wants to transfer data that is associated with another person? Who “owns” that data? How should commercially confidential or proprietary information or derived data be identified in particular sectors?
3. How should organisations protect privacy while enabling portability?
    - Does the transferring party bear any responsibility if an individual ports their data to a third party that misuses their data? Can a transferring organisation impose some baseline data protection restrictions even when carrying out a transfer to comply with a portability request. If so, which conditions or limitations of liability are appropriate?
4. When individuals’ data is transferred, who is accountable if the data is misused or otherwise improperly protected?
    - Sectoral codes of practise based on an existing global standard and that address consumer safeguards, counterparty assurance, interoperability, and security of data could help shed light on specific answers to the above challenges to implementing data portability mechanisms and provide information to individuals about the obligations on transferring and recipient organisations. The codes of practise could require entities to implement privacy and security safeguards

appropriate to particular sectors before receiving user-requested data. Compliant organisations could then be identified with a seal or other certification and would be eligible to receive data from transferring organisations pursuant to portability requests.

- Data processors should also be excluded from the data portability obligation. Data processors act on behalf of responsible data users and generally do not have visibility over individuals' data from the data subjects and would not be able to process data portability requests made by individuals. They also do not generally have direct relationships with the data subjects and are therefore unable to meaningfully or effectively communicate to data subjects directly on the porting of data.

A seal or certification associated with a code of practise could also provide users with at-a- glance information about the practises of a third party organisation, and service providers that port data to compliant recipients could be exempted from liability in the event data is misused or improperly processed following a user's data portability request.

However, if the data portability requirement is to be incorporated into the Act 709, the new provision on the right to data portability should be drafted in a specific and clear manner. A broad legal obligation to ensure data portability may be abused and hamper market development. In particular, the following points should be taken into account: -

- The scope of data subjected to the data portability requirement should be strictly limited to the original personal data fields provided by the data subject himself/herself to the data user. Other data which the data user may generate in respect of the individual pursuant to his/her use of the data user's goods/services should be explicitly excluded from the scope of the data portability requirement for clarity. The latter category of data will inevitably include valuable proprietary information and intellectual property of the data user. The requirement to transfer such data to third parties will erode the investments made by existing market players and may have the long-term effect of discouraging companies / service providers from innovating in the first place. Further, provision of such data to third parties will unlikely be helpful unless they are competitors of the porting organization, adding to our earlier point that such requirement will have the long-term effect of discouraging creation of proprietary information (and innovation).
- There should be a cut-off period for data which are subject to the data portability requirement. Data users are unable to provide/disclose data which they have destroyed in accordance with the applicable laws.
- If a data subject submits a request for a data user to port his/her personal data to a third party organization, the data user should be able to comply with the request without being required to ask for the third party's organization consent or conduct any further checks. A data user or receiving third party organization should not be required to second guess the data subject's decision provided that the data user has verified the requestor's identity and confirm that the requestor is indeed the data subject. In line with the foregoing, the data subject should have the sole right to decide to what extent he/she would like his/her raw personal data to be ported and should specify exhaustively what personal data he/she would like to be ported (i.e. all personal data he/she provided to the data user or

which specific personal details). Data users may make available a standard form to obtain all required details from data subjects who make such a request.

- The data fields to facilitate data portability should be specifically defined across all industries to facilitate adoption.
- Data subjects should assume the risk in requesting for the data porting, given that the porting organization will not have the right to audit the receiving third parties' systems or to ensure that the receiving third parties' systems have received the transmitted data in full.
- Not every company will have the technical capability to comply with data portability requirements so perhaps further studies should be conducted to consider the impact of this requirement on each industry and consider whether this should be limited to certain industries (e.g. telco, medical, insurance, etc.). To minimize friction, perhaps the JPDP may exercise its power under S21 of Act 709 to designate a data user forum for industry-specific code of practice to be issued to address this point instead of making the right to data portability a general right under Act 709.
- A data user should have the right to impose a fee on the data subject making such request in view of the time and costs the data user is required to allocate in order to process the request. Note that a fee has been prescribed for processing of access requests submitted under S30 of Act 709.

Reference: Please also refer to AIC's Submission on Singapore's Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions

C. Section 3: Recommendation on Proposal to have a Data Protection Officer (DPO)

Comments: The law can reasonably request a point of contact (or other mechanism to reach out) for the JPDP and other agencies to ask questions about privacy practices. However, the requirement to mandate the appointment of a DPO should be circumspect and clearly scoped, as it can impose significant compliance costs for SMEs and Start-ups. We recommend that any requirement for appointment of a DPO should be contingent on a data controller exercising control over some significant minimum threshold of data.

In addition, we also recommend that the JPDP provide as much flexibility as possible on how organizations decide on their appointments, including allowing for models where the appointed DPO is not physically based in Malaysia, as this does not diminish the organization's or DPO's accountability to the JPDP.

Data protection responsibilities may also be assigned to other employees or a team. Data users should also be permitted to select its DPO based on their suitability and organizational structure. It should also be made explicit that the DPO may be based outside of Malaysia and speak a language other than Bahasa Malaysia, as these factors do not diminish the organization or DPO's accountability to the JPDP. In addition, the role should not define strict requirements such as single appointment or appointment within the organization.

To recap, JPDP may wish to include guidelines around the appointment of a DPO, such as:

- Minimum threshold requirements for appointment, such as the size or the organization, volume of personal data being processed, nature of the data processing activities, etc
- Broad functions and responsibilities
- Possibility of handling it as a function (with more than one individual) vis-à-vis a singular rol
- Possibility of outsourcing the role to an external consultant
- Presence within or outside of Malaysia
- No personal liability for any violation caused by an act of the company

D. Section 4: Recommendation for a risk-based mandatory notifiable data breach framework that ensures that a reasonable timeframe is put in place for organizations to confirm that a breach had occurred before requiring notifications

Comments: With regard to the mandatory data breach notification, we favor the introduction of breach notification systems that incentivize organizations to maintain robust protections for personal data, while enabling data subjects to take action to protect themselves when their data is compromised. We believe any such system should be crafted based on the following core principles:

- ensuring that users receive timely and meaningful notifications about data breaches;
- material risk of identity theft or other economic loss;
- incorporating a risk-based trigger for the notification obligation to ensure consumers are not overwhelmed with breach notifications in instances where there is no credible risk of harm (or deferring this decision to the DPO, as under GDPR);
- providing reasonable timeframe for organizations to fully investigate the scope and potential;
- considering the impact of a breach, taking the steps necessary to prevent further disclosures, and undertaking a risk analysis to determine the extent of exposure so as to ensure that consumers receive actionable information.

Furthermore, the Act should encourage best practices in cybersecurity and incident remediation by encouraging organizations to take remedial action to ensure the data is no longer accessible (e.g. deletion), is rendered unintelligible (e.g. encryption), or is placed in a form from which individual data subjects cannot be identified. This could be achieved by clarifying that the mandatory notification requirements will not apply in these circumstances because there will be no risk of serious harm to individual data subjects.

We also recommend that data processors be excluded from direct obligations to notify either the JPDP or data subjects. Data processors often do not have visibility over the content of personal information controllers, meaning that they would not be able to distinguish between a mere security breach and a personal data breach. As such, any notification to the PDP Commissioner by the processor should be made via the controller, per existing contractual arrangements and terms of use policies.

However, if there is to be a mandatory data breach notification ("DBN") requirement, in addition to a new provision to make it mandatory for a data user to report data breach incidents, guidelines on handling data breaches should be issued. Amongst others, we recommend that:

- The notification process be simple via an online form on the JPDP's official portal. The website would need to be available for access at all times (i.e. 100% uptime) and secured from any unauthorized access/disclosure.
- The timeline for the DBN to be lodged should be reasonable and flexible (e.g. "as soon as practicable" or "as soon as feasible" after becoming aware of the incident, in line with international standards, such as the Australian and Canadian regimes) in order to give organizations adequate time to investigate and determine the scope and impact of a data breach.
- The DBN should be kept confidential until after the breach is contained or investigation is completed to avoid unnecessary panic or invite further abuse. There should also be guidelines issued by the Commission on the threshold for when affected data subjects should be informed.
- The threshold for the DBN requirement should be clearly defined to prevent the Commissioner from being inundated with DBNs. The trigger for DBN should be hinged on the potential for serious harm or risks to individuals taking into account the nature of personal data and scope of data subjects affected. For instance, it would be unnecessarily burdensome to the Commissioner (and discourage proactive conduct of penetration testing) if DBN is required for mere vulnerabilities discovered in the course of routine sweeps and via bug bounty programmes.
    - A materiality, or "harms-based" threshold ensures that regulators have visibility into actual risk posed to users, and allows regulators to focus guidance and prioritize oversight into areas most needed. A threshold that is too low could result in over-notification to the PDP Commissioner and/or individuals. For example, within the first nine months after the GDPR took effect, 64,684 data breach notifications were made to EU data protection authorities.[1]

E. Section 5: Clarity in the consent of data subject

Comments: International best practice has been to encourage and empower end users to make informed choices about their personal information by providing and promoting a robust set of privacy tools. These tools include clear explanations that allow users to modify privacy settings at a granular level based on their individual comfort levels. Organisations certainly should provide appropriate mechanisms for individual control over how personal data is processed. However, this does not necessitate a narrowly defined meaning of consent, or requiring consent at each juncture or for each activity that uses personal data.

Currently, Act 709 [s6] is practically articulated to include multiple grounds of processing including consent. Consent as a ground for processing has been defined broadly and could benefit from further clarification, which could be done either as a continuation of the same section or a separate subsection. In adding clarity to this ground, JPDP could consider including a provision on when new consent may or may not be required, the concept of deemed consent, and situations in which such consent may or may not be acceptable. However, the withdrawal of consent should not affect the processing of activities prior to that withdrawal. On the other hand, data users should also notify the data subject if the data processor has changed.

[1] International Association of Privacy Professionals, "EDPB: Authorities received 65K data breach notifications in first nine months of GDPR." May 17, 2019. Available at: https://iapp.org/news/a/edpb-authorities-received-65k-data-breach-notifications-in-first-nine-months-of-gdpr/

Requiring individuals to give consent at every step of personal data processing would be time-consuming, disruptive and result in "consent fatigue." This approach could inadvertently divert attention from the most important controls for users, without delivering corresponding benefits. In Europe, the ePrivacy Directive, colloquially known as the "Cookie Law," has been widely criticised as ineffective, as it resulted in a situation where the majority of website users would simply blindly accept or ignore popups informing them about cookies.[2]

Privacy regulations around the world recognise that different forms of consent can be valid under different circumstances. Consent can be provided in writing via a checkbox, implied by action, or by accepting a broader agreement. In some circumstances, failure to opt out could constitute valid consent. Individuals should be provided with appropriate mechanisms to exercise control that is feasible and coherent in the context of the service being provided. We urge JPDP to look at substance over form when determining if consent had in fact been given by an individual. There should be other legal basis than consent for the processing of data. Consent is a challenging concept (what happens if the user does not consent, but the data is needed for the contract or fraud detection etc. and how to handle when the data is not directly collected from the individual) and is not guaranteed to protect a user.

It may also be beneficial to set out reasonable purposes for processing personal data without the need for obtaining consent. Such an approach makes sense when companies need to process certain types of data in order to provide a service. Requiring express user consent in such scenarios would not be very meaningful because users who do not provide consent simply would not be able to enjoy the service. This can be supplemented with additional consent guidelines illustrating examples or scenarios for further clarification. For example, if a health insurance customer submits a medical claim form to their insurer for reimbursement, the insurer needs to be able to process the information regardless of whether it is sensitive and regardless of whether the customer provides express consent or has previously withdrawn consent. Similarly, for reinsurance, insurers share personal data with reinsurers to enable the provision of insurance coverage for certain high-risk applicants or issue high-value policies. For reinsurers, obtaining explicit consent directly from individual data subjects is impractical because they have no legal or commercial relationship with the data subjects. To this extent, consent to a service should be delinked from consent to direct marketing.

Furthermore, it is rare to have a one-size-fits-all solution that can take into consideration all interactions between the organization and data subject. Whereas consent may offer a robust protection of privacy, we would also recommend that JPDP provide other lawful bases for processing personal data as are currently addressed in [s6(2)]. This would allow organizations legitimately operating within the digital eco-system to process personal data without having to establish a relationship with, and collect additional data from, the data subject. It would also ensure that agencies are required to assess the basis upon which processing is taking place and ensure the standards for that ground are met.

This diversified approach is also found in other jurisdictions, such as in the EU GDPR [Art. 6] and [Art. 9] which provides six grounds for processing personal data and 10 for special category (sensitive) data. One such ground in particular – that the processing is in the "legitimate interests" of the controller (user), and does not prejudice the rights of the subject – would be a strong addition to the Act, which would also protect subjects' rights on an ongoing basis throughout the data lifecycle. Singapore is also considering amending its Personal Data Protection Act to include

[2] Different Regulators have given diverging interpretations on compliance. "ICO, CNIL, German and Spanish DPA revised cookies guidelines: Convergence and divergence," IAPP. Available at, https://iapp.org/media/pdf/resource_center/CNIL_ICO_chart.pdf

"legitimate interest" as a ground for processing. This ground would be particularly beneficial for processing data for fraud prevention purposes, as it would compel agencies continually to balance the subject's rights with those of the broader goal of preventing fraud. For example, the purpose of preventing fraud may be frustrated if individuals with dishonest intent could simply refuse to allow their transaction data to be assessed for fraud. As Malaysia moves towards a less-cash society, effective anti-fraud tools will be needed to build and strengthen consumers' trust in safe and efficient electronic payments and the overall digital economy.

These examples all show that while rules around consent remain an important feature in privacy legislation, their limitations are widely recognised. Such rules should by no means be the paramount or sole focus in new legislation.

Lastly, PDPA should recognize and enable the processing of data for a range of valid reasons, including legitimate business purposes that are consistent with the context of the transaction or expectations of consumers. Other valid purposes include processing in connection with the performance of a contract; in the public interest or the vital interest of the consumer; necessary for compliance with a legal obligation; or based on the consumer's consent. Furthermore, PDPA should not restrict organizations' legitimate cybersecurity efforts; implementation of measures to detect or prevent fraud or identity theft; the ability to protect confidential information; or the exercise or defense of legal claims.

F. Section 6 and 13: Creation of a clear framework for the transfer of personal data outside of Malaysia

Comments: We commend the JPDP for proposing a clarification that the transfer of personal data outside of Malaysia is permitted. The free movement of data underpins the modern economy – benefiting both new and traditional industries alike – and plays a fundamental role in ensuring data-driven growth and innovation. The effective and efficient functioning of data processing across borders is a fundamental building block in any data value chain. To this end, we recommend that the JPDP provide a legislative framework for cross-border data flows, that includes mechanisms to ensure data that is transferred globally and will continue to be protected to a comparable standard to if it were processed within the country. Specifically, the framework 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 to ensure that personal data will continue to be protected to the same standard, regardless of where it is transferred.

We recommend that in issuing the guidance of cross-border data transfers outside of Malaysia, JPDP consider the following:

- Elimination of the proposed whitelisted jurisdictions as listed in the 2017 order (with reasonable exceptions where there are known concerns about data security within the country)
- Recognition of existing internationally recognized data transfer mechanisms (e.g. APEC CBPR, Binding Corporate Rules, EU Standard Contractual Clauses, Certification, etc.)
- Adoption of an accountability-based model for data transfers where the data users are required to be responsible for ensuring security of the personal data transferred in compliance with the Act.

We also recommend that the JPDP align itself to best practices including the GDPR Section 46, and explicitly recognize measures that permits the flow of data including: (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 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; or (iv) the recipient has established systems and processes that comply to internationally recognized standards such as requisite ISO certifications.

Recognising a range of mechanisms to allow for cross-border data flows helps ensure that privacy legislation accommodates different business models, and helps to promote security, service reliability, and business efficiency. Privacy regulation should support flexible cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms that ensure protections follow the data, not national boundaries.

G. Section 7: Data user to implement privacy by design

Comments: We welcome the proposed implementation of the "privacy by design" concept. However, this requirement should focus on adoption of an accountability-based approach that supports the application of appropriate technical and organizational measures and safeguards into the data processing activities commensurate with the associated risks, available resources, costs, technology, etc. instead of prescriptive and onerous requirements on data users to follow and demonstrate their compliance. The "privacy by design" guideline should be made obligatory for all data users, without providing for formalistic and prescriptive requirements, such as requiring companies to submit privacy review documentation to the PDP Commissioner before any product launch. As with the scope outlined in [Art. 25] of the EU GDPR, the guideline should include explanation of this concept and various methods with illustrations on how privacy could be embedded throughout the data lifecycle of products and services. We also express support for certain protective measures, such as anonymization and encryption (for data in motion and at rest), and to this extent, any encryption standards should rely on international standards or industry practices (e.g. NIST, ISO, Common Criteria, etc.) to ensure interoperability and proper business functions.

H. Section 8: Data user to establish Do Not Call Registry

Comments: A Do Not Call Registry (DNCR) established and maintained by data users would be onerous on data users whilst having limited utility in protecting the interests of data subjects. We would recommend that JPDP look to the example of Singapore, which requires the Commission to keep a DNCR. Data users are required to check the registry before contacting any person with a "specified message."

Clarity is required on the types of unsolicited direct marketing activities (e.g. telephone, fax and/or email) that will be covered by DNCR. Section 43 of the PDPA already gives data subjects a right to require data users to cease processing their personal data for direct marketing purposes. It is not clear what additional protection a DNCR would bring to the data subjects.

I. Section 9: Right of data subject to know the third party which his personal data has been/to be disclosed to

Comments: The proposed right which will allow a data subject to request for specific third-party information that holds his personal data is not practical. The provision is problematic in the context of complex data processing operations that are commonplace in most organizations and involve the utilization of multiple third-party organizations by the data user. Many organizations rely on express notice from the data subject that personal data may be shared to authorized third parties, to which most organizations have appropriate contracts or other measures in place to protect personal information. Identifying each and every third-party data system which may hold a data subject's personal data could involve disproportionate efforts and be very difficult.

The EU GDPR's right to access also provides the option to organizations to either provide details on either the recipients or the categories of recipients to whom the personal data have been, or will be, disclosed. Such rights should also be subject to any exceptions applicable to the general access rights by data subjects as outlined in [s32] of the existing Act.

If this right must be aligned with the requirement that organizations maintain a list of all third parties to which personal data has been disclosed to (which may also need to be provided to the JPDP upon request, in the event of an inspection) , the data user should be allowed to provide the data subjects with this standard list (containing all third party disclosures) as an alternative to mapping and providing only that specific set of third parties to which the personal data (concerning the particular data subject) has been disclosed. It would also be beneficial if the categories of third parties are properly defined by JPDP.

Given the efforts that may be required in specifying each and every third party, if this right were to be expanded, we recommend that it should reasonably allow organizations to only provide for categories of third parties which process their data. Furthermore, other vendors which are already contractually obligated to an organization to only use data for that organization's purpose should not be subject to this provision.

Other points of consideration:

- Providing the list of third parties to whom the data subject's personal data has been disclosed will not be helpful to the data subjects without further context. The current S7 of Act 709 which requires data users to inform data subjects about the purposes for which the personal data is/ will be processed; and of the class of third parties to whom the data user discloses / may disclose the personal data, should be sufficient to enable data subjects to understand how their personal data is being processed.
- In most circumstances, such third party lists constitute sensitive business information of the data users. In the majority of cases, contracting parties are also subject to confidentiality requirements to not disclose their relationship to third parties. Accordingly, such requirement will put data users in a difficult position.
- Such right may be abused for the purposes of industrial espionage. Competitors may get a hand on the data user's trade secret/confidential information / commercial partners via the list of third parties which may erode any competitive advantage the data user may have.

J. Section 10: Civil litigation against data user

Comments: A private right of action which will allow data subjects to file civil lawsuits claiming damages or compensation for PDPA violations or breaches would not be an effective tool for enforcement, as such litigation may not result in recovering damages or compensation all the time. To the opposite effect, it could inevitably result in unnecessary lawsuits (without proper standing)

and pose significant costs on both the data subjects (legal fees) as well as the business. Whereas the EU GDPR provides aggrieved data subjects with private right of action, the EU privacy landscape has had years of precedents with respect to privacy violations as compared to Malaysia. To this end, we highly recommend casting off on the right to stipulate civil litigations directly by the data subjects.

Under unavoidable circumstances where a private right of action is introduced, such action should not be brought until after the JPDP has made a final decision in respect of such contravention of key privacy obligations by the data user under the Act. A similar approach has been adopted in Singapore.

K. Section 11: Supporting policies related to the security of data collection endpoints

Comments: We commend the JPDP for proposing the issuance of a policy that clarifies the importance of using state-of-the-art security techniques, including encryption of data collection end-points to increase the abilities for data users to protect the personal data they have collected. To this end, we recommend that any such policy should be regarded as voluntary or best practice, rather than mandated, given the speed at which technology progresses and the need for organizations to have the flexibility to decide the appropriate security measures to put in place in a given context. A baseline law can provide clarity, while ongoing reviews (e.g., rulemakings, published guidance, administrative hearings) can provide more flexible and detailed guidance that can be updated without wholesale restructuring of the legal framework. Governments can support these goals by rewarding research, best practices, and open-source frameworks. Creating incentives for organizations to advance the state of the art in privacy protection promotes responsible data collection and use.

We would also recommend that instead of developing guidelines on a specific topic (e.g. "endpoint security"), JPDP consider issuing broader security guidelines based on internationally recognized security standards and industry best practices and methods developed through a "privacy by design" approach for the protection of personal data throughout the lifecycle. This approach should take into consideration consumer privacy, data security, as well as a company's ability to continue to innovate to deliver efficient, cost-friendly products and services. Furthermore, regulated industries (e.g. financial institutions), should not have additional security requirements placed on them. As industry regulators are best able to ensure a calibrated approach to data security and data protection, we would instead encourage the JPDP to coordinate with the respective industry regulators to ensure there is compatibility among regulations.

We also suggest that some of the known security standards be adopted instead of creating a new one (for example, the NIST standard/ISO and etc). We look forward to collaborating further with the JPDP to discuss this issue in the future.

L. Section 12: The application of Act 709 to the Federal Government and State Governments

Comments: As Malaysia moves towards a digital economy, expanding the scope of the current Act to include Federal and State governments could make the legislation more transparent, robust and comprehensive. To this end, we welcome having one governing law instead of often duplicative regulations on how data should be collected, stored and secured.

M. Section 13: The exchange of personal data for data use with an entity located outside Malaysia

Comments: We welcome the recognition that businesses are operating internationally, particularly as Malyasian corporations and banks expand and serve end users globally. We agree that security should be the foremost concern when companies transfer data to subsidiaries or affiliates. International norms have recognized intercompany agreements as a valid mechanism to achieve this objective.

N. Section 14: Support the exemption of business contact information from compliance with the PDPA

Comments: We agree with the JPDP's proposed approach to exempt business contact information from PDPA compliance. However, as the term 'business contact information' may cover information other than personal data in a business card and name card, we propose that there be a clear definition of the term 'business contact information' within Act 709 if such term will be used. For instance, clarity needs to be given as to whether this would cover information of an individual in a directory (e.g. SSM/public company records, riders / drivers on e-hailing platforms or sellers on e-commerce platforms) published by the employer or independent partner of the individual? If so, at what point does the information start to be exempted from the requirements under Act 709?

Going a step further, in connection with this point, JPDP should also use the same opportunity to clarify whether; if it can be proven by the data user that the personal data was obtained from publicly available sources (for whatever reason), will the use of such personal data by the data subject be exempted from Act 709?

We also agree that it is important to consider the risks of how business contact information could be misused for purposes other than to carry out and facilitate business interaction. In this regard, we recommend that the JPDP make clear in its implementation and guidelines: (i) the sources of business contact information (e.g. information on a business card) and (ii) that the exemption would not apply when the business contact information is used for business-to-consumer purposes (e.g. direct marketing to an individual subject). (iii) Purpose of use of business contact information (e.g. where it is used as part of business activities, exceptions for use for personal purpose)

O. Section 15: Disclosure of personal data to government regulatory agency

Comments: Where disclosure of personal data to a government regulatory agency is required, standard protocols for acquiring data (e.g. subpoena) should be followed, and any corresponding court orders should be produced with clear indication of intent. We also caution against introducing any "back door" requirements as whenever an ability to override a security measure to access data in an authorized manner is maintained, it brings about the possibility of being exploited by a bad actor in an unauthorized manner. We recommend that the JPDP include the following areas for consideration in any subsequent guidelines:

- Circumstances in which such requests can be reasonably made, similar to that specified in [s39(b)]
- Data security practices and applicable regulatory requirements which would ensure the protection of such personal data by public sector agencies
- Guidance on responding to foreign government and/or law enforcement requests
- The right to appeal in case of any grievances
- Exceptions to the requirement

P. Section 16: Class of data user based on business activity and Section 17 Voluntary Registration

Comments: The requirement to register a broad class of data users would not necessarily improve data protection standards or compliance in Malaysia. Currently, the registration requirement under the Act entails mandatory registration for 13 categories of data users with the JPDP. However, we find this approach ineffective as the registration procedure described in the Act is intense and could impose unnecessary costs and burdens on businesses, without resulting in any real privacy benefits to data subjects. Further, the current data user categories potentially disregard some important sectors such as e-commerce, fast-moving consumer goods, etc. which also handle a significant volume of personal data.

In line with global privacy laws, the broad intent should be to ensure that the data users are aware of their data processing activities. Currently, the ICO requires organizations to mandatorily register if they have any function processing personal data (subject to exemptions) by payment of the applicable fees (subject to a number of factors including number of staff, annual turnover, status of the organization, etc.). The registration procedure is light-touch with payment of the fees and organizations are responsible for maintaining the records of processing activities. Unlike the Act, the burden is not on the Commissioner (ICO) to review if the processing activity and other information warrants a certificate or registration or not.

We recommend that the registration requirement is made voluntary for all data users and instead, all organizations processing personal data should be required to maintain records of their data processing activity similar to the requirement under the EU GDPR. This would also be in line with global best practices and take off a considerable burden away from both the JPDP as well as organizations.

Q. Section 18: The application of Act 709 to non-commercial activity

Comments: If it is intended for Act 709 to cover all charities and religious activities, we would recommend stating so instead of using the broad term 'non-commercial transaction' which may be interpreted to cover any activity. If the intention of this proposed revision is indeed to cover all non-commercial transactions, the need to conduct training on Act 709 to the public at large should be considered.

R. Section 19: Retaining current applicability of the PDPA to only data processed in Malaysia

Comments: Data protection law should hew to established principles of territoriality, regulating businesses to the extent they are actively doing business within the jurisdiction. Extra-territorial application is not recommended, as enforceability on foreign entities 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 entities and ultimately detract from the aim of privacy laws to protect personal data.

Extra-territorial application unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions. In particular, small businesses shouldn't have to worry about running afoul of foreign regulators merely because a few people from another country navigate to their website or use their service. This is unnecessarily burdensome and in fact poses as a barrier for small businesses to engage in cross-border digital trade.

Instead, the law should contemplate interoperability with global norms. This will make it less onerous to operate businesses regionally or globally, and will demonstrate a modern approach to governing data protection. Trade agreements increasingly focus on addressing regulatory fragmentation by encouraging adherence to or alignment with regional data protection standards, while preventing restrictions on cross-border data flows. The USMCA Agreement, for instance, references the APEC CBPR. By focusing on interoperability rather than extra-territorial reach, governments can reduce barriers to cross-border digital trade and ensure that small businesses have the opportunity to participate in the global digital marketplace.

Furthermore, a provision similar to Art 22(1) of the GDPR may not be the best solution in tackling such concern given that the said Art 22(1) is aimed at regulating a very specific type of processing, that is, a processing activity which is wholly automated and leads to decisions that impact on individuals in a sufficiently significant (adverse) way (e.g. automatic refusal of an online credit application) and providing the data subject with a chance to reject such automated processing and to request for human involvement instead.

Perhaps a better alternative in tackling the concern about the processing of Malaysians' personal data outside of Malaysia is to ensure secured cross border transfer of personal data as discussed under item 6 of this Public Consultation Paper No. 1/2020 and to issue guidelines on the recommended security standards to be deployed in such circumstances, as discussed above.

S. **Section 20: Data users to provide a clear mechanism on the way to unsubscribe from online service**

Comments: Clarification is needed on the scope of "digital or electronic marketing" that the guideline proposes to cover. For example, does it include marketing communication sent through email, SMS, fax or telephone only or it covers something more which is not yet captured in the PDPA. Likewise, clarification is required on what types of "online service" that the guideline proposes to cover.

Clarity should be provided on the followings:

- Scope of direct marketing (e.g. use of different marketing channels (calls, SMS, e-mail, etc.)
- Individuals' rights (e.g. access, opt-out/withdrawal, objection, etc.)
- Exemptions to the requirement
- Use of personal data for sale or data brokering services in relation to direct marketing.
- Definition of "online services"

Guidelines on processing of personal data for digital and electronic marketing would be useful, especially if it includes:

- guidance on the information to be provided to data subjects after they opt out, if any;
- a clear definition of the term digital/electronic marketing – would it cover marketing information conveyed via online calls; and
- guidance on the consent required for opt-in and whether it makes a difference if the marketing message sent electronically is targeted at the recipient (instead of a marketing email sent to the public at large). If yes, care should be taken to ensure that there is no overlap with the guidelines on direct marketing (if such guidelines will be issued) or inconsistencies.

Data users should have the right to determine the methods by which they give data subjects the ability to unsubscribe from direct marketing. This most effective method will depend on the nature of the marketing (e.g. email vs text message). The JPDP should avoid prescriptive requirements around unsubscribe options and should instead focus on technology-neutral principles (e.g. that the option be easily accessible by data subjects).

T. **Section 22: Processing of Personal Data in Cloud Computing**

Comments: We commend the JPDP for its proposal to provide clarity on the processing of personal data in cloud computing. As reflected in the Consultation, Cloud Computing offers significant cost savings, flexibility and agility and allows for innovation. This is particularly true for the many Malaysian businesses leveraging the cloud to build, digitize, secure, and scale their business.

Crucially, cloud computing also provides companies access to state-of-the-art security solutions and secure infrastructure. That said, data breaches do occur, even when organizations use the cloud – this could sometimes be because organizations are unaware of the full suite of security features on

the cloud and may not be able to design their solutions or deployments to meet their security needs.

To this end, we recommend that the JPDP clarify for organizations using the cloud, how to identify the appropriate service providers to meet their security needs. For example, by aligning recommendations to international standards like ISO 27018 (PII on public cloud) instead of creating some new requirements in the to-be-defined guideline on usage of cloud computing for data users. ISO/IEC 27018:2019 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO/IEC information security standard 27002 and provides implementation guidance on ISO/IEC 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

We also recommend that the JPDP clarify that cloud service providers (CSPs) are data processors and are not regulated differently from any other data processor. This would be in line with international norms, which treat CSPs as a data processor. Enterprise users of cloud services (i.e. enterprise customers) are data controllers. The CSP only processes the data in accordance with the instructions from the data controller.

As a standard practice, the CSP, as a data processor, has contractual clauses with the cloud business user. The cloud customer is ultimately responsible for the security of their collected data. The CSP may provide basic security technologies, which can be further configured by the customer. The CSP has very limited visibility into the data practices or security events of an individual customer.

We are of the view that specific guidelines on use of cloud computing are not necessary, as:

- It should be sufficient if the cloud service providers (as data processors) are made directly responsible to ensure compliance with Act 709.
- There are existing guidelines on cloud storage services such as the technical code entitled 'INFORMATION AND NETWORK SECURITY - CLOUD SERVICE PROVIDER SELECTION' issued by the Malaysian Communications and Multimedia Commission which provide guidelines as to what to look out for when engaging a cloud service provider.
- Regardless, if such guidelines are to be issued, we propose that the guidelines merely set out the general requirements and provide flexibility for data users to implement the most practical mechanism to ensure compliance with the guidelines.

We would also be keen to offer our further support and collaborate with the JPDP in its development and refinement of its cloud guidelines.

PART II – ABOUT YOU

i) Name: Sarthak Luthra

ii) Email address: secretariat@aicasia.org

iii) You are commenting as:
(Please mark ✓ in the third column given)

No.	Respondent category	✓
1	**Data subject** (individuals who are the subject of the personal data)	✓
2	**Registered data user** (data user which belong to the 13 classes of data users)	
3	**Unregistered data user** (any person that process personal data but does not belongs to the 13 classes of data users)	
4	**Data processor** (any person that process data solely on behalf of the data user)	

iv) If you provide comments as no. 2, 3 or 4, please state your organisation's name:

N/A

v) If you provide comments as no. 2, please state your data user's sector (from the 13 classes of data user):

N/A

vi) If you provide comments as no. 3 or 4, please state your organisation business's sector:

N/A