

Asia Internet Coalition (AIC) Industry Submission on The Draft Digital Personal Data Protection Bill, 2022

20 December 2022

To,

Shri Ashwini Vaishnaw

Hon'ble Minister of Communications; and
Electronics and Information Technology
Ministry of Electronics and Information Technology
New Delhi, India

Cc:

Shri Alkesh Kumar Sharma

Secretary, Ministry of Electronics and Information Technology

Shri Amit Agrawal

Additional Secretary, Ministry of Electronics and Information Technology

The Ministry of Electronics and Information Technology (**MEITY**) has introduced the latest iteration of the country's data protection law, titled the '[Digital Personal Data Protection Bill, 2022](#)' (**DPDP Bill**), for public consultation. In this regard, I write to you on behalf of the [Asia Internet Coalition](#) (**AIC**) to acknowledge and appreciate the efforts of the MEITY in re-formulating the DPDP Bill with forward-looking provisions that are at par with global best practices and standards. It is truly commendable that the MEITY accounted for inputs it received during previous consultations while formulating the DPDP Bill.

AIC is an industry association comprising leading internet and technology companies. We seek to promote technology and policy issues in the Asian region, and we are fully committed to the cause of safe and open internet. In this capacity, we take the opportunity to provide inputs with respect to the DPDP Bill to highlight key concerns before the same is introduced before the Parliament of India for deliberation and enactment. We believe that this will go a long way in strengthening the country's data protection law and will ensure that the same contains holistic provisions. It will also help further the goal of achieving a 'Digital India.'

The DPDP Bill, 2022, like its predecessors allows the central government to exempt any of its entities from the Bill on grounds like the security of State and public order. This would give the notified government instrumentalities immunity from the application of the law, which could result in immense violations of citizen privacy. This is because these standards are excessively vague and broad, therefore open to misinterpretation and misuse. If the law is not applied to government instrumentalities, data collection and processing in the absence of any data protection standards could result in mass surveillance. Any exemption sought by government agencies should be granted only if they fulfil the standards of legality, necessity, and proportionality. It is essential that government collection and processing of citizen data is

regulated to prevent misuse of use. In addition, the DPDP Bill, 2022 mentions the phrase ‘as may be prescribed’ 18 times. This is symbolic of the vague and unchecked powers that the Union Government has retained for itself to frame rules at a later stage in the absence of legislative guidance.”

Please see below our key concerns on the DPDP Bill.

1. Regulating cross-border transfer of personal data:

- Since the DPDP Bill does away with sub-categories of personal data, Clause 17 governs the transfer of all forms of personal data outside India. As per this, the Central Government is empowered to (after accounting for necessary factors) notify countries outside India to which data fiduciaries may transfer personal data. However, such transfer will have to take place in accordance with the terms and conditions that the Central Government may eventually specify. While this provision has substantially simplified the framework governing cross-border data transfers, we believe that the MEITY ought to provide further clarity in the final version of the draft law and also account for certain factors – as highlighted below. We would hope that Government further clarifies the following information before the Bill is put into operationalization:
 - The timeline it has in mind for notifying such countries. Until such countries are notified, this provision of the Bill should not be operationalized.
 - The criteria for notifying countries/ territories remains unclear

Comments and suggestions:

- Clause 1(2) of the DPDP Bill stipulates that different provisions may come into force on different dates – as may be appointed by the Central Government. In this regard, we urge the MEITY to, at the very least, ensure that Clause 17 is only enforced after countries or territories to which personal data can be transferred outside India have been notified. This will ensure regulatory certainty for all stakeholders – especially those whose businesses rely on cross-border data flows, as well as ensure that they have sufficient time for comply with applicable requirements under the law.
- Another feasible model is that the MEITY may consider is devising a list of countries or territories to whom personal data cannot be transferred, for example, after accounting for factors that indicate that such countries may be unsafe for the purpose of transferring personal data of Indian citizens. This model would enable data fiduciaries to continue to transfer personal data outside India to those countries that are not on this prohibited list. A carve out may also be created within this list for data fiduciaries that provide global services – i.e., they may be permitted to transfer personal data to countries on the prohibited list (especially if they cater to individuals in these countries as well), as long as they ensure adequate data privacy and protection measures.
- An additional concern regarding Clause 17 is that it does not prescribe timelines within which data fiduciaries will be required to comply with the terms and conditions of transfer that the Central Government may eventually specify, or the timelines within which data fiduciaries will be expected to stop transferring or storing data in countries that are not approved by the Central Government. It is essential to ensure that stakeholders have

adequate time to comply these requirements – as and when introduced – to ensure that the same do not unduly increase the regulatory burden on them. In addition, in the event the MEITY introduces any kind of regulatory approval requirements under terms and conditions introduced under Clause 17, it will be essential to ensure that there are timelines in place within which such approvals will be granted to data fiduciaries, so as to not leave them in a lurch and adversely affect their cross-border business operations.

- Lastly, we would like to highlight our concern with a potential scenario that may arise under the DPDP Bill – i.e., data fiduciaries being based in countries that are not permitted by the Central Government for the purpose of cross-border data transfers. In line with global frameworks, such as the E.U.’s General Data Protection Regulation (**GDPR**), relaxations ought to be granted to data fiduciaries that find themselves in such a situation. This is especially important if personal data transfers are considered necessary for providing services, adhering to contractual obligations owed to a data principal, for public interest purposes, or even participating in international data transfer frameworks or trade agreements. For this purpose, stakeholders ought to be able to rely on intra-group transfer schemes (for transfers within the same entity) or standard contractual clauses (for transfers to different entities) for transferring personal data to non-permitted jurisdictions.
- To summarise our key suggestions, we recommend that the MEITY consider the option of providing a negative list of countries where personal data cannot be transferred – thereby allowing data fiduciaries to transfer data to other countries not on this list. Sufficient time ought to also be provided for data fiduciaries to comply with all allied requirements under Clause 17 (such as terms and conditions for the transfer, etc.) – irrespective of whether the MEITY introduces a positive list or negative list of countries. Additional exemptions (as discussed above) may also be introduced in the interest of ease of doing business.

2. Notice

As per Clause 6(2) of the DPDP Bill, where a data principal has given consent to the processing of her personal data prior to the commencement of the DPDP law, the data fiduciary is required to provide an itemized notice in a clear and plain language containing a description of the personal data collected and the purpose for which such data has been processed, as soon as it is reasonably practicable.

This requirement should apply only 'prospectively' since data fiduciaries may or may not have maintained records of the purpose of the processing of personal data in the past in the absence of a law requiring this.

3. Introducing secondary grounds of processing:

We note that under the DPDP Bill – especially Clause 7 thereof – consent continues to remain the main ground for processing personal data. The DPDP has also introduced the concept of ‘deemed consent’ under Clause 8 of the DPDP Bill for processing personal data for specific purposes, including that of ‘public interest’. Under the ‘public interest’ ground, the Central Government is empowered to prescribe fair and reasonable purposes after considering factors such as “whether the legitimate interests of the data fiduciary in

processing data for that purpose outweigh any adverse effect on the rights of the data principal.” In this regard, we have the following comments.

4. Comments and suggestions:

- Global frameworks – such as that of the GDPR – enable the processing of personal data on certain secondary grounds, without obtaining consent from the concerned data principals. These grounds include contractual necessity and legitimate interests. While the DPDP Bill does envisage legitimate interests as a ground for processing data vis-à-vis deemed consent, it leaves the determination of the same to the Central Government.
- The non-inclusion of contractual necessity as a ground of processing personal data without consent (or by assuming deemed consent) may lead to a scenario where consent has to be taken from data principals during every stage of processing their personal data, even if done in pursuance of contractual obligations. This can lead to consent fatigue and cause data principals to resort to giving meaningless and uninformed consent as a matter of routine. It may also have the unwarranted effect of preventing data fiduciaries from processing personal data that is considered necessary prior to entering into a contractual relationship with data principals.
 - It is worthwhile to note that even the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 recognizes contractual necessity as a ground basis which sensitive personal data can be transferred or disclosed to third parties without additional consent.
- Regarding the legitimate interests of a data fiduciary – as noted above – the Central Government has the power to decide whether legitimate interests of a data fiduciary form part of fair and reasonable purposes for processing personal data without consent. The DPDP Bill does not stipulate whether the regulators will consult with the concerned stakeholders before introducing such a ground. We believe that legitimate interests ought to be introduced as a stand-alone ground, and data fiduciaries should be allowed to self-determine whether processing of personal data without consent/basis deemed consent is in their legitimate interest. This will make compliance easier and more flexible, as well as improve the ease of doing business in India. It will also help prevent a situation where data principals are not only approached each time their consent is needed to process data for legitimate business reasons but are also able to unilaterally withdraw consent for data that is crucial for the processing activities of a data fiduciary.
- Lastly, Clause 8(2) of the DPDP Bill can be revised so that processing on the basis of deemed consent and for the performance of any function under law or the provision of any service or benefit to a data principal is made applicable to non-State actors as well. We believe that this can, among other things, go a long way in promoting innovation and the development of new and emerging technologies across a plethora of sectors.
 - To summarise our key suggestion, we believe that the MEITY ought to consider incorporating contractual necessity and legitimate interests of a data fiduciary as standalone grounds for processing personal data under Clause 8 of the DPDP Bill.

5. Processing of children's personal data:

- We note that the DPDP Bill, in line with previous iterations, continues to define a child under Clause 2(3) as someone below the age of 18 years. Interestingly, Clause 2(6) also defines a data principal to include a child's parent or legal guardian vis-à-vis their child's personal data.
- Clause 10 of the DPDP Bill contains additional obligations regarding processing of children's personal data. These include obtaining 'verifiable' parental consent (in a manner as may be prescribed by the Central Government), not undertaking tracking or behavioural monitoring of children, and not targeting advertisements directed at them. As per Schedule 1, failure to comply with these obligations can lead to the imposition of financial penalties up to INR 200 crores. In this regard, we have the following comments.

Comments and suggestions:

- With regard to the age of consent under the DPDP Bill, while this is in line with the age of majority prescribed under the Indian Majority Act, 1875 and the fact that minors are not considered as competent to contract under the Indian Contract Act, 1872, it is at odds with global best practices. It also does not acknowledge the autonomous development of children above a particular age. For instance, the United States and European Union recognize the varying levels of maturity of young adults and teenagers while laying down the age of consent.
 - While competency to enter into a valid and binding contract may be an important consideration as individuals may be required to have a certain degree of maturity and understanding – the same does not necessarily apply to obtaining consent for processing personal data. The maturity of the modern-day child ought to be accounted for while affixing the age of consent under a niche law such as the DPDP Bill. This will be in line with other domestic laws, albeit in the labour law field – such as the Factories Act, 1948 and the Apprenticeship Act, 1961 which largely permit children above 14 years of age to be employed in factories or engaged as apprentices.
 - Requiring parental consent for children below the age of 18 years may result in a situation where many children are prevented from accessing online beneficial services – such as if their parents unilaterally withhold consent, do not agree with their child's needs or requirements to access a particular online service, or simply do not have the adequate amount of digital literacy to understand why their consent is crucial for their child to access an online service.
 - An age-gate of 18 years may inevitably also prevent data fiduciaries from offering critical and beneficial services to children in order to avoid regulatory complexities and compliance hurdles. This may, in turn, prevent children from accessing especially those services that have been designed for them (such as ed-tech services).
- In addition to the above, the mechanism for obtaining 'verifiable' parental consent has not been delineated under the draft law. The same is left to the rule-making powers of the Central Government. We urge the MEITY to reconsider this provision – and instead,

empower data fiduciaries to develop their own internal consent or age verification mechanisms. This will not only ensure that data fiduciaries have the flexibility to arrive at such mechanisms, keeping in mind the nature of their services, platform interface, etc. Alternatively, the MEITY can also encourage data fiduciaries to collaborate and develop industry standards on carrying out age verification, etc.

- Once verification has been carried out / parental consent has been obtained – the DPDP Bill may also be amended to include a provision ensuring that data fiduciaries will be exempt from liability arising out of processing of a child’s personal data.
- Another point to keep in mind is that the requirement to obtain verifiable parental consent prior to processing children’s personal data may, in effect, require data fiduciaries to verify the age of all their users (irrespective of whether they provide services to children) to determine which users to obtain parental consent from. This will not only go against the principle of data minimization but will entail significant compliance costs.
- The overall prohibitions on monitoring, profiling and targeted advertising should also be reconsidered by the MEITY. This is because the bar on monitoring or tracking children may lead to a scenario where data fiduciaries are unable to undertake tracking or beneficial monitoring of children to deter online harm and ensure their online safety, or to even offer safety features specifically designed to keep children safe online. Similarly, a bar on issuing targeted advertising may prevent data fiduciaries from offering age-appropriate and beneficial content and services to children (such as those relating to mental health, education, physical well-being, etc.).
 - To summarise our key suggestions, the MEITY ought to reconsider the age of consent under the DPDP Bill – and 13 years may be considered as a feasible option, in line with global standards. As regards the requirement to obtain parental consent – data fiduciaries should be empowered to develop internal mechanisms / industry standards regarding the same. Lastly, tracking, monitoring, etc. ought to be permitted if done in the best interests of a child, and as long as the same is age appropriate.
 - We suggest that reliance on self-declaration of age is limited to circumstances in which the personal data processing is low risk or self-declaration of age is used in combination with other techniques. For children younger than this age group, the government could look at prescribing verifiable parental consent. This will allow the children in the age group of 13-17 years with sufficient autonomy as they look to define and shape their digital experiences. Any other age assurance solution must also involve implementing privacy by design principles at the initial development stage to proactively protect minors while not disproportionately deterring users or potentially compromising anonymity.
 - Further the means and form of obtaining parental consent has not been defined. We are concerned that this should not become a condition wherein significant data fiduciaries are asked to onboard government identifications of users. Key to the protection of privacy and data is the concept that when seeking to protect a person’s privacy or data, additional privacy or data protection risks should not be created.
 - Finally, the Bill should be revised to contain certain exceptions for when profiling and tracking are in the best interest of the child or when necessary to provide the digital service. Lastly, given that the Bill puts restrictions on processing of personal data in

areas that are likely to cause harm to a child, it should clearly define what such harmful conditions could be.

6. Consent Managers

The Bill defines consent managers as an entity that is accountable to the Data Principal and acts on behalf of the Data Principal. The Bill further adds that every Consent Manager shall be registered with the Data Protection Board in such manner and subject to such technical, operational, financial, and other conditions as may be prescribed.

Comments and suggestions: Where a data fiduciary provides its own consent management tool, this should not apply. To integrate third party solutions would be burdensome to do for businesses and be confusing for data principals to understand. Consent managers should be considered as potential solutions or service providers to data fiduciaries that do not have their own consent management systems.

Moreover, consent manager services should be approached carefully as they could potentially become weak points that can be exploited by potential attackers who can modify a person's consent. In many cases, the operators of consent services do not have the data privacy and security infrastructure of more established companies and thus forcing the established companies to integrate these providers creates a risk to data principals.

7. Incorporating a co-regulatory model under the law:

- The earlier iterations of the DPDP Bill envisaged the implementation of 'codes of practice' to promote good practices of data protection and facilitate compliance with the law. Further, codes of practice could be issued for a whole host of obligations under the law. We believe that the absence of such a provision from the DPDP Bill may not be in the best interests of the internet ecosystem.

Comments and suggestions:

- Given that technology and the services that rely on the same are constantly evolving, co-regulatory systems akin to 'codes of practice' will ensure that data fiduciaries operating or offering services within India are able to comply with the requirements under the DPDP Bill with ease. Implementing codes of practice will also ensure that the same can be amended, as and when required – such as in order to keep pace with changing and newer forms of technologies – without having to go through the cumbersome process of amending the law itself.
- To summarise our suggestion, we request the MEITY to re-introduce a provision on codes of practice, in the interests of promoting co-regulation.

8. Section 9(5) (Obligation to Notify in case of Data Breach):

- Ideally, the obligation to notify data breaches should be limited to informing the Board and upon the Board requiring notification to the data principals depending on the severity of the issue or the likely impact upon the data principals, they may be informed. Even if data principals are to be informed at the first instance, this should be limited to situations where certain action is required on part of the data principal for security, such as changing passwords.
- It appears from the wording of the provision that the data fiduciary and data processor can contractually determine which of the two will be responsible for breach notification depending on at whose end the breach occurred..... (TCG seems to have a slightly different view on this point)
- Currently, reporting obligations in case of “cyber security incidents” exists under the Information Technology CERT-In Rules (as amended recently). Under the Information Technology Act, 2000 (“IT Act”), CERT-In, which is the nodal body empowered to deal with cyber security issues, has the power to issue guidelines, directions, etc. to entities in response to cyber security incidents. On a similar note, the proposed DPDP law also empowers the Board to direct data fiduciaries to adopt urgent measures to remedy personal data breaches or mitigate the harm caused to data principals.

Therefore, in cases of incidents reportable under both laws, an entity may need to not only report the breach to two statutory bodies but may also need to comply with directions issued by two separate bodies. Additionally, the question arises if the Board will have the expertise to understand the complexity of data breaches to be able to issue measures that will help remedy a breach or mitigate harm.

9. Data Protection Board is not independent

The Bill proposes the establishment of a Data Protection Board to ensure compliance with the Act. “The strength and composition of the Board, the process of selection, the terms and conditions of appointment and service, and the removal of its Chairperson and other Members shall be such as may be prescribed by the Union Government at a later stage. Further Clause 19(3), the Chief Executive of the Board will be appointed by the Union Government. These provisions continue the disappointments of previous iterations as the Data Protection Board (DPB) still does not have the independence needed to sufficiently protect the interests of Data Principals,” IFF noted. “Since the DPB will oversee compliance to the provisions of the legislation by the private sector as well as government agencies, it is pertinent that the board be fundamentally independent from the executive’s control,” IFF added.

10. Requirements relating to Data Protection Officers:

- Under Clause 11(2) of the DPDP Bill – significant data fiduciaries (SFDs) are required to appoint an officer known as a ‘Data Protection Officer’ (DPO). Among other things, the DPO has to be based in India. While we note that this requirement may have been introduced to ensure a DPO’s availability for communication and timely redressal of grievances – we request the MEITY to reconsider this requirement. We say so for the following reasons.

Comments and suggestions:

- This requirement seems unnecessary as it poses additional costs for hiring an in-country data protection officer without any consequent advantages to effective data protection. Moreover, where the processing in fact occurs outside of India it is critical that the Data Protection Officer be near where the processing is being done so that they can operationalize the requirements of the Bill. Indeed, placing a data protection officer in India while processing occurs in another country, would effectively be meaningless if the goal is to protect the Indian principal's data where it is being processed.
 - **Authorities across Europe have recognised this reality and do not require the data protection officer to be located in the country.** Instead, they require that the data protection officer **be easily and readily accessible** both to the authorities and principals, which can be achieved effectively in other ways.
 - Many data fiduciaries that offer services in India have one global DPO responsible for compliance with legal obligations across various jurisdictions. Even if data fiduciaries have local DPOs, they are often required to communicate and coordinate with their global counterparts – as and when required. Thus, we apprehend that the requirement to have a DPO based in India may not serve any beneficial purpose. The possibility of imposition of penalties under the DPDP Bill for failure on account of a DPO to undertake their functions is, in any case, sufficient to ensure compliance.
- To summarise our suggestion, we urge the MEITY to reconsider the requirement of DPOs being based in India. The grievance redressal requirements under the DPDP Bill can be equally met by DPOs situated abroad.

11. Reconsidering the requirement to conduct audits:

- Given that the DPDP Bill has retained the concept of significant data fiduciaries (SDFs), it seeks to impose additional obligations on them. Over and above the requirement to appoint a DPO, there is also the requirement to appoint an independent auditor, conduct data protection impact assessments, and undertake periodic audits – as per Clause 11(2).

Comments and suggestions:

- We believe that the objective behind conducting periodic audits is subsumed vis-à-vis the requirement for independent auditors to assess compliance with the law, as well as the carrying out of data protection impact assessments. In particular, impact assessments may be sufficient to assess whether any harms exist to data principals with regard to processing activities of SDFs and determining the best ways to remedy these harms.
 - We are concerned that in the event periodic audits are carried out by third party auditors, the same may expose the personal data records stored by SDFs to potential data breaches or leaks, assuming data auditors will have to access the same in order to carry out audits.
- To summarise our suggestion, we believe that to ease the compliance burden on SDFs, requirements such as conducting periodic audits may be reconsidered. Separately, we request the MEITY to reassess whether there is a legitimate need to create a separate

carve out for SDFs, given that the obligations of regular data fiduciaries and SDFs are largely similar.

12. Data breach reporting obligations

- In addition to the term ‘personal data breach’ being defined in a broad manner, we note that under Clause 9(5) of the DPDP Bill, data fiduciaries / data processors have to notify the Data Protection Board and each affected data principal of a personal data breach. This reporting requirement does not prescribe impact thresholds and also overlaps with reporting requirements under other laws. We have elaborated on the same below.

Comments and suggestions:

- As per the DPDP Bill, it appears that each and every kind of personal data breach has to be reported. Such broad-based reporting may not only flood the Data Protection Board with excess information but may also cause undue distress to data principals (for example, if a breach is reported to them even if no actual harm or risk occurred). It is important for the law to prescribe minimum impact and harm thresholds that will guide stakeholders, while determining when and whether to report a personal data breach to the regulator, and if a high enough level of risk has accrued to a data principal to entail reporting to them.
- In addition, this requirement overlaps with the cyber-incident reporting requirements under the Information Technology Act, 2000 read with the applicable rules and directions issued thereunder. Since the Indian Computer Emergency Response Team expects cyber-incidents such as data breaches or data leaks to be reported to it in a specific format and within specific timelines, a dual requirement under the DPDP Bill may increase the compliance burden on data fiduciaries and data processors, without resulting in any added benefits. Accordingly, we request the MEITY to reconsider the provision on reporting personal data breaches under the DPDP Bill. Alternatively, the law can mandate stakeholders to report incidents to only one regulator (which can then report it onwards to its counterpart) and in a uniform format.
 - To summarise our suggestion, we request the MEITY to reconsider the requirement to report personal data breaches to both the Indian Computer Emergency Response Team, as well as the Data Protection Board. If the requirement to report breaches is retained, the law ought to contain impact thresholds that guide entities in assessing whether to report an incident.
 - The government should consider defining ‘grievance’ similar to the Information Technology Act - Intermediary Guidelines for clarity on the types of grievances that can be registered.
 - The time period of 7 days appears very less. It is unclear in which instances a shorter timeline (shorter than 7 days) may be prescribed.
 - The roles of the Data Protection Officer (under DPDP) and Grievance Officer (under the IT Act) should be delineated for clarity and independence of the grievance redressal mechanism.

13. Other issues:

- **Consultation for subordination legislation:** We note that the exact details and contours of various provisions under the DPDP Bill have been left to subordinate legislation. We request the MEITY to ensure that it undertakes adequate stakeholder consultation prior to adopting subordinate legislation, as this will ensure that the same is holistic and accounts for concerns across the digital ecosystem. To alleviate concerns in this regard, the MEITY may consider incorporating language within the DPDP Bill that mandates the Central Government to undertake public consultation prior to arriving at rules or regulations under the draft law.
- **Express transition period:** While Clause 1(2) of the DPDP Bill stipulates that the Central Government may appoint different dates for the enforcement of different provisions, we request the MEITY to incorporate an express transition period under the draft law. This will provide all impacted stakeholders with adequate clarity to plan and implement their compliance obligations. A transition period will also be in line with the recommendations of the Joint Parliamentary Committee, as well as global frameworks such as the E.U.'s General Data Protection Regulation, and Digital Services Act that have provided a 2-year transition period.
- **Subject Access Rights:** While we have no issue with the introduction of general subject access rights like deletion etc, the Bill does not provide a timeframe by which organizations have to comply with such requests. Some of the examples include the lack of deadline for deleting personal data, lack of timeline for the Board to adjudicate on a complaint, no deadline for the data fiduciary to erase personal data once the intended purpose is served, etc.
- **Processing personal data of foreign nationals:** Clause 18(1)(d) of the DPDP Bill provides certain exemptions for data processors in India processing personal data of data principals residing overseas. However, it does not provide a similar exemption for data fiduciaries in India that are involved in processing personal data of data principals that are abroad. The MEITY may consider incorporating such an exemption to account for scenarios where a data fiduciary in India provides services to foreign nationals and processes their data – especially in light of Clause 17 of the DPDP Bill and to account for instances where a foreign national may be located in a country that is not approved by the MEITY.
- **Prescription of Rules:** For a company to be able to maintain and strengthen its data protection frameworks, consistency and predictability are important prerequisites. The Bill allows for ambiguity and uncertainty, given that the Central Government maintains the power to notify rules at a later stage. This includes issues such as processing personal data, form and manner of reporting data breaches, the composition, qualifications, and selection of members of the Data Protection Board (DPB), among others.

Our recommendation is that these criteria should be collectively developed with inputs and feedback from the industry. Until such time these criteria are not developed, the Government should hold the implementation of the Bill.

- **Section 29 (Consistency with other laws):** The Bill states that in the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict. There are sectoral laws where there may be provisions contrary to the DPDP law. e.g. Reserve Bank of India has mandated payments data localization but under Section 17 of the DPDP Bill cross border data transfer may be permissible. This may create confusion in terms of compliance. Hence, clarity is required in this regard.
- **Section 30 (Amendments):** Once the DPDP Bill is enacted, Section 43A of the Information Technology Act (this provision provides for the compensation for failure to protect data, and specifically, the SPDI Rules have been enacted for this purpose) will be omitted. The Bill, however, does not explicitly repeal Section 72A of the Information Technology Act, which prescribes a penalty (including imprisonment and fines) for service providers disclosing personal information about a person without their consent, or in breach of contract, with intent to cause, or knowledge that such breach is likely to cause wrongful loss to the person, or wrongful gain to the service provider. The Government may consider repealing this provision as well and consolidating all prohibitions under the DPDP law.
- **Timelines for Implementation:** The DPDP Bill states that “The Bill shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint. It further adds that different dates may be appointed for different provisions of this Act. It would be very beneficial if the government clearly defines a timeline for different provisions of the Bill. This will allow companies to plan better and accordingly work towards ensuring compliance with the provisions of the Bill

In conclusion, AIC would, once again, like to express gratitude to the MEITY undertaking a thorough exercise in revising the DPDP Bill. We look forward to engaging in constructive discussion on the issues highlighted by us, before the draft law is introduced before the Parliament.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,



Jeff Paine

Managing Director

Asia Internet Coalition (AIC)