16 December 2022

Government of India
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003

Via Online Submission

Subject: Draft Digital Personal Data Protection Bill, 2022

Dear Ministry of Electronics and Information Technology:

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity from the Ministry of Electronics and Information Technology (the "Ministry") to provide additional feedback on the draft Digital Personal Data Protection Bill, 2022 (the "Bill"). In March 2022, SIIA joined other organizations in providing input on an earlier version of the Bill, and we appreciate revisions made by the Ministry since that time.[1] We write to provide additional suggestions that we believe will help to strengthen the Bill and achieve the Ministry's overarching objectives.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 600 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services. Our members are unified in their support for policy measures that promote a robust, healthy digital ecosystem and information lifecycle worldwide.

We commend the Ministry for its efforts to build a strong personal data protection framework to advance protection of privacy, security, and the advancement of innovation and growth in India. What follows are our recommendations in key areas with regard to the draft legislation. These suggestions will serve to strengthen the work of the Indian Ministry of Electronics and

[1] Joint trade association letter to Minister Vaishnaw (1 Mar. 2022), available at https://www.siia.net/wp-content/uploads/2022/03/Global-association-letter-on-Data-Protection-bill-01032022.pdf.

Information Technology (the "Ministry"), while prioritizing responsible approaches to the use of data in the digital economy.

Recommendation 1: Create Greater Certainty for Cross-Border Data Transfers

The proposed Bill would permit cross-border data transfers by Data Fiduciaries only to those countries identified by the Central Government, subject to limited exemptions.[2] While we recognize the importance of providing the Central Government with authority to suspend or restrict cross-border transfers in extraordinary circumstances, we are concerned by the broad grant of discretionary authority and lack of alternative legal grounds for cross-border transfers.

In today's interconnected, digital world, ensuring the ability of Data Fiduciaries to transfer data across borders is essential for businesses of all sizes and all sectors. The approach contemplated by the Bill is truly unique. While other nations have incorporated "whitelists" into their cross-border data transfer frameworks, few have done so without also preserving alternative means for data transfers and/or providing clear guidelines for government adequacy determinations.[3] In Japan, for example, transfers are permitted to whitelisted countries and are also permitted based on contracts with data recipients overseas and in situations where the data subject (the "Data Principal") has given prior consent.[4]

We are concerned that the approach contemplated by the Bill will have negative consequences for the Indian economy. It can be expected to create unpredictability for domestic businesses and foreign investors that will lead to constraints on the ability of Indian-based businesses to grow, reduce foreign investment, and limit the choices and services available to Indian consumers.

Allowing avenues to transfer data across borders facilitates innovation, enables new business opportunities, provides consumers with additional and more robust services, and promotes collaboration and development across sectors that strengthen national economies. In short, cross-border data flows are integral to India's economy and business environment, including in the arenas of startups, global competitiveness, and investments in India's strong IT sector. These data flows should be viewed as an expectation and not an afterthought.

---

[2] *See* Digital Personal Data Protection Bill, 2022, at Sections 17-18, available at https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

[3] *See, e.g.,* Government of the United Kingdom, United Kingdom, Information Commissioner's Office, ICO's Guide to the UK GDPR and Data Protection Act of 2018: Exemptions, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

[4] *See* Government of Japan, Personal Information Protection Commission, Amended Act on the Protection of Personal Information, available at https://www.ppc.go.jp/files/pdf/APPI_english.pdf.

We believe an approach that provides greater certainty and predictability and opens India to data flows is critical to achieving the Ministry's ambitious program to realize a $1 trillion digital economy in India.[5] The Ministry has proposed measures to advance the Indian digital economy based on a recognition "that the digital world is essentially borderless, with capital, innovation, data, and design capabilities flowing into countries that offer the fewest pain points."[6] While the Ministry has expressed caution about a widening "digital deficit," and the importance of positioning India favorably "in the global digital diffusion race,"[7] we suggest that doing so can be achieved only by opening India to incoming and outgoing data flows that satisfy core preconditions critical to India's values, such as national security, cybersecurity, and privacy.

Moreover, it is likely that the compliance and business impact of unpredictability with regard to cross-border transfers will fall disproportionately on small and medium sized enterprises (SMEs) – both Indian SMEs and foreign SMEs doing business in India. SMEs will be forced to spend a significant portion of their resources to navigate complex compliance measures, and/or may get boxed out of participation.

In addition, predictability and certainty around cross-border data transfers will further Indian interests in the international economy. In the past few years, India has made strides to connect with other democratic nations in advancing coordinated approaches and dialogues on data and technological development. This includes India's critical regional and global role, reflected in its participation in the Quad (along with Australia, Japan, and the United States) and participation in the Global Partnership on Artificial Intelligence.[8] Codifying recognition of transfers to other nations would help to further India's ties to other Quad partners, who notably are among the participants in the Global Cross Border Data Privacy Rules (CBPR) Forum, established in 2022.[9] The Global CBPR Forum will provide a mechanism to promote trusted data flows among participant nations through a uniform system intended to further mutual economic interests, including digital trade, while recognizing each nation's distinct domestic interests and approaches on data privacy, security, and other interests. As India assumes the G20 Presidency in 2023, the nation will have an important role in setting a global agenda for data governance and building stronger digital relationships with its key partners. Cross-border data flows will be at the core of these relationships.

---

[5] Government of India, Ministry of Electronics & Information Technology, *India's Trillion-Dollar Digital Opportunity* (2019), available at https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

[6] *Id.* at 28.

[7] *Id.*

[8] *See, e.g.,* Quad Principles on Technology Design, Development, Governance and Use (24 Sept. 2021), available at ttps://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/.

[9] *See* Global Cross-Border Privacy Rules Declaration (21 Apr. 2022), available at https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

We urge the Ministry to incorporate a framework that would permit cross-border data transfers regardless of a nation's status on the whitelist. This may include, for example, criteria tied to the technical feasibility of digital transfers, the data security and level of protection of the services, contract terms, user consent, and certifications. We would recommend that the criteria permit a Data Fiduciary that is able to provide an appropriate and reasonable level of protection in accordance with pre-specified requirements be able to transfer data across borders - even to a nation not on the whitelist.

By allowing for these business exemptions, the draft would align to GDPR[10] and other global privacy regimes, so that businesses can effortlessly continue in these engagements, including those data flows that are underpinned by standard contractual clauses and/or other legal agreements between entities housed in separate, foreign jurisdictions. Businesses – including those that may be on the restricted list – should also continue to benefit from participation in the APEC Cross Border Privacy Rules and other multilateral trade agreements, approved across foreign governments, which should be incorporated into the exemptions. This approach will promote foreign investment in India by creating greater transparency, streamlining and aligning data flows to existing global regimes, and lowering compliance costs for companies across a wide array of sizes and scope of data processing.

In addition, Section 17 lacks a guiding principle for the Central Government to develop factors and undertake an assessment of a nation's adequacy. We believe this will create additional risk for companies doing business or considering operations in India (and, for reasons stated above, will also impede the ability of Indian-based businesses to grow). For example, Section 17 could direct the Central Government to make an assessment based on India's national security, extraordinary circumstances, or other principles. Further clarity is critical not only for the Central Government but for consumers, domestic and foreign industry, and foreign governments. From a business perspective, we believe this will create significant risk for companies doing business in India or interested in entering the Indian market.

Further, the Bill does not identify a timeline for implementation of any restrictions that the Central Government may impose on cross-border data transfers. To ensure that businesses can continue to operate and provide services to Indian consumers, businesses, and government agencies without interruption, we recommend that the Ministry establish a reasonable implementation period of no less than 12 months from the date that the Central Government provides notification along with any terms and conditions.

As an alternative to the whitelist approach proposed in Section 17, we encourage the Ministry to consider authorizing the Central Government to identify a list of countries to which data *cannot* be transferred. This "blacklist" approach would avoid many of the concerns around uncertainty that we have highlighted and, because it would focus on potential harms – such as

[10] *See* European Union, General Data Protection Regulation, Article 49, Derogations for Specific Situations, available at https://gdpr-info.eu/art-49-gdpr/.

privacy, cybersecurity, and other risks associated with any transfers – would likely ease the burden on the Central Government.

In sum, we respectfully recommend that the Ministry amend Section 17 to undertake all of the following:

1. Either (a) provide guiding principles for the Central Governments' development of factors for transfer of data outside of India, (b) identify specific factors that the Central Government should consider, or (c) implement a blacklist approach, in lieu of a whitelist approach, that identifies only those countries to which transfers should not be allowed or should be allowed with specific additional conditions.

2. Provide alternative bases for transferring data outside of India, such as contracts or international certifications (such as a CBPR certification).

3. Establish an implementation timeline of at least 12 months from the date the Central Government has notified and provided terms and conditions before transfer restrictions take effect.

Recommendation 2: Prioritize Children's Rights and Privacy

We are encouraged by India's interest in protecting the privacy of children but are concerned that this draft does not reflect the spirit of the UN Convention on the Rights of the Child ("Convention") to which India is a signatory. Access to information is a key pillar of the Convention and this proposal could put India at odds with it. India urgently needs to create more pathways to cyber and ICT careers. Access to information, training, and data online is critical to ensuring those pathways remain open for India's children.

We urge revisions of certain provisions in this draft so the best interest of children will be at the heart of it. For instance, some provisions under Section 10 may restrict teenagers' access to information – the age of consent, the proposed ban on behavioral monitoring, and the ambiguity around the harm threshold.

This proposal establishes an age of consent that would be outside of the norms sent around the world. Children may have parents that do not have the ability due to work location or availability and would put those children at a disadvantage in terms of access to digital content and services compared to their peers around the globe. A three year old is treated the same as a 17 year old in this legislation which does not account for the maturity or capacity of older children. Global standards range from 13 to 16 years of age, with many countries such as Japan, Singapore, and Australia setting their age of consent at 13.

In sum, we respectfully recommend that the Ministry amend the Bill to:

- Identify restrictions for consent in line with global norms to enable teen access to information and education online.

- Revise text to remove "likely to cause harm" standard and replace with, "A Data Fiduciary shall not undertake such processing of personal data which is contrary to the best interests of children" and define "best interests of children" in accordance with the UN Convention on the Rights of the Child".

Recommendation 3: Establish an Implementation Timeline for the Bill

The current version of the Bill does not include a timeline for implementation of its provisions. We recommend that the Ministry incorporate a clear timeline for implementation into the legislative text. The Ministry may wish to consider the implementation frameworks provided for in other data protection instruments with cross-border implications. For example, the European Union's General Data Protection Regulation provided for a 24-month implementation period. We understand a previous version of the Bill included a 24-month implementation period and recommend that this be reinserted into the bill text.

In sum, we respectfully recommend that the Ministry amend the Bill to:

- Incorporate language specifying that the terms of the Bill will take effect 24 months following enactment of the bill.

Conclusion

Thank you for the opportunity to share our views. We look forward to continuing to support these efforts with India to ensure effective, secure, and robust cross-border data flows that enhance global trade and accelerate innovation.

Please direct inquiries to: Paul Lekas, SIIA's Senior Vice President for Global Public Policy, at plekas@siia.net and Divya Sridhar, Senior Director for Data Policy, at dsridhar@siia.net.