Comments on Digital Personal Data Protection (DPDP) Rules, 2025

April 2025

Recommendations

MeitY should ensure the Digital Personal Data Protection Rules align with the following principles to advance practical and effective privacy protections, support economic development, and allow Indian citizens to use and benefit from the open, global, and secure Internet.

- Promote globally recognized best practice standards for privacy.
- Invest more in research for privacy-preserving age verification technologies that prevent excessive data collection and block access to the Internet.
- Avoid mandated data localization and restrictions on cross-border data flows, which can threaten the security of people, businesses, and economic development in general.
- Promote non-binding guidelines and follow globally recognized best practice standards for privacy to protect data wherever it goes, in transit and at rest, using technologies like strong encryption.

Executive Summary

The Internet Society appreciates the opportunity to contribute comments on the draft Digital Personal Data Protection (DPDP) Rules 2025. The Internet Society is a global charity and non-profit organization that supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society.

This document outlines and articulates our main points of concern. We hope that our submission will help the Indian government advance practical, effective privacy protections that allow Indian citizens to use and benefit from the open, global, and secure Internet.

We urge MeitY not to mandate verifiable parental consent, as this approach could increase risks to users' privacy, security, and safety. Instead, we recommend that the DPDP Rules focus on improving privacy protections for all users, whether adults or children. This can be achieved by adopting and enforcing globally recognized best practice standards for privacy.

Further, we urge MeitY not to impose data localization requirements because of the harmful effect they could have on the Internet, its users, and the Indian economy. Instead, we recommend that the DPDP Rules focus on protecting personal data handled by online services in India without regard to its physical location.

We appreciate that there is increasing policy interest in requiring the use of age-verification technologies to restrict children's access to certain services and content. Current methods for age verification present significant risks to privacy, security, and accessibility. These risks could negatively affect children and everyone online, as age verification techniques typically must apply to everyone, potentially chilling normal Internet usage.

Verifiable Parental Consent

The draft DPDP Rules require verifiable parental consent, using age and identity verification, for the processing of personal data for individuals under 18 years of age. Protecting children's privacy is crucial, but the proposed requirement is likely to hinder Indian digital inclusion, access, privacy, safety, and security.

Concerns

Practical and Operational Challenges: Enforcing verifiable parental consent across a diverse population with varying levels of digital literacy is challenging. Additionally, many online platforms, particularly smaller ones, are likely to lack the technical capacity to implement safe, secure, and privacy-preserving age and parental verification mechanisms.[1] Additionally, this requirement for processing personal data could unintentionally exclude minors from essential services such as educational platforms, mental health resources, domestic violence resources, and online communities.[2]

Privacy and Data Security Risks: Parental relationship and age verification mechanisms often require the collection of additional personal or sensitive data, potentially leading to excessive data collection, retention, and heightened risks of data misuse or data breaches.[3] This increases privacy and data security risks, including the risk of identity theft. It also contradicts the principles of data minimization and purpose limitation outlined in the draft Rules and found in international best practices.[4] While trying to protect privacy, these draft Rules could greatly weaken the privacy of Indian citizens.

---

[1] Livingstone, S., & Stoilova, M. 2021. The 4Cs: Classifying Online Risk to Children. Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

[2] Centre for Communication Governance at National Law University, Delhi. available at https://ccgnludelhi.wordpress.com/2023/11/21/navigating-the-indian-data-protection-law-childrens-privacy-and-the-digital-personal-data-protection-act-2023/

[3] See Unpacking Age Assurance: Technologies and Tradeoffs, Future of Privacy Forum. June 2020, available at https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/

[4] OECD Privacy Guidelines. 2013, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Negative Impact on Anonymity Protections: With substantial digital penetration in India, many individuals, including minors, rely on online pseudonymity or anonymity to safely access vital resources on sensitive topics, including social stigma, mental health, and sexuality,[5] or to seek help when facing domestic violence and abuse. Teenagers are increasingly using online spaces to gain knowledge and community support so that they can make informed and safe choices.[6] Age and parental consent verification mandates could discourage or prevent young users from seeking vital help and engaging in safe digital spaces, leading to uninformed decisions and very serious negative social and health consequences.

Further details regarding our concerns about the efficacy, safety, security and privacy of age verification technologies are set out in a joint amicus curiae brief we submitted to the Supreme Court of the United States in *Free Speech Coalition v. Paxton*.[7]

Data Localization and Its Broader Impact on Security

The draft DPDP Rules include provisions mandating the storage of certain categories of personal data within India. While intended to enhance data security, data localization introduces several risks that may hinder India's digital economy, cybersecurity, and cross-border trade.

Concerns

Economic Impacts and Compliance Burdens: The growth of India's digital economy could be significantly restricted as data localization rules increase the cost of doing business in India. Data localization policies require service providers to create additional hosting facilities, which in turn means they need reliable infrastructure to keep the data physically in the country. Because not all countries are capable or equipped to facilitate such infrastructure, service providers could encounter additional costs and possible infrastructure vulnerabilities or simply choose not to provide their services in those countries. Small and medium enterprises and multinational businesses will face increased costs associated with setting up and maintaining local data storage and processing infrastructure, potentially damaging investment and innovation in India.[8] The compliance burden could disproportionately impact startups and reduce their ability to compete in the digital marketplace globally. This could encumber

[5] Electronic Frontier Foundation. 2023, available at https://www.eff.org/document/eff-one-pager-age-verification

[6] See Young People's Sense of Belonging Online, Digital Wellness Lab. October 2024, available at https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/

[7] A joint amicus curiae brief to the Supreme Court of the United States in *Free Speech Coalition v. Paxton*, the Center for Democracy & Technology, New America's Open Technology Institute, the Internet Society, and Professors Daniel Weitzner, Eran Tromer, and Sarah Scheffler, available at https://www.supremecourt.gov/DocketPDF/23/23-1122/326510/20240920161551554_23-1122%20Amicus%20Brief.pdf

[8] Burman & Sharma. 2021. Carnegie Endowment for International Peace, available at https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india?lang=en

the growth of India Stack,[9] make the Internet in India less open, and potentially cement the dominance of existing large providers.

Resilience and Connectivity: Another issue with data localization requirements is that data may not be stored optimally, both in terms of resilience and connectivity. The topologically closest—meaning "closest" in terms of the network's structure, and therefore fastest—location in the network for storing data may not be in the same country. Data is stored where it makes most sense—and this involves dynamic considerations of efficiency and performance reliability rather than location. Even if data is located in one country, the transmission path may cross national borders for resilience or performance reasons, and this may change on a millisecond basis. Data localization measures may either directly or indirectly force Internet data to follow national borders at the expense of efficiency, meaning Indian users will experience a less powerful and useful Internet.

Restrictions on Cross-Border Data Flows: Limiting cross-border data transfers could disrupt efficient global business operations and restrict India's ability to participate in global digital trade. This can also hinder innovative and emerging industries.[10] Reciprocal or retaliatory data localization restrictions from other nations on Indian businesses abroad may create new barriers to Indian businesses that seek to access international markets. Foreign businesses may also exit India to avoid data localization restrictions. Data localization mandates risk fragmenting the Internet and creating isolated islands of digital services along national borders.

Data localization mandates impose economic, operational, and security risks without guaranteeing improved data protection. A more effective way to protect personal data is to focus on privacy principles and security measures that keep data secure both in transit and at rest—wherever information travels or is stored.

Conclusion

While the DPDP Rules, 2025, aim to enhance data protection, rigid localization mandates and overly strict age verification requirements could inadvertently harm India's digital ecosystem. MeitY should align the Digital Personal Data Protection rules with global best practices to enhance privacy while supporting economic growth and an open, secure Internet. This includes investing in privacy-preserving age verification, avoiding data localization mandates, and ensuring secure cross-border data flows. Adopting non-binding guidelines and strong encryption will further protect data in transit and at rest.

For further discussion and clarity please contact apac@isoc.org.

[9] India Stack - https://indiastack.org/

[10] Economic Times. 2024, available at https://economictimes.indiatimes.com/news/economy/foreign-trade/indias-stance-on-data-transfers-at-wto-spooks-chip-giants/articleshow/107937033.cms?from=mdr