C-HELP | CENTRE FOR HEALTH EQUITY, LAW & POLICY

ILS

Submission to the Ministry of Electronics and Information Technology (MeitY) on the Draft Digital Personal Data Protection Rules, 2025

February 2025

About

The Centre for Health Equity, Law & Policy is a research, knowledge production and advocacy forum which works on law & policy issues related to health, embedding its work in the right to health as envisaged within India's constitutional framework and her international commitments. It is located at the Indian Law Society, Pune.

Authors

Shivangi Rai and Shefali Malhotra

Contact Information

contact@c-help.org
Centre for Health Equity, Law & Policy
Indian Law Society
Law College Road
Pune, 411004, Maharashtra, India

1. Rule 3 - Notice given by Data Fiduciary to Data Principal

a) In the interest of and to fulfil the constitutional obligation of transparency, which is the cornerstone of the right to informed consent, autonomy and privacy, the draft rules must mandate disclosure in the notice on: sharing of data with third parties; transfer of data abroad; retention or storage limitation; and information on all the rights under the Act.

b) The Rules mention that the notice must have the communication link for accessing the website or app, or both and a "description of other means, if any". It is submitted that the Rules must categorically mandate that notice and consent mechanisms must be provided on both the website, the app and offline as well. This is important to ensure that digital divide and digital familiarity do not prevent data subjects from exercising their rights under the Act.

c) The Act said that the Rules will prescribe the manner in which the data principal will exercise her rights under the Act as well as make a complaint to the Board. However, the Draft Rules do not prescribe the manner at all. The Draft rules must have more detail on the manner so that the process becomes clear with some uniformity and standardisation across different Data Fiduciaries.

d) In order for the notice and consent mechanism to be really accessible to all, including people with disability, the Rules ought to mandate provision of audio/visual tools, at the minimum.

2. Rule 5 - Processing of personal data for provision or issue of any subsidy, benefit, certificate, license or permit by state or its instrumentalities

It is submitted that the relevant section in the law violates the privacy principle of purpose limitation, without any sufficient or reasonable cause and is hence disproportionate. However, at the minimum the rules should not include subsidies or services provided under any executive action into the category of policy. This exception should only apply to benefits or subsidies mandated by law, and should not cover executive instructions.

Further, it is reiterated that services, even if mandated under law or policy, should not automatically be exempt from the need for consent before processing of personal data, if they are in the nature of a fundamental right, such as the right to education or right to health.

3. Rule 6 - Reasonable security safeguards

The Rules are vague on 'appropriate technological and organizational measures" as well as "appropriate security measures" to be adopted. These should be accompanied by:

a) The standards should mandate that the Data Fiduciary is not just obligated to implement appropriate security measures but also to be able to *demonstrate* that data processing is carried out in conformity to those standards and to law.

b) The Rules should mandate that Data Fiduciaries adopt internal policies on organisational, technological and security measures.

c) The rules should mandate that these measures should be reviewed and updated periodically.

d) There should be some measurable benchmark with which to judge adequacy of the "appropriateness" of the measures. It cannot be left to the discretion of the individual data fiduciaries. The rules should lay down some standards or mandate a certification of adequacy. This would also empower users of digital services with adequate information. For eg. EU GDPR (Art 24) mandates data fiduciaries to adhere to a code of conduct (Art 40) or approved certification mechanisms (Art 42) as a means to demonstrate compliance with appropriate technical, organisational and security measures.

e) The obligations for audit (at the minimum) and for conducting Data Protection Impact Assessment, should not have been limited only to the SDF. The fact that startups may be exempted from adopting any data protection and security measures under the Act is also problematic. According to a report by ransomware recovery specialists, Coveware, a "tactical shift" has been introduced by many ransomware gangs, which includes a "deliberate attempt to extort companies that are large enough to pay a 'big game' ransom amount but small enough to keep attack operating costs and resulting media and Law Enforcement attention low." The report notes that 82% of attacks that took place in 2021 impacted organizations with less than one thousand employees.

f) There are no obligations or provisions on "pseudonymisation", “de-identification” and “anonymization.” of personal data. Consequently, no legal thresholds for it and no penalty for de-anonymisation.

g) There should be some clarity or minimum criteria for selecting data processors. There should have been obligations to ensure that the contract entered into between DFs and data processors have clauses on conformity with the law, data protection and security measures and accountability.

4. Rule 7 - Intimation of personal data breach

Rule 7 mandates that data fiduciaries notify data principals immediately upon becoming aware of a personal data breach. However, given the complexities and realities involved in responding to a data breach, this provision may be overly burdensome and prone to violations. For instance, in the 2023 AIIMS data breach, the hospital took up to two weeks to fully assess the scope of the breach and implement corrective measures. This delay highlights the challenges organizations face in managing the aftermath of such incidents. Therefore, it is recommended that Rule 7 be amended to establish a more reasonable and staggered timeframe for informing data principals about the breach, as well as for updating them on the ongoing assessment and mitigation efforts. This approach would balance the need for transparency with the practicalities of managing a data breach.

5. Rule 9 - Contact information of person to answer questions about data processing

Rule 9 should mandate that the contact information of the person who will answer questions about data processing should be prominently displayed in a conspicuous place on both the website and app, as well as in every communication with data principals.

6. Rule 10 - Verifiable consent for processing of personal data of a child or of a person with disability who has a lawful guardian

At the outset, the DPDPA’s reliance on parental (or legal guardian’s) consent raises fundamental issues as to the decisional autonomy of children and persons living with

disabilities, and may be at odds with the UN Convention on the Rights of Child 1989 and UN Convention on the Rights of Persons with Disabilities 2006 in certain circumstances.

Rule 10, in itself, suffers from a significant deficiency in so far as it appears to rely on the child to inform the data fiduciary that they are minors or below 18 years. In reality, identifying a child accurately is a significant challenge, especially when parental consent is required for the collection of children's data. This difficulty has led to the imposition of additional provisions across various jurisdictions to ensure better protection of children's online privacy. For example, the Children's Online Privacy Protection Act in the U.S. not only mandates parental consent for children under 13 but also requires websites and apps to provide clear privacy policies, limit the type of data they collect from children, and retain that data only as long as necessary. The Personal Data Protection Act (PDPA) in Singapore requires parental consent for children under 13 but also ensures that personal data of minors is not shared with third parties unless explicitly consented to. In Brazil, the Lei Geral de Proteção de Dados (LGPD) similarly mandates parental consent for children under 16 and emphasizes that children's personal data should only be processed in a way that protects their fundamental rights, including the right to privacy.

Rule 10 also treats all websites and apps on an equal plane. In contrast, in other jurisdictions, risk categorization for children's data processing plays a key role in ensuring robust privacy protections. These jurisdictions assess risks based on factors like the type of data collected, the purpose of processing, and the potential impact on children's privacy. For instance, the General Data Protection Regulation (GDPR) in the EU and the Children's Online Privacy Protection Act (COPPA) in the U.S. require data fiduciaries to adopt stricter safeguards for high-risk activities, such as collecting sensitive data or engaging in profiling. Such an approach may be better suited to protect children's privacy as well as other rights.

7. Rule 11- Exemptions from certain obligations applicable to processing of personal data of a child

Rule 11 and Part A of the Fourth Schedule exempts healthcare workers and establishments from the obligation to collect parental consent for processing children's data or from engaging in behavioral monitoring, citing the broad rationale of providing

healthcare services and protecting health. However, this exemption should be limited to situations involving medical emergencies, where immediate action is required for the child's well-being. In all other cases, there is no compelling reason to grant such an exemption. Children's privacy rights must still be upheld in non-emergency situations as well as once an emergency situation has passed, and healthcare providers should adhere to the same data protection standards as other entities processing children's data, ensuring parental consent and safeguarding against unnecessary behavioral monitoring and profiling.

Further, Part B of the Fourth Schedule permits the tracking and profiling of children to prevent access to information that may have a detrimental effect on their well-being. However, this provision is overly broad and lacks a clear definition of what constitutes detrimental to a child. Without specific guidelines, it could restrict children's access to important information online, particularly hindering their participation in social media activities. This is especially concerning for children in abusive or restrictive family environments who may rely on the internet for support and education. For instance, similar laws in the U.S. have been used to block children from accessing content related to sexuality, gender identity, and other topics that may conflict with their parents' ideologies. Such overreach risks limiting children's ability to explore diverse perspectives and access vital resources for their development.

8. Rule 12 - Additional obligations of significant data fiduciary

a) There should be more safeguards/ guardrails conditions for the contract between DF and data processors – transparency, compliance with the law, accountability etc.
b) There should have been more guidance on conducting DPIA. For eg. see Art 35 of the EU-GDPR.
c) The results of DPIA could be placed in the public domain for transparency and for educating the users.
d) The DPDPA deleted the requirement of "Data protection/privacy by design and default", which was there in previous iterations of the bill. That mandate should have been retained and DFs should have been obligated to implement the mandate by incorporating principles of data minimization for every stage of data

processing and other security measures that operationalize privacy by design and default.

9. Rule 13 - Rights of data principals

a) Rule 13 (1) should be amended to mandate data fiduciaries to publish the specified details on both the website and the app.
b) Rule 13(3) must lay down the process of grievance redress that must be followed by the data fiduciaries. This should not be left to the discretion of the data fiduciaries. In the absence of these processes, data principals are likely to face the risk of arbitrary rejection of complaints. As an example, one of the most common complaints against Indian health insurance companies, who are free to lay down their own procedure for settlement of insurance claims, is the
c) Rejection of claims without any reasoning. It is also not clear what remedies will be available to the data principal at the conclusion of the grievance redress process.

10. Rule 15 - Exemption from Act for research, archiving or statistical purposes

Given that the exemption under Rule 15 removes the applicability of the law and restricts the rights of data principals, Clause (f) of the Second Schedule must establish a high threshold for data fiduciaries, ensuring that personal data is rigorously protected and secure. These standards should be clearly defined to avoid ambiguity and ensure consistent compliance. Moreover, failure to uphold these standards must result in penalties that are proportional to the severity of the violation. For example, under the General Data Protection Regulation (GDPR) in the EU, data fiduciaries are required to meet stricter requirements when using personal data for research purposes, including conducting Data Protection Impact Assessments (DPIAs) and ensuring that data is anonymized or pseudonymized wherever possible. Similarly, the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. places heightened standards on healthcare data fiduciaries, demanding strict controls on how personal health data is used for research, and requiring patient consent or ethical approval. By adopting similar high standards in Rule 15, the law would not only hold data fiduciaries accountable but

also create strong incentives to prioritize the privacy and security of personal data, while safeguarding the rights of data principals.

11. Rule 16 - Appointment of Chairperson and other members

a) Given that the government is the largest data processor in the country, the composition of the Search-cum-Selection Committee should have parity among government and public members. It should be headed by a member of the public as well.
b) Rule 16 should specify the process that the Search-cum-Selection Committee will follow to appoint the chairperson and members of the Data Protection Board. In addition, the rule should include an obligation that the minutes and decisions of the Search-cum-Selection Committees will be placed in the public domain.

12. Rule 18 - Procedure for meetings of the Board

Rule 18 must obligate that the schedule, agenda and minutes of the meetings of the Data Protection Board should be placed in the public domain.

13. Rule 19 - Functioning of the Board as a digital office

Given the challenges of the digital divide and varying levels of digital literacy across India, the Data Protection Board should not function solely as a digital office. It is crucial that the Board also establish physical offices in various regions of the country to ensure accessibility for the majority of the population, particularly those in rural areas or those without reliable internet access or digital skills. In India, where many individuals may lack the resources to navigate online platforms, having physical offices would enable citizens to directly engage with the Board, seek assistance, and address concerns regarding their data privacy rights. This approach would help bridge the gap for those who might otherwise be excluded from the digital process, ensuring a more inclusive and equitable implementation of data protection laws across the country.

14. Rule 22 - Calling for information from Data Fiduciary or intermediary

Rule 22 read with Schedule 7, does not pass the constitutional standard of substantive and procedural due process. The Rules ought to have specified the grounds or reasons

for which the Central Government could call for information from the Data Protection Board, Data Fiduciary or intermediary.

The Rules and the Schedule ought to have laid down safeguards such as: the specific designated officer of the Central Government that could call for such information; there should be mandate for reasons to be recorded in writing before issuing any such direction; it should have been made subject to preferably a judicial oversight mechanism; and it should have been restricted in time, for eg. a duration of 3 months, which could only be extended subject to review and oversight.