IT for Change's Submission on the Draft Digital Personal Data Protection Rules, 2025

IT for Change

March 2025

IT for Change's Submission on the Draft Digital Personal Data Protection Rules, 2025

IT for Change

March 2025

IT for Change submitted its feedback/comments on the draft Digital Personal Data Protection Rules, 2025 (DPDP Rules) released by the Ministry of Electronics and Information Technology. The comments are as below.

Rule 1 - Short Title and Commencement

NA

Rule 2 - Definitions

NA

Rule 3 - Notice given by Data Fiduciary to Data Principal

1. Rule 3(b) imposes an obligation upon the Data Fiduciary to issue a notice that shall give "a fair account of the details necessary to enable the Data Principal to give specific and informed consent." There is a requirement to include in the notice, at the minimum, "an itemised description of such personal data" and "an itemised description of the goods or services to be provided or uses to be enabled by" such processing.

Recommendation:

- In order to ensure that the principles of data minimisation and purpose limitation in processing are adhered to, and to ensure free and fair consent for data processing, the notice should also incorporate the following elements:

i. Business contact information of the Data Protection Officer/a person who is able to answer the Data Principal's questions about the processing of personal data. While these details are to be

published by Data Fiduciary on its website/ app (Rule 9), for ease of reference and to further informed consent, such information should also be shared in the notice itself.

ii. Data retention time period (in conformity with storage limitation principles).

iii. The recipients and categories of recipients of personal data shared (Article 13, General Data Protection Regulation (GDPR) has a similar requirement).

iv. Intimation about the use of personal data for any form of automated decision-making, including profiling, and its consequences for the Data Principal (Recital 60 - Information Obligation and Article 13, GDPR have similar requirements).

2. Under Section 5(2) of the Digital Personal Data Protection Act, 2023 (Act), in cases where consent is given prior to commencement, the Data Fiduciary should give the Data Principal notice “as soon as it is reasonably practicable”. It is not clear whether the notice-related requirements under Rule 3 are also applicable to cases where consent has been given prior to the commencement of the Act. Further, the time period within which such notices are to be issued has also not been prescribed.

Recommendation:

- Specificity on the timeline to share notice where consent is given prior to commencement of the Act is essential to ensure substantive compliance with the legal provisions. Further, the substantive requirements under Rule 3 should also apply to such notices.

Rule 4 - Registration and Obligations of Consent Manager

1. The Consent Manager’s obligation to implement "reasonable security safeguards", under the First Schedule Part B, Clause 7 requires a clearer definition to build public trust.

Recommendation:

- Clause 7 should specify that the security safeguards taken by Consent Managers (CMs) must meet the minimum standards required from Data Fiduciaries under Rule 6. Clause 8 should clarify that rules applicable to Data Fiduciaries also apply to CMs.

- The rules should ensure CMs act as responsible custodians by requiring them to demonstrate prior experience in data handling, undergo periodic security certifications, and prevent the harvesting of consent metadata for unintended purposes. These measures would safeguard against unauthorised use and minimise security risks.

2. First Schedule Part B, Clause 2 imposes an obligation upon the CM to ensure that it cannot read the personal data it handles. However, Clause 3 requires the CM to maintain records on the Consent Manager Platform (CMP), which include consents given/denied/withdrawn, notices for consent, and records of sharing personal data with transferee Data Fiduciary.

Recommendation:

- It is our submission that the obligation under First Schedule Part B, Clause 3 to maintain records of consents, notices, etc. cannot be imposed upon the CM in view of the requirement under Clause 2 regarding non-readability of data. While the concept of consent management has already been introduced under the Data Empowerment and Protection Architecture—a secure consent-based data sharing framework (https://tinyurl.com/5n6t26pf), through the account aggregator ecosystem in the financial sector (https://tinyurl.com/c7se4yzs), clarity on the techno-design elements of the CMP is essential to ascertain the extent to which the existing technological architecture can be utilised, and to ensure platform readiness.

Rule 5 - Processing for provision or issue of subsidy, benefit, service, certificate, license or permit by State and its instrumentalities

1. The Second Schedule of the Rules provides for the standards for the processing of data by the State and its instrumentalities; however, there are gaps that require further elucidation.

Recommendation:

- As per the Second Schedule, Clause (d), processing of data should be done while making “reasonable efforts to ensure the accuracy of personal data.” Expansion of the term “reasonable efforts” is required to ensure uniformity in standards adopted across the State and its instrumentalities for data processing.

- Clause (f) states that “Reasonable security safeguards to prevent personal data breach” shall be implemented. Minimum standards as to what constitutes reasonable security safeguards should be prescribed to help guide compliance.

2. While the Second Schedule, Clause (g) provides that the Data Principal shall be given the business contact information of a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about processing of her personal data, there is no clarity on the time period within which the questions will be answered. Further, it is unclear how the Data

Principal can address his/her grievances in case the questions remain unanswered/are not satisfactorily answered.

Recommendation:

- Clarity is crucial on the time period within which Data Principal's processing-related questions will be answered as well as the manner in which Data Principal can track these questions.

Rule 6 - Reasonable security safeguards

Rule 6(1)(g) provides that the Data Fiduciary shall take "appropriate technical and organisational measures to ensure effective observance of security safeguards." However, the measures are not prescribed/detailed and are left to the discretion of Data Fiduciaries.

Recommendation:

- To ensure meaningful personal data protection, the security safeguards must be robust and not left to interpretation. For instance, Article 25, GDPR provides for data protection by design and by default—this includes the implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

Rule 7 - Intimation of personal data breach

Rule 7 imposes an obligation upon the Data Fiduciary to intimate to the Data Principal and the Data Protection Board (Board) "without delay" the details of personal data breaches. Detailed information of the breach (along with a report regarding the intimations given to the Data Principals) has to be shared by the Data Fiduciary with the Data Protection Board within seventy-two hours. However, the time period of seventy-two hours is extensible by the Board upon receipt of a written request. In such cases of extension, it is unclear how the Board will ensure that remedial measures for data breaches are undertaken without delay.

Recommendation:

- In order to ensure compliance, a time period for intimation should be expressly prescribed. This can be in line with the period prescribed upon service providers, intermediaries, data centres, body corporate and Government organisations for reporting cyber-security incidents to CERT-In i.e. six hours (Cyber Security Directions No. 20(3)/2022-CERT-In dated 28 April 2022).

Rule 8 - Time period for specified purpose to be deemed as no longer being served

1. Rule 8 prescribes the time period for data retention for three classes of Data Fiduciaries—e-commerce entities, online gaming intermediaries, and social media intermediaries having a certain number of registered users as detailed under the Third Schedule. However, the data retention duration for categories of Data Fiduciaries other than these is not clear.

Recommendation:

- Data retention duration for all Data Fiduciaries should be explicitly clarified.

2. The Rules also do not elucidate what qualifies as erasure of data—for instance, Data Fiduciaries may psuedonymise/anonymise data while claiming compliance with 'personal data erasure' under the law.

Recommendation:

- Guidelines/details should be provided as to what meets the requirements of data erasure under the law.

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

NA

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

1. Rule 10 infantilises persons living with disabilities by treating them as incapable of providing informed consent independently. In an India-based research, guardians of persons with mental disability were found to act in violation of the scope of their authority under the Rights of Persons with Disabilities Act, 2016 (https://tinyurl.com/3ts4adpy).

Recommendation:
- It is important to adopt an approach that underscores the decisional autonomy of persons with disabilities, and equips them with necessary support for informed decision-making. This is followed in Australia by placing an obligation on the Data Fiduciary to provide assistive resources for informed consent by persons with disabilities (https://tinyurl.com/4rvsjuf7).

2. We appreciate that Rule 10 adopts an age-verification approach instead of age-gating. However, the suggested modality of age verification—the use of DigiLocker for verification of parents' government-issued IDs or ID tokens—raises the risk of data breach/profiling.

Recommendation:
- As CNIL (French data protection agency) has argued, it may be advisable to adopt age verification systems, where a trusted third party incorporates a double anonymity mechanism that prevents it from identifying the website/app at stake and sharing users' personal data to said website/app. (https://tinyurl.com/9na93t3x)

3. Also, by treating all persons under 18 as a monolithic category, the Rule fails to recognise the rights and agency of persons younger than 18.

Recommendation:
- Inspiration can be taken from GDPR & CNIL to arrive at a rights-based approach, ensuring the child's best interests. GDPR permits the age verification threshold to be set at 13/16 years based on national-level approaches. In India, a 16-year-old can be subject to criminal prosecution as though they are an adult. Thus, a threshold of 16 years should also be maintained for determining one's right to navigate the Internet. This may better serve the interests of young adults and their reproductive and sexual freedoms.

- A rights-based approach also requires adequate restriction on processing of publicly available personal information of children in online media, which is currently absent.

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

1. Under Part B, Fourth Schedule, the restriction on processing aims to protect children from accessing information that could cause a "detrimental effect" on their well-being. However, the term "detrimental effect" is vague, opening the door to subjective interpretations that could lead to overreach, as has been experienced in other jurisdictions (https://tinyurl.com/2s35tu4c).

Recommendation:

- An explanation as to what constitutes a "detrimental effect" is required to prevent arbitrary application of the provision.

Rule 12 - Additional obligations of Significant Data Fiduciary

1. We appreciate the imposition of obligations upon Significant Data Fiduciaries (SDF) vide the requirement of Data Protection Impact Assessment (DPIA) and audit. However, guidelines and standards for these are absent.

Recommendation:

- Guidelines/standards should be prescribed for the DPIA and audit to be undertaken by SDFs to ensure effective observance of legal provisions.

2. While sub-rule (3) requires that the SDF shall observe “due diligence” that algorithmic software deployed by it is “not likely to pose a risk to the rights of Data Principals”, the vagueness in terminology used may lead to circumvention and lack of compliance.

Recommendation:

- Guidance on what constitutes “due diligence” is of the essence.

- The low compliance threshold, i.e. “not likely to pose a risk”, requires a relook given the dangers of bias, discrimination, and infringement of rights by algorithmic software. Elements of a risk-based approach, similar to the one laid down under the EU AI Act and envisioned in India’s Subcommittee on AI Governance and Guidelines Development’s report, (recommending “there may be a need for a baseline framework that applies to the development and deployment of AI systems that are considered medium-to-high risk across domains and sectors”) should be incorporated under the Rules to ensure a future-ready data protection framework.

Given that SDFs are categorized as such on the basis of volume, sensitivity of data processed, risk to the Data Principal’s rights, State security, etc. —any algorithm deployed by such SDFs requires adequate oversight and risk assessment including Fundamental Rights Impact Assessment (Article 27, EU AI Act).

3. Further, Rule 12(4) requires SDFs to ensure personal data and the “traffic data” (this term does not find mention in the parent legislation) pertaining to its flow, as specified by the Central Government, is not transferred outside India. If the legislature is of the opinion that certain types of personal and traffic data shall be localized by SDFs, the question arises as to why other fiduciaries are exempt from the same requirement.

Recommendation:

- Uniform applicability of data localization requirements across Data Fiduciaries is a must to ensure the protection of citizens' data privacy rights.

- Clarity is needed on what constitutes "traffic data" and what standards apply to the processing of such data.

Rule 13 - Rights of Data Principal

1. The manner in which requests for the right to erasure of data shall be made (a right granted to Data Principals by the Act) has not been prescribed under the Rules, which appears to be an oversight.

Recommendation:

- The manner in which data erasure requests may be made should be prescribed.

- Clarity must also be provided regarding the process to be followed by Data Fiduciaries in dealing with requests for personal data processing. How should the Data Principal be supported in tracking such a request? Within how many days of receipt of the request should the data be deleted by the Data Fiduciary?

2. Further, with respect to grievance redressal, sub-rule (3) provides that every Data Fiduciary and Consent Manager shall "publish the period under its grievance redressal system for responding to Data Principals' grievances".

Recommendation:

- The determination of the time period should not be left to the discretion of Data Fiduciaries. Instead, a reasonable time period should be prescribed under the Rules to ensure the effective realisation of Data Principals' rights, in order to enforce Section 13 of the Digital Personal Data Protection Act effectively.

Rule 14 - Processing of personal data outside India

There are no clear criteria for when restrictions on cross-border data flows can be imposed, creating the potential for arbitrariness. We appreciate the government's interest in retaining the powers to regulate cross-border flows of personal data stemming from considerations of citizen privacy, law enforcement, national security, and digital sovereignty. However, such restrictions should be based on clear grounds and not subject to arbitrariness. The EU and China, for instance,

have specified approaches towards cross-border data flows (https://tinyurl.com/3u7sdyt6, https://tinyurl.com/mpfjx4yf) - similarly, we need an India-specific approach that takes into account constitutional principles and socio-economic priorities.

Recommendation:

- The Committee of Experts under the Chairmanship of Justice B.N. Saikrishna (https://tinyurl.com/525srjkb) suggested that data transfers outside India should be governed by model contracts containing key obligations on transferee such as purpose limitation, security, responsibility to fulfil rights of individuals, etc.

Sufficient clarity is needed on the type of requirements that the Central Government may impose with respect to the transfer of personal data outside India.

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

Rule 15 provides a broad exemption for non-consensual personal data processing related to research, archiving, and statistical purposes but lacks clarity on key aspects.

Recommendation:

- Definition of the terms “research”, “archiving”, and “statistical” along with the eligibility criteria for such processing is required to avoid ambiguity about who can invoke this exemption. For instance, it is unclear whether AI developers qualify under this provision.

- Clarity on whether the category of researcher (private, governmental, etc.) and purpose of research (commercial or non-commercial) affect the Rule’s applicability is of the essence.

- Sufficient safeguards in the processing of data for research/archiving/statistical purposes should be prescribed. For instance, in Vietnam, Hong Kong, Malaysia, and New Zealand, various safeguards, such as ensuring that statistics and/or research do not identify data principals, and encryption and pseudonymisation measures, are adopted before processing. In Singapore, there is a standard of ‘reasonable necessity’ for processing personal data in an individually identifiable form with prohibitions on using research results to make decisions about individuals and processing personal data for archival or historical purposes if a reasonable person would consider the processing too sensitive at the proposed time.

Rule 16 - Appointment of Chairperson and other Members

The decision to utilise a Search-cum-Selection Committee comprising executive officials from the Central Government to determine the composition of the Board raises serious concerns about its independence and impartiality, both in terms of objective and subjective bias. The Board, tasked with carrying out judicial functions, is part of the tribunal system, with appeals directed to the Telecom Disputes Settlement and Appellate Tribunal. The Supreme Court, in its rulings on tribunals, has consistently emphasised the need for independence from the executive in matters of selection, composition, tenure, and security of tribunal members (*Madras Bar Association v. UOI*, 2014). Thus, given that tribunals are substitutes for the High Court, empowering the Central Government to appoint the members violates the independence of the judiciary (*S.P. Sampath Kumar v. UOI* 1987). In 2019, the Supreme Court reiterated that the lack of judicial dominance in the selection committees of tribunals violates the doctrine of separation of powers (*Madras Bar Association v. UOI*, 2014).

The executive-dominated selection process is also not in line with comparative best practices. In the European Union, the GDPR mandates that data protection authorities be free from external influence (whether direct or indirect) and requires safeguards to ensure their impartiality, including adequate financial, human, and technical resources. In Canada, the Privacy Commissioner is appointed with the approval of both chambers of Parliament, while South Africa's data protection regulation includes specific provisions to prevent conflicts of interest. Similar safeguards ensuring the independence and impartiality of data protection authorities exist in Australia, New Zealand, Singapore, Kenya, and Brazil.

Recommendation:

- A relook of the composition of the Committee may be necessary to avoid the potential for bias. Further, what qualifies as "suitability of individuals" under Rule 16(3) should be expanded upon for clarity.

Rule 17 - Salary, allowances and other terms and conditions of service of Chairperson and other Members

NA

Rule 18 - Procedure for meetings of Board and authentication of its orders, directions and instruments

NA

Rule 19 - Functioning of Board as digital office

NA

Rule 20 - Terms and conditions of appointment and service of officers and employees of Board

NA

Rule 21 - Appeal to Appellate Tribunal

NA

Rule 22 - Calling for information from Data Fiduciary or intermediary

Rule 22, along with the Seventh Schedule, enables the Central Government to compel a Data Fiduciary or intermediary to provide personal data. However, this provision raises serious constitutional concerns. The ground of "performance of any function under any law" is overbroad and wide enough to include *any* public purpose authorized by a statute. The Supreme Court, in a number of cases, has found overbreadth to be a basis for declaring a provision unconstitutional, such as in *Chintaman Rao v. State of Madhya Pradesh* (1951) and *Shreya Singhal v. Union of India* (2015).

The requirement for meaningful safeguards regarding state agencies' collection of personal data can also be found in the jurisprudence of the European Court of Justice, the European Court of Human Rights, and the Human Rights Committee.

Recommendation:

- The grounds for invocation in the Seventh Schedule should not be overly broad, and the government should introduce meaningful safeguards. These safeguards should include independent judicial oversight—both ex-ante and ex-post—a retention period, a data minimisation requirement, a review period, a requirement to use the least restrictive measure, technical safeguards, and transparency reports. The requirement for judicial safeguards stems from the *Puttaswamy II* decision, where the Court declared a provision unconstitutional as it did not require judicial scrutiny for the state's use of Aadhaar data for other purposes under the law.