Comments & Suggestions on

Draft Digital Personal Data Protection Rules 2025

Submitted by

Centre for Cyber Laws, NLU Delhi

This Report has been prepared & presented by Centre for Cyber Laws, National Law University Delhi.

Efforts and contributions have been made by the following student members of the Centre for Cyber Laws at NLU Delhi:

- Ira Srivastava, Student Fellow
- Aniya Damithia, Student Associate
- Manya Gupta, Student Associate
- Sanskruti Yukta Nayak, Student Associate

We would like to thank the immense support lent to this Project by Hon'ble **Vice-Chancellor Prof. (Dr.) G.S. Bajpai** Sir, Respected **Registrar Prof. (Dr.) Ruhi Paul** Ma'am and **Dr. Aparajita Bhatt**, **Director** Centre for Cyber Laws. We thank them for the continuous institutional support given to this Project & team at various stages.

Table of Contents

About this Report

Data protection law in India has undergone an interesting journey. What started as the Personal Data Protection Bill in 2018, underwent a series of consultations and engagement with civil society and a variety of stakeholders to emerge as the Digital Personal Data Protection Act 2023.

Briefly, the journey started with the Supreme Court laying down fundamental tenets of the Right to Privacy, with special emphasis on the situation in the digital context in 2017, in the case of Justice K.S. Puttaswamy v. Union of India. Thereafter, the Central Government constituted a committee of experts under the Chairmanship of Retd. Justice B.N. Srikrishna, which came out with a Report in 2018, in order to understand the practical aspects of data protection & privacy of individuals. Soon after that, the Personal Data Protection Bill was introduced in 2018, which was replaced by the Personal Data Protection Bill 2019. This 2019 version was referred to a Joint Parliamentary Committee, which submitted its feedback on the Bill via its Report in December 2021. Based on the Committee's recommendations & industry input, the Digital Personal Data Protection Bill 2022 was introduced. Finally, another version in the form of the Digital Personal Data Protection Bill 2023 was passed to culminate into the Digital Personal Data Protection Act of 2023. Thus, we see the Act has continuously evolved and comes at the end of a long-drawn out process of consultation, dialogue and engagement.

In pursuance of operationalizing the Act, the Ministry of Electronics and Information Technology (MeITY) released the much-awaited Draft Digital Personal Data Protection Rules on January 3, 2025.

This Report by the Centre for Cyber Laws, NLU Delhi is a humble contribution to the national (and global) engagement & discourse on the DPDP Rules in order to ensure that the final version of the Rules effectively implements the principles of the Act.

About NLUD

The primary objective of the University is to evolve and impart comprehensive and interdisciplinary legal education that is socially relevant. Through this education, we aim to promote legal and ethical values and foster the rule of law and the objectives enshrined in the Constitution of India. Furthermore, the University works toward the dissemination of legal knowledge and its role in national development, so that the ability to analyze and present contemporary issues of public concern and their legal implications for the benefit of the public is improved. These processes strive to promote legal awareness in the community and to achieve political, social, and economic justice.

Many believe that the path of liberalization we embarked upon in the early 90s unleashed India's potential. Undoubtedly the country has undergone vast changes in all spheres and we see a more confident India asserting itself on the global stage. However, this progress has come with very significant challenges to the country. India's various social classes are yet to be assimilated; their participation in the process of governance remains fractured. Cumulative progress needs to be fair and equitable. And integral to that is a legal system that empowers the marginalized, is just and fair in letter and spirit, and most importantly, does not use the law as a tool of oppression.

Our sincere endeavour is to make legal education and justice education, an instrument of social, political, and economic change. Each individual who is part of this institution must be remembered for the promotion of social justice. Our students will not only be shaped as change agents as the country achieves its social and developmental goals, but will also be equipped to address the imperatives of the new millennium and uphold the Constitution of India.

About the Centre

The Centre for Cyber Laws has been established to understand the socio-legal issues related to ever-evolving cyberspace. Cyberspace is infinite and has the potential to grow and evolve infinitely. The issues related to cyberspace are also evolving with the advancement of information technology. The global IT revolution and the emergence of new technologies such as artificial intelligence, the Internet of Things, the e-commerce industry, new forms of virtual currency, issues pertaining to the governance of cyberspace and more particularly the post-pandemic new world order have necessitated the need to focus on the legal research pertaining to new kinds of cybercrimes, issues related to cyber security and data protection and online privacy laws and above all into the new evolving cyberspace trends and patterns which shall shape the future of human civilisation and legal issues pertaining to it.

Vision & Objective

The vision of the Centre for Cyber Laws is to create a research-oriented space through which further research, discussions and deliberations on issues related to cyberspace and cyber laws can be done. The objective of the Centre is to bring professionals, academicians, cyber law experts, technology experts, law enforcement agencies, researchers and students together to have focused deliberations, discussions and debates related to issues of cyberspace and cyber laws. The Centre also aims to spread awareness related to various issues related to cyber laws such as cybercrimes, contraventions and cyber security issues.

LIST *of* ABBREVIATIONS

Abbreviation	Expanded form
Aadhar Act	The Aadhar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[1]
CCPA	California Consumer Privacy Act of 2018[2]
CM	Consent Manager
DF	Data Fiduciary
DP	Data Principal
DPA	Data Protection Authority
DPB	Data Protection Board of India
DPDP Act; the Act	Digital Personal Data Protection Act 2023[3]
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation of the European Union[4]
Puttaswamy	Hon'ble Supreme Court in the case of Justice *K.S. Puttaswamy v. Union of India*, decided in 2017[5]
SDF	Significant Data Fiduciary
Srikrishna Committee Report	Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna *A Free and Fair Digital Economy*, released in 2018[6]

[1] accessible at Aadhaar_Act_2016_as_amended.pdf
[2] accessible at Codes Display Text
[3] accessible at Digital Personal Data Protection Act 2023.pdf.
[4] accessible at General Data Protection Regulation (GDPR) – Legal Text
[5] accessible at justice k s putiaswamy (retd.), union of india and ors. 1700550294.pdf
[6] accessible at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

This page is intentionally left blank.

TABLE *of* SUGGESTIONS

Rule	Provision	Gap	Suggestion	Jurisprudence/Basis
NOTICE FOR OBTAINING CONSENT				
3(a)	Notice given by Data Fiduciary to Data Principal. Must be presented independently of any other information given by DF.	Lack of accessibility in the form of language barriers. While multiple aspects of the Act & Rules make it possible to ensure ease of data protection rights, the very medium also needs to convey the same.	Add provision to give the notice in vernacular languages as well, i.e., Eighth Schedule of the Indian Constitution (22 languages).	Requiring notice in multiple languages "*where necessary and practicable*" was provided under clause 7(2) of the 2019 Bill and clause 8(2) of the 2018 Bill. No comments in the JPC Report on clause 7 (deemed approval).[7] Srikrishna Committee Report acknowledges that it may be necessary for information (in the notice) to be conveyed in multiple languages.[8] Under the principles of GDPR, the Dutch DPA fined TikTok €750,000 for violating the privacy of young children by providing the notice (during installation & otherwise) only

[7] Joint Parliamentary Committee Report on the 2019 Bill, accessible at 17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf
[8] Srikrishna Committee Report on *A Free and Fair Digital Economy*, Page 58, accessible at Data_Protection_Committee_Report.pdf

				in English – which was not always understandable.[9]
3(b)	Notice given by Data Fiduciary to Data Principal. Inclusion of certain coordinates.	Minimum requirement is inadequate. Additional disclosures are required for the meaningful dissemination of educating data principals about their rights and providing a truly empowered opportunity to give consent.	Should include the rights of the data principal to withdraw her consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on lawful grounds; the source of such collection, if the personal data is not collected from the data principal; the individuals or entities including other data fiduciaries or data processors,	Suggested additions taken from 7(1) of the 2019 Bill and 8(1) of the 2018 Bill. No comments in the JPC Report. Consistent with S. 5, DPDP Act 2023 and principles of the Act & Rules.

[9] Dutch DPA: TikTok fined for violating children's privacy | European Data Protection Board

			with whom such personal data may be shared, if applicable; information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; the period for which the personal data shall be retained the existence of and procedure for the exercise of rights of the DP.	
NOTICE OF BREACH				
7	Intimation of personal data breach.	The current requirements for giving notice are inadequate, even compared to the current requirements of consent.	Notice to follow the same standards as that of notice for consent (plain language etc.)	Principles of Act & Rules (accessibility by data principals)
7(1)	Intimation of personal data breach.	Lack of timeline for notification.	Specify a reasonable timeline for the notification of breach to each DP by the DF.	R. 7(2) gives the timeline of notification to the Board as within 72 hours or an extension obtained in writing from the Board. Here too, this clause of timeline can be added in order to provide certainty to the DP and maintain the principles of transparency.

ERASURE OF PERSONAL DATA				
8(1)	Time period for specified purpose to be deemed as no longer being served.	Applicability of time period after which purpose of collection of personal data is deemed to be served should be widespread & applicable to all. Basis on which entities are classified to which thresholds are applicable needs to be more comprehensive.	Firstly, requirements should be applicable to *all* not specified DFs.[10] Secondly, even if numerical thresholds apply, they should be on the basis of number of active users & not registered users as registered users do not give an idea of the real use & impact of a platform.	For the specified purposes, the following are required to erase personal data except as necessary for compliance with any law. (i) e-commerce DP 2cr+ (ii) online gaming intermediary DF 50L+ (iii) social media intermediary 2 cr+. All figures based on registered users.[11]
8	Time period for specified purpose to be deemed as no longer being served.	Ambiguity in defining "specified time period" across various contexts. Potential data retention conflicts with other legal obligations.	Establish industry-specific timelines for data retention. Clarify exceptions where legal compliance necessitates prolonged retention.	Based on the GDPR's "data minimization"[12] and "storage limitation" principles.[13] Supreme Court guidelines on data retention in *PUCL v. Union of India.*

[10] Third Schedule classifies by volume (no. of registered users) depending on the type of DF.
[11] Third Schedule of the Draft DPDP Rules 2025.
[12] Article 5(1)(c), GDPR
[13] Article 5(1)(e), GDPR

CONSENT MANAGER				
4(4)	Registration and obligations of Consent Manager.	Potentially burdensome obligations. The Consent Manager (CM) faces cancellation of registration and penalties in case of non-adherence to conditions & obligations laid down. This has the potential to disincentivise companies from registering as CMs. Further, the DPB may on its satisfaction revoke the license of the CM, which makes the DPB too powerful.	The Central Government must formulate and notify a detailed framework on the functioning of CMs. This would include CMs being a body corporate with defined roles, powers, functions and so on. Monitoring of CMS must also be well-defined. This is important given that the volume of data being dealt with is unmatched and personal data is not sector-specific, thus having wide-ranging impact.	SEBI regulates market intermediaries (like stock brokers, stock exchanges, Investment Advisers, Research Analysts, etc.). TRAI, RBI and other sectoral regulators release information and guidelines for the operation of intermediaries (by whatever name so called) in their respective sectors.
VERIFIABLE PERSONAL CONSENT (IN THE CONTEXT OF CHILDREN)				
10(1)	Verifiable consent for processing of	Data collected by the mechanism to verify consent is not specifically protected.	Verification through entities trusted by the Government – add: such verification data	R. 3(vii) & 3(viii) of the SPDI Rules to be invoked.

	personal data of child or of person with disability who has lawful guardian.		including virtual token to be treated as "*sensitive personal data*" and to be subject to the SPDI Rules.[14]	The recent amendment[15] to the Aadhar Act allows private entities to use the Aadhar for authentication, including age. This needs to be handled with utmost care in order to abide by the principles of the DPDP Act and protect individual data principals. Although the current framework, via amended rules, provides for certain safeguards like submitting a proposal & justification statement before the use of Aadhar, anonymous verification is a better option in the interest of DPs given the enormous volume of data that will be dealt with (through *all* websites).
10(1)(b)	Verifiable consent for processing of personal data of child or of	No reason to invest in anonymous mechanisms of age verification over the use of Aadhar.	Rule to include provision incentivising investment in anonymisation mechanisms. This can be in-house by a DF or as a service availed by DFs,	One such mechanism could be Aadhar verification by OTP wherein a child's Aadhar phone / contact number is linked to their parent, without accessing data of Aadhar itself.

[14] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, [भाग II- खण्ड 3(i)] भारत का राजपत्र : असाधारण 7.

[15] Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025.

	person with disability who has lawful guardian.		which would be deemed related parties. Such verification can happen by mapping virtual tokens.	Examples of services (anonmyous verification / virtual tokens) provided in other comparative jurisdictions include Yoti in the UK[16] and YOid in Spain.[17] An incentive to invest in such virtual mapping could be providing points towards positive credit rating, or a similar / equivalent framework for personal data protection.
10(2)	Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian.	No obligation to ensure consent being provided for children is by their parents / guardians only, the Rule merely requires to ensure that the person giving consent is *an* adult.	Add due diligence requirements for the identification of a parent, similar to the requirements for guardian(s).	The idea is to link the claimant parent to the child in order to provide lawful consent. Misuse is possible in case of the requirement of *any* adult providing consent. Therefore, it becomes important to impose a duty on the DF to verify this link.

[16] Age verification tools for online customers and custom-built apps · Yoti
[17] Verify your legal age without losing your anonymity - YOiD

10 explanation	Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian.	Current provisions provide age-gating content for *all* sites and for all children up to the age of 18. The age limit is too high & must be brought down.	First, restrictions should apply only for specific notified sites like for instance gambling, etc. Second, even if restrictions apply to all kinds of content it should only be for beyond a certain age and to this end, the definition of child under this Rule should be amended to mean a person below the age of 16 years.	The GDPR stipulates a child to be a person under the age of 16 years, with Member States having an option to bring this down to 13 years. The US stipulates parental consent for *certain* sites for persons under the age of 13 years.[18]
RIGHTS OF DATA PRINCIPALS				
13	Rights of Data Principals, including access, erasure, grievance redressal, and	1. Absence of clear timelines for grievance redressal response by Data Fiduciaries. 2. No standardized method for identity verification when a Data Principal exercises rights.	1. Include a mandatory timeline (such as 15-30 days) for grievance redressal responses. 2. Provide standardized methods for Data Fiduciaries to verify the identity of Data	Justice K.S. Puttaswamy v. Union of India (2017) emphasized the protection of individual privacy rights, which includes timely redressal and clear procedural safeguards for exercising data rights. The General Data Protection Regulation (GDPR), under Art. 12 and 15, mandates

[18] Children's Online Privacy Protection Rule ("COPPA") | Federal Trade Commission

	nomination rights.	3. Lack of procedural clarity on how nomination rights can be practically exercised. 4. Insufficient mechanisms for ensuring transparency in cross-platform grievance resolution.	Principals, such as multi-factor authentication. 3. Lay down procedural guidelines for nomination rights, including documentation and notification protocols. 4. Establish interoperability standards for grievance redressal systems across Data Fiduciaries and Consent Managers.	response to data access and erasure requests within one month, serving as a global benchmark. The California Consumer Privacy Act (CCPA), under Sec. 1798.130(a), explicitly mandates response timelines and identity verification measures. The Srikrishna Committee Report (2018), stressed the need for strong grievance redressal systems to protect data rights. The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) Recommendations on Digital Identity[19] advocates for multi-layered identity verification in digital environments.
DATA PROCESSING				
5	Processing for provision or issue of	Lack of explicit guidelines on accountability for misuse or data	Incorporate specific legal remedies and penalties for misuse of personal data by	Jurisprudence surrounding "Right to Privacy" as held in *Puttaswamy* mandates

[19] accessible at https://www.itu.int/rec/T-REC-X.1251-200909-I

	subsidy, benefit, service, certificate, licence or permit by State and its instrumentalities.	breaches when public data is processed by the State.	State entities. Ensure regular audits of data processing practices.	accountability and security in processing personal data.
14	Data transfers outside India are subject to conditions imposed by the Central Government.	Absence of clear criteria for determining permissible jurisdictions for data transfers.	Publish a comprehensive whitelist of jurisdictions with adequate data protection frameworks.	Jurisprudence from Schrems II decision[20] in the EU invalidating Privacy Shield emphasizes the need for robust data protection in cross-border transfers.

[20] *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems,* accessible at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155

Second Schedule	Establishes standards for lawful processing, accuracy, retention, security safeguards, accountability, and transparency.	Lack of detailed accountability measures for State actors processing sensitive data.	Mandate independent data protection audits and specify penalties for violations.	Basis from OECD Privacy Guidelines[21] and global standards for lawful processing.
DATA PROTECTION OFFICER				
9	Contact information of person to answer questions about processing.	No clear definition of qualifications or expertise required for DPOs.	Set qualifications and training requirements for DPOs to ensure effective handling of data processing issues.	Derived from global practices such as the Contact information of person to answer questions about processing requirements for DPOs (Article 37).

[21] *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data*, Guideline No. 7, accessible at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188#mainText

9	Contact information of person to answer questions about processing.	Absence of explanation of modalities on the operation of such a person, including who they will be.	In order to promote efficiency, the said person (under R. 9) can be from the office of the CM.	There is an overlap in the role of this functionary (not explicitly mentioned in the Act) and the Consent Manager (who is expected to fulfil the role of grievance redressal for the DP and act in the interest of the DP). In the interest of efficiency, since both the person under R. 9 & the CM have a duty towards the DP, the person referred to under R. 9 can be from the office of the Consent Manager.
DATA PROTECTION BOARD				
18	Procedure for meetings of Board and authentication of its orders, directions and instruments.	1. Absence of detailed protocols for emergency decision-making criteria, beyond recording reasons. 2. No explicit guidelines on transparency requirements for agenda-setting by the Chairperson. 3. Limited procedural safeguards for disclosing conflicts of interest and	1. Introduce more detailed guidelines for defining emergent situations requiring immediate Board decisions. 2. Require public disclosure (at least internally) of the agenda-setting criteria for Board meetings to ensure procedural transparency.	The prohibition against Members voting where a conflict of interest exists follows the principle of *nemo judex in causa sua* (no one should be a judge in their own case). Similar procedures for decision-making and quorum requirements can be seen in entities like SEBI and TRAI. Courts have often emphasized transparent and participative decision-making in

		mechanisms to resolve disputes regarding the same. 4. Insufficient mention of digital authentication security standards.	3. Implement clear procedural mechanisms for handling conflicts of interest, including a formal process for Members to disclose potential conflicts in writing. 4. Include requirements for secure digital authentication standards to protect Board decisions and records.	administrative bodies (Refer: *Maneka Gandhi v. Union of India* (1978) and *Centre for PIL v. Union of India* (2011)).
19	Board functions as a digital office and may adopt techno-legal measures.	No standards specified for the adoption of digital technologies.	Develop a comprehensive digital strategy guideline, including cybersecurity measures and remote hearing protocols.	Inspiration must be drawn from the Supreme Court's E-Committee Guidelines[22]and the Government's eCourts Integrated Mission Mode Project.[23]
20	Terms and conditions of appointment	1. Absence of detailed recruitment criteria or transparent procedures for selection.	1. Develop comprehensive recruitment and selection guidelines to ensure a	Ensuring transparency in public appointments aligns with constitutional

[22] accessible at https://ecommitteesci.gov.in/document-category/policy-action-plan-documents-en/
[23] accessible at https://ecommitteesci.gov.in/project/brief-overview-of-e-courts-project/

	and service of officers and employees of Board	2. No explicit mention of performance evaluation mechanisms or professional development opportunities for employees. 3. Ambiguity regarding autonomy in appointment decisions vis-à-vis the Central Government's overarching control.	transparent and merit-based hiring process. 2. Include performance evaluation mechanisms and professional development frameworks to enhance employee efficiency and satisfaction. 3. Clarify the extent of autonomy granted to the Board in appointment decisions while maintaining the Central Government's oversight.	values (Refer: *Centre for Public Interest Litigation v. Union of India* (2011)). Courts have underscored the importance of clear and transparent service conditions for public employees (Refer: *State of Haryana v. Piara Singh* (1992)).
22	Calling for information from Data Fiduciary or intermediary	Bypassing consent undermines privacy protections and Supreme Court safeguards against state surveillance.	Any call for information shall be made via a formal written request by the authorities to the data fiduciary. Clear safeguards must be in place, including oversight by a review committee and a	The government has the authority to demand data from data fiduciaries and can exercise broad discretion without the consent of the data principal for reasons listed under the 7th Schedule. The agents requesting data are appointed by the government.

			requirement for requests to specify the intended use of the information. Companies must inform individuals when their data is requested by the state, ensuring that such requests comply with established guidelines and the three-part test of **legality, necessity, and proportionality** from. *Puttaswamy*. Additionally, an appeal process and an independent oversight mechanism should be implemented to uphold transparency and accountability.	Intercepting communications violates the constitutional right to life and personal liberty unless done through legally established safeguards. Specific safeguards for such interceptions were mandated in PUCL v. Union of India[24]. Any demand for data must be reasonable, necessary, and proportionate. Additionally, any government action affecting a citizen's right to privacy must comply with the *Puttaswamy* standards. These standards require: **Legality**: A valid law must justify the action. **Legitimate State Aim**: The action must serve a valid government purpose, such as national security, crime prevention, or social welfare. **Proportionality**: The action must be reasonable and not excessive in relation to its purpose.

[24] (1978) 1 SCC 248

				These principles ensure that government actions are lawful, fair, and do not disproportionately infringe upon an individual's right to privacy.
SIGNIFICANT DATA FIDUCIARY				
12(1) & 12(2)	Additional obligations of Significant Data Fiduciary	The DPDP mandates annual, organization-wide DPIAs and audits, regardless of data processing changes, with submissions to the DPB, creating unnecessary burdens and inefficiencies for SDFs.	The requirement to conduct DPIAs and audits on an annual, whole-organization basis should be reconsidered. DPIAs must not only be an annual requirement. Instead, DPIAs should also be triggered by significant changes in data processing or risk profiles, and audit submissions should be more aligned with global best practices.	The DPDP requires SDFs to conduct annual DPIAs and audits on a whole-organization basis, rather than when there are changes in data processing activities or risk profiles. DPIAs should not be limited to an annual requirement. Instead, they must also be conducted whenever there are significant changes in data processing or risk profiles. Additionally, audit submissions should be better aligned with global best practices. While DPIAs and audits promote data protection, the absence of clear guidelines on their scope may result in inadequate assessments. Reporting to the DPB could

				become a mere formality without effective external oversight.
12(3)	Additional obligations of Significant Data Fiduciary	Lack of clear guidelines on due diligence measures for SDFs to assess algorithmic risks to data principals' rights. Lack of a strict standard for compliance.	The government shall provide clear guidelines on the scope, textend and nature of the due diligence. The risk assessment criteria, methodologies, documentation, transparency standards, and independent oversight for algorithmic due diligence, preferably in a standard format, must be provided to ensure consistent implementation. Furthermore, the current due diligence standard requires that the algorithmic software be "not likely" to pose a risk. This language imposes a lower threshold for fulfilling SDF's	The rules require SDFs to verify that their algorithmic software does not pose risks to DPs' rights but fail to specify the exact due diligence measures to be followed. This lack of clarity creates uncertainty, forcing businesses to interpret and implement compliance on an individual basis, which may lead to inconsistent or inadequate safeguards. The current due diligence standard, requiring that algorithmic software be "unlikely" to pose a risk, imposes a weak obligation on SDFs. This revision is required to ensure stronger, clearer accountability and protection for data principals. The term "not likely" sets a low threshold, potentially allowing risks to persist. An absolute obligation would compel SDFs to

			obligation, as it only requires a minimal likelihood of risk. The standard should be revised to impose an absolute duty on the SDF to ensure that no risks to data principals exist by omitting the ambiguous term "not likely."	proactively eliminate any risks, ensuring more robust safeguards for personal data and aligning with the higher legal standards for privacy protection.
12(4)	Additional obligations of Significant Data Fiduciary	The lack of clear criteria for data transfer restrictions creates uncertainty and potential arbitrary limitations.	The DPDP Rules should clearly define the scope of data transfer restrictions, specifying whether they apply to certain data categories or specific organizations, to provide greater clarity and reduce operational uncertainty for SDFs.	The DPDP Rules allow the Central Government to impose data transfer restrictions, but it is unclear whether these apply to specific data categories or organizations, potentially creating uncertainty and operational challenges for SDFs. Clear definitions are necessary to ensure SDFs can comply effectively and avoid operational disruptions. Data fiduciaries must not face unreasonable and arbitrary restrictions or at the discretion of the

				government without any rationale. Clear, objective criteria must be defined to prevent arbitrary restrictions, ensuring that data transfers are only limited when absolutely necessary for legitimate reasons. This will facilitate smoother operations, help businesses adhere to regulations, and prevent unnecessary compliance burdens while safeguarding privacy and data protection rights. Further, the requirement to localize data for Significant Data Fiduciaries raises concerns about cross-border data transfers and could have a significant impact on international trade in services.

Concluding Remarks

The Centre for Cyber Laws has submitted these comments to the Ministry of Electronics & Information Technology.

The Centre appreciates the collaborative efforts undertaken by MeITY.

We strongly believe that the modifications, as proposed above, will enhance data protection of individuals, and hence recommend that these be introduced and implemented at the earliest in line with principles of the Digital Personal Data Protection Act 2023.

Dated: 22nd February 2025