COMMON CAUSE

Dedicated to Public Causes Since 1980

Common Cause House, 5, Institutional Area,
Nelson Mandela Road, Vasant Kunj, New Delhi –110 070. Phone: 26131313
www.commoncause.in; e-mail: commoncauseindia@gmail.com; contact@commoncause.in

Ministry of Electronics and Information Technology,
Government of India,
New Delhi

February 14, 2025

Recommendations for Draft Digital Personal Data Protection Rules (DPDP) 2025

General Comments

1. The draft Digital Personal Data Protection (DPDP) Rules 2025 need to address a pressing concern that has been voiced across India by civil society organizations – the amendment to section 8(1)(j) of the Right to Information (RTI) Act. Section 44(3) of the DPDP Act (2023), amending section 8(1)(j) of the RTI Act, cripples the RTI Act by immensely expanding the purview of the exceptions granted by Section 8. No piece of personal information can now be divulged, due to the current amendment. The RTI Act has played a paramount role in the fight against corruption. It has also improved governance, empowered citizens, and strengthened participatory democracy. In our view, it is an important step towards building better transparency and accountability. We strongly recommend a change to Section 44(3) of the DPDP Act (2023), but since such recommendation is not under the ambit of the DPDP Rules 2025, we recommend that the Rules provide clarity on Section 44(3) by establishing that personal information should be disclosed when such disclosure concerns any public activity or interest.

2. The feedback/comments submitted by stakeholders for the Rules should be made publicly available.

3. The Rules need to overall meet the constitutional requirements outlined in *K.S. Puttaswamy v. Union of India* (2017).

4. Terms such as “sovereignty and integrity of India” and “security of the state” are subject to wide interpretation. The use of such vague terms can allow infringements on the right to privacy as well as allow prejudicial targeting of people perceived by the government in power as dissenters or critical of the government. Specific language should be used, detailing the circumstances in which mandatory disclosure of information by Data

Fiduciaries is warranted, and the government be exempted from the provisions of DPDPA 2023.

5. Though included in our specific recommendations, we want to expressly point out the highly concerning **Fourth Schedule** of the DPDP Rules 2025, which lays out exceptions for the processing of children data. The liberty, privacy, and autonomy of children and their parents are impacted here and the adverse effects stemming from such exceptions traverse the digital realm and pour into the physical world. There is potential for the excessive surveillance of children and institutions have been granted the power to act on the "best interests" of the child without permission or consent from her parents. A misalignment regarding the "best interests" of the child between institutions and parents can cause harm to the physical and mental health of a child, create tension between institutions and parents, and disrupt harmony amongst everyone involved.

6. Another source of major concern is the independence of the Data Protection Board. Under the current Rules, the Board would be under the thumb of the Central Government, affecting the enforcement of the DPDP Act and the impartiality of the Board.

7. Our more specific recommendations are as follows:

<u>Specific Recommendations</u>

Rule/Schedule Number	**Rule/Schedule Title**	**Content of Rule/Schedule Under Scrutiny**	**Recommendations**	**Comments**
Rule 3	Notice given by Data Fiduciary to Data Principal	Section (b)	New sub-section. "(iii) with which parties such personal data is being shared with"	When providing consent, the Data Principal should be informed on **whom her data is being shared with**. This clause exists in the Canadian PIPEDA. Personal data is often shared with third-party organizations by the Data Fiduciary for the provision of services.

Rule 3	Notice given by Data Fiduciary to Data Principal	Section (b)(ii): "the specified purpose of…"	Modify the language. Change "the specified purpose of" to "the specified purpose(s) of".	Data Fiduciaries can have more than one purpose for collecting and processing personal data. The current language can create a loophole where Data Fiduciaries can pick and choose which purpose they want to inform the Data Principal of, or use overly broad language to bring numerous purposes under a single umbrella.
Rule 7	Intimation of personal data breach	Section (1)(a)	Include "an itemized list of personal data that was breached or leaked"	The current phrasing does not necessitate informing the Data Principal precisely which personal data of hers was breached or leaked. The Data Principal must know the particulars of her personal data that was breached or leaked.
Rule 8	Time Period for specified purpose to be deemed as no longer being served	Section (2) : "…unless she logs into her user account… or exercises her rights in relation to the processing of such personal data."	(i) Remove "unless she logs into her user account." (ii) Remove "exercises her rights in relation to the processing of such personal data" (iii) Specify the timeline for when the user should log into her user account, or exercise her rights in relation to the processing of such personal data. (iv) Apply rule to all personal data processing	(i) Under the current phrasing, a Data Principal logging into her user account is accepted as reason enough to not provide her with the notice of data erasure and extends the data retention period. A user logging into her account does not necessitate that she is in need of the Data Fiduciary's services (accessing account details, downloading invoices, etc.). Furthermore, as laid out in the **Third Schedule, enabling access to her personal account is not a purpose for the processing of personal data**, thereby the current phrase contradicting the Third Schedule.

				(ii) A user exercising her rights is an overly broad term to be included here. For instance, a user exercising her right to nominate another individual in the event of her death holds no grounds to preclude her from receiving a data erasure notice. (iii) The section is ambiguous on when the users' actions preclude them from receiving a data erasure notice. Does logging into her account 1 year before the data erasure time period allow the Data Fiduciary to not issue a notice? Same applies to exercising her rights. (iv) A three-year period has been prescribed, after which the specified purpose would be deemed to be no longer being served (after which personal data must be erased) for the following entities: • e-commerce entity with not less than two crore users in India; • online gaming intermediary with not less than 50 lakh users in India; and • social media intermediary with not less than two crore

				users in India. The three-year time has been prescribed only for the above stated entities. It does not extend to regulated entities (banks, non-banks, payment service providers, asset management companies and other intermediaries) and would require further clarity from MeitY for data retention periods applicable to them.
Rule 10	Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian	Section (1) and Section (2)	Provide clarity on what happens to parents'/lawful guardian's data once verification is complete. Either the provided data must be deleted post-verification or must only be made accessible to the Data Protection Officer post-verification, until the child turns 18 years of age. This measure will prevent abuse of such data by the Data Fiduciary.	The current rule does not provide direction on what is to be done with the personal data collected from a parent/lawful guardian. This data will be sensitive in nature as it is a government-issued ID/document and must be protected with utmost security and not utilized for any other purposes.
Rule 12	Additional obligations of Significant Data Fiduciary	Section (1)	Set standards for what constitutes a Data Protection Impact Assessment. These can include: (i) Segregation of data based on sensitivity. (ii) Amount of data held by the Data Fiduciary. (iii) Necessity and proportionality of collected data. (iv) Purposes of processing.	The current Rule has no guidelines on what standards and information needs to be present in the Data Protection Impact Assessment. Leaving the DPIA to the Significant Data Fiduciary's discretion will result in assessments of variable depth and quality being submitted to the Board. The Board must release a template for the DPIA and require the SDFs to follow such template to ensure consistency and

			(v) Measures taken to mitigate risk of a data breach and subsequent evaluation of those measures against industry standards as well as best practices. (vi) Consultations with privacy, data security, and technology experts.	transparency.
Rule 12	Additional obligations of Significant Data Fiduciary (SDF)	Section (3)	(i) Replace “not likely” with “do not” (ii) Replace “rights of Data Principals” with “rights of Data Principals or cause harm to a person.” (iii) Include the definition of “harm” under this section.	(i) Using the phrase “not likely” is vague and open to interpretation. Even when the algorithmic software can pose risks to the rights of Data Principals, they can still be used without any modifications. (ii) Significant Data Fiduciaries must also ensure that their algorithmic software do not cause harm to the Data Principals. Harm is not covered under the Rights of the Data Principals as outlined in Chapter 3 of the Act. As seen in cases of Facebook conducting emotional surveillance and present studies on TikTok’s algorithmic software adversely impacting adolescent and young adults’ mental health and body image, harms do arise out of algorithmic software and Data Principals must be protected against such harm. (iii) A detailed definition and constituents of harm can be found in the

				Canadian PIPEDA and Recital 75 of the GDPR. (iv) Corresponding DPDP Act Section (S. 10(1) and 10(2)): Lays down the indicative criteria basis which the Central Government may notify any data fiduciary or a class of data fiduciaries as SDFs, including: • the volume and sensitivity of personal data processed; • risk to the rights of Data Principal; • potential impact on the sovereignty and integrity of India; • risk to electoral democracy; • security of the State; and • public order. It also grants power to the Central Government to prescribe additional obligations for SDFs. However, • 'SDFs have not yet been notified by the Central Government. • The Draft Rules give the Central Government power to specify the nature of personal data that

				would have to be localised in India – an absolute bar on transfer outside India. This seems to be a departure from the DPDP Act to not impose a data sovereignty rule.
Rule 13	Rights of Data Principals	Section (1)	Include subsection "(c) rights of the Data Principals"	Data Principals should be informed of what rights they can exercise under the Act. Being informed of their rights helps them make an informed decision that suit the purpose of exercising their rights.
Rule 13	Rights of Data Principals	Section (3)	(i) Expand on what are "appropriate technical and organizational measures." (ii) Fix a time period for responding to grievances. An appropriate time for first response to a grievance would be within 72 hours. An appropriate time period for resolving the grievance will be 14 days. If the redressal requires extensive measures to be taken by the Data Fiduciary, the period, including the 14 days, can be extended to 30-45 days, with prior approval by the Board. After the elapse of the grievance redressal period, the Data Principal can approach the Board for redressal.	(i) This section is incredibly vague, provides no direction to Data Fiduciaries/Consent Managers on how to address grievances, and leaves the time period for grievance redressal up to the discretion of the Data Fiduciary/Consent Manager. (ii) A timeline should be established for grievance redressal as the current Rule does not establish one. The absence of such a timeline can lead to Data Fiduciaries not acting on grievances in a timely manner, Data Principals not having their rights respected, and more importantly cause harms to the Data Principal.
Rule 16	Appointm	Section (1)	Eliminate the involvement	Stemming from a criticism

	ent of Chairperson and other Members	Section (2) Section (3)	of the Cabinet Secretary of the India in the Search-cum-selection committee. The Search-cum-Selection committee could consist of experts specializing in privacy, information technology, law, and business administration, headed by the Secretary of the Department of Legal Affairs, Secretary of the Ministry of Electronics and Information Technology and the Attorney General of India. The Search-cum-Selection committee will report to the Parliament regarding the appointment of the Chairperson and Members of the Board.	of the Act itself, the independence of the Board is highly questionable owing to the overarching involvement of the Central Government in the constitution of the Board. The Board will be under the thumb of the Central Government, affecting its core operations and enforcement of the Act, especially when it concerns the State and its instrumentalities. These recommendations take after precedents in the EU, UK, Canada, and Australia whose equivalents to the Data Protection Board only report to the Parliament, thereby having the power to act independently and hold the government accountable.
Rule 18	Procedure for meetings of Board and authentication of its orders, directions and instruments	Add New Section	"(10) The Board shall meet once every three months to discuss the Board's status quo, pending complaints, and any other matters as they see fit for the effective functioning of the Board	Currently, there is no timeline set for the frequency of the Board's meeting. Apart from Section (1), there needs to be more specificity on the Board's meetings to assure its efficient functioning and provide a platform for its Members to discuss any emergent issues.
Rule 20	Terms and Conditions of appointment and service of officers and employees	Section (1)	Only the Board must have the authority to appoint its officers and employees.	As mentioned before, this Section further truncates the independence of the Board and it becomes an entity that is entirely constituted by the Central Government. The Board must have full autonomy over the appointment of its

	of the Board			officers and employees to ensure that it operates independently, transparently, and does not hesitate to hold the government accountable.
Rule 22	Calling for information from Data Fiduciary or intermediary	Add New Section	(3) A Data Fiduciary reserves the right to refuse any call for information if it decides that the requested information does not fulfill its stated purpose laid out in the Seventh Schedule. The Data Fiduciary's decision must be defended before the Board, and the Board will decide on the validity of the stated purpose for call for information and can subsequently either grant or deny the call for information.	The current Rule does not grant the Data Fiduciary any discretionary power over their data. Furthermore, it gives the State blanket powers to elicit any amount of information, without any transparency or accountability, for any purpose, by just furnishing the Data Fiduciary with one of the three purposes laid out in the Seventh Schedule. The purpose may or may not be true and there is neither oversight nor a measure to verify if the stated purpose is true. Therefore, this Rule creates a loophole that can be exploited for mass surveillance and serve any ulterior interests of government officials.
First Schedule	Part B Obligations of Consent Manager	Section (4)(b): "…information contained in such record, in machine-readable form."	Replace "machine-readable form" to "a text-based document in plain language."	A machine-readable form means that the document provided by the Consent Manager can be in source code, XML, JSON, or CSV format. These are not accessible to an average person and cannot be read by them. Hence, the provided data on such record should be in a text-based document in .docx or .pdf formats, and be presented in plain language

				that can be easily understood by the reader.
Third Schedule	Third Schedule	Entire Schedule	(i) Decrease the number of registered users for all classes of Data Fiduciaries. (ii) Increase the classes of Data Fiduciaries.	(i) The threshold of two crore and fifty lakh user accounts is too high a number. Even entities such as BigBasket, Swiggy, smaller banks, or ed-tech platforms (process sensitive data), do not possess 2 crore users. An acceptable limit for e-commerce entities would be 75 lakh users and 10 lakh users for gaming intermediaries. (ii) The current classes of Data Fiduciaries are very restricted. An umbrella term such as e-commerce entity is ambiguous and can lead to confusion for businesses over the application of the Rule to them. For instance, ed-tech, telecom, or streaming services can fall into other categories such as education, telecom, and video-on-demand entities.
Fourth Schedule	Part A Classes of Data Fiduciaries in respect of whom provisions of sub-sections (1) and (3) of section 9 shall not apply	S.No. 3. (3)(b) in the interests of safety of children enrolled with such institution.	"Interests of safety of children enrolled with such institution", must be expanded to specify when processing is lawful.	The broad nature of condition gives way to potential for abuse and justifies excessive surveillance of the child. What is more alarming is that parental consent is not required for this type of processing, thereby granting educational institutions full autonomy over the freedom, privacy, and interests of the child. There is also potential for education institutions to act

				adversely towards the child if misunderstandings arise between the institution and parents.
Fourth Schedule	Part B Purposes for which provisions of sub-sections (1) and (3) of section 9 shall not apply.	S.No.1 (2) and (3) (2) For the exercise of any power, performance of any function or discharge of any duties in the interests of the child, under any law for the time being in force. (3) Processing is restricted to the extent necessary for such exercise, performance or discharge.	Either **remove** the purpose and condition or **specify** what power, function, and duties can be administered for which **specific** interests of the child.	This is an **overbroad** purpose that has **no limits** and can be **extremely detrimental** to the liberty, privacy, and interests of the child and her parents if enacted. Parental consent and protection of a child from tracking, targeting, and monitoring are not measures that can be easily forgone nor taken for granted as authorized by this purpose and condition. This purpose and condition also have a very real potential for function creep and can be very easily abused by both public and private entities/authorities just by referring to their duties as being in the best interests of the child and being enabled by law.
Fourth Schedule	Part B Purposes for which provisions of sub-sections (1) and (3) of section 9 shall not apply.	S.No. 4. (2) (2) For ensuring that information likely to cause any detrimental effect on the well-being of a child is not accessible to her.	Change “detrimental effect” to “harm” and comprehensively define harm to include physical, mental, and financial harm.	Who decides what “detrimental effect” is? This is a broad and subjective term that should not be used here.