CUTS COMMENTS ON DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

SUBMITTED TO
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CUTS Comments on Draft Digital Personal Data Protection Rules, 2025

Published by

CUTS International
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Authors: Asheef Iqubbal and Krishaank Jugiani, Senior Research Associates, CUTS International

For any clarifications/further details, please feel free to contact: Asheef Iqubbal (aql@cuts.org) and Krishaank Jugiani (kju@cuts.org).

Acknowledgement: The authors are thankful for the support and guidance of Amol Kulkarni, Director (Research), CUTS International, who can be reached at amk@cuts.org.

© CUTS International, March 2025

The material in this publication may be reproduced in whole or in part and in any form for educational or nonprofit purposes without special permission from the copyright holders, provided the source is acknowledged. The publishers would appreciate receiving a copy of any publication which uses this publication as a source.

CUTS Comments on Draft Digital Personal Data Protection Rules, 2025

Background

Consumer Unity & Trust Society (CUTS) expresses gratitude to MeitY for inviting comments and suggestions on the draft Digital Personal Data Protection Rules, 2025.[1] CUTS looks forward to MeitY accepting the below suggestions and assisting in its efforts to empower consumers and lead to effective and optimum regulation- making to protect personal data of the consumers. We would be glad to make an in-person presentation of our submission before MeitY.

About CUTS

CUTS[2] is an independent, nonpartisan, and non-profit policy think and action tank that has been working towards enhancing the regulatory environment through evidence-based policy and governance-related interventions across various sectors and boundaries. In its 40 years of operation, CUTS has come a long way from being a grassroots consumer centric organisation headquartered in Jaipur, having centres in Delhi,[3] and Kolkata,[4] to now opening overseas Resource Centres in Vietnam,[5] Kenya,[6] Zambia,[7] Ghana,[8] Switzerland,[9] and in the United States of America.[10] CUTS has been actively representing consumers' interest before different state governments and central government ministries through various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE),[11] Centre for Consumer Action, Research & Training (CART),[12] Centre for Human Development (CHD)[13] and Centre for

[1]Draft 'Digital Personal Data Protection Rules, 2025', available at: https://innovateindia.mygov.in/dpdp-rules-2025/ - :~:text=The%20Ministry%20of%20Electronics%20and,President%20on%2011th%20August%202023.
[2]CUTS International – Consumer Unity & Trust Society, available at: https://cuts-international.org/
[3]CUTS Delhi Resource Centre, available at: https://cuts-international.org/DRC/
[4]CUTS Calcutta Resource Centre, available at: https://cuts-crc.org/
[5]CUTS Hanoi Resource Centre, available at: http://www.cuts-hrc.org/
[6]CUTS Nairobi, available at: https://cuts-nairobi.org/
[7]CUTS Lusaka, available at: https://cuts-lusaka.org/
[8]CUTS Accra, available at: https://cuts-accra.org/
[9]CUTS Geneva, available at: http://www.cuts-geneva.org/
[10]CUTS Global, available at: http://cuts-global.org/
[11]CUTS Centre for International Trade, Economics & Environment (CUTS CITEE), available at: https://cuts-citee.org/
[12]CUTS Centre for Consumer Action, Research & Training (CUTS CART), available at: https://cuts-cart.org/
[13]CUTS Centre for Human Development (CHD), available at: https://cuts-chd.org/

Competition, Investment & Economic Regulation (CCIER).[14]

CUTS works on various issues to foster an inclusive digital economy,[15] including issues of multi-party privacy,[16] behaviour monitoring of children's data,[17] verifiable parental consent[18] and other general issues of data protection,[19] data localisation,[20] children's data protection,[21] and encryption.[22]

CUTS also works with various ministries and government departments for advocacy efforts[23] on issues within digital economy, more recently on the draft broadcasting bill,[24] draft guidelines for prevention and regulation of dark patterns,[25] draft registration of consumer organisations (amendment) regulations[26], draft telecommunication mobile number portability regulations,[27] digital competition,[28] competitive neutrality,[29] among others.

Based on such evidence-based work, CUTS is pleased to submit its comments on the draft Digital Personal Data Protection Rules. We have observed a few critical issues in the draft Rules, which have been discussed in subsequent sections, along with a few

[14]CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), available at: http://www.cuts-ccier.org/
[15]Inclusive Digital Economy, available at: https://cuts-ccier.org/digital-economy/
[16]"My data or yours?" Unravelling Multi-Party Privacy (MPP) among Consumers of Digital Credit in India, available at: https://cuts-ccier.org/my-data-or-yours/
[17]Examining the Scope of Behaviour Tracking and Targeted Advertisement of Children and Suggesting an Optimum Regulatory Approach, available at: https://cuts-ccier.org/examining-the-scope-of-behaviour-tracking-and-targeted-advertisement-of-children-andsuggesting-an-optimum-regulatory-approach/
[18]Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries, available at: https://cuts-ccier.org/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-onconsumers-and-data-fiduciaries/
[19]Data Privacy and Consumer Welfare in India: Consumer Perception Analysis, available at: https://cuts-ccier.org/cdpp/
[20]Understanding the Impact of Data Localisation on Digital Trade, available at: https://cuts-ccier.org/understanding-impact-of-data-localization-on-digital-trade/
[21]Highlighting Inclusive and Practical Mechanisms to Protect Children's Data, available at: https://cuts-ccier.org/highlighting-inclusive-and-practical-mechanisms-to-protect-childrens-data/
[22]Understanding Consumers' Perspective on Encryption, available at: https://cuts-ccier.org/understanding-consumers-perspective-on-encryption/
[23]Advocacy, available at: https://cuts-ccier.org/advocacy/
[24]CUTS Comments on Broadcasting Services (Regulation) Bill, 2023, available at: https://cuts-ccier.org/pdf/comments-on-draft-broadcasting-services-bill-2023.pdf
[25]CUTS Comments on Draft Guidelines on Prevention and Regulation of Dark Patterns, available at: https://cuts-ccier.org/pdf/comments-on-draft-guidelines-for-prevention-and-regulation-of-dark-patterns.pdf
[26]CUTS comments on TRAI Consultation Paper on the draft Registration of Consumer Organisations (Amendment) Regulations, 2023, available at: https://cuts-ccier.org/pdf/cuts-submission-to-trai-on-registration-of-consumer-organisations-amendment-regulations.pdf
[27]CUTS comments on Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023, available at: https://cuts-ccier.org/pdf/comments-on-trai-consultation-paper-on-draft-telecommunication-mobile-number-portability-regulations-2023.pdf
[28]CUTS comments on Draft Digital Competition Bill, 2024, available at: https://cuts-ccier.org/pdf/comments-on-digital-competition-bill-2024.pdf
[29]Promoting Competitive Neutrality in Government Using Advocacy, available at: https://cuts-ccier.org/pdf/promoting-competitive-neutrality-in-government-using-advocacy-june-20-2023.pdf

recommendations to address them.

CUTS' General Comments

In line with the enactment of the DPDP Act, we welcome MeitY's efforts in conducting stakeholder consultations on the published Draft Digital Personal Data Protection Rules, 2025 (DPDP Rules, 2025). These Rules expound on the Act's provisions and provide guidance for their implementation with the intention of balancing innovation, privacy, and efficiency. While this is a positive step, some rules require further discussion to ensure that the data protection framework effectively balances the interests of all relevant stakeholders, including businesses, the state, and consumers and does not result in any unintended adverse consequences. It is also important to ensure that Rules operate within the scope prescribed by the Act and do not venture beyond it.

a. Use of Regulatory Impact Assessment (RIA) Mechanisms

The draft DPDP Rules aim to operationalise the DPDP Act, providing necessary details and implementation framework. Given the broad impact the Rules may have on various stakeholders, including data principals and data fiduciaries, it is crucial to assess their effectiveness and potential consequences before finalisation.

To ensure that the Rules achieve their intended objectives without imposing unnecessary costs, including compliance and administrative burdens, conducting a Regulatory Impact Assessment (RIA)[30] – including a Cost-Benefit Analysis – is essential. Suboptimal regulations can lead to unintended costs, reduce regulatory efficiency, and create barriers to compliance, ultimately hindering the effectiveness of the DPDP Act.

An RIA enables a systematic evaluation of the direct and indirect impacts of regulatory proposals using consistent analytical methods. It provides a checks-and-balances mechanism to ensure that the government exercises its regulatory authority in a manner that effectively protects the data rights of Indian citizens while avoiding excessive burdens on businesses and service providers. For instance, the Rules envisage specific mechanisms for obtaining verifiable parental consent. It would be beneficial to assess whether alternative approaches could achieve the same regulatory objectives more efficiently, minimising costs while maximising benefits for data principals.

To this end, CUTS has developed an RIA toolkit[31] which involves a participatory

[30]Regulatory Impact Assessment (RIA), available at: https://cuts-ccier.org/regulatory-impact-assessment/
[31]REGULATORY IMPACT ASSESSMENT TOOLKIT, available at: https://cuts-ccier.org/pdf/Regulatory_Impact_Assessment_Toolkit.pdf

approach via a public consultation to assess such impact, determine costs and benefits, and select the most appropriate regulatory proposal. It is, therefore, recommended that the government engages with organisations experienced in conducting RIA, before finalising provisions of the new law. Engaging stakeholders through structured consultations will help refine regulatory provisions, address concerns from industry and civil society, and enhance compliance feasibility. Additionally, these consultations should not be limited to Tier-I cities but should also happen in Tier-II and III towns, where real challenges often emerge because of challenges like lower digital literacy and limited regulatory awareness. This will ensure that the regulatory framework is informed by diverse perspectives, including those of smaller businesses, regional service providers, and affected communities, leading to more inclusive and informed policy decisions. This will ensure that the DPDP Rules are balanced, effective, and aligned with global best practices, fostering a data protection regime that is both protective and enabling for India's digital economy.

b. Support Consumer Interest Groups and Raise Awareness in Data Principals

The draft DPDP Rules emphasise the protection of digital personal data for India's digital citizens. In line with this objective, the Right to Grievance Redressal must also be effectively safeguarded. Ensuring that data principals can enforce their rights requires not only a strong grievance redressal mechanism but also awareness-building and capacity-enhancement initiatives.

To support this, it is recommended that the Data Protection Board assist relevant stakeholders–including central and state governments, Data Fiduciaries, and other entities–in conducting consumer awareness and capacity-building activities as part of their responsible business practices. For example, awareness efforts should focus on critical provisions of the Rules, including notice requirements, safety standards, and breach disclosure obligations of data fiduciaries, among others. Ensuring widespread awareness of these provisions will empower data principals with greater control over their personal data.

Additionally, consumer rights organisations and civil society groups should be actively involved in these initiatives to ensure broad outreach and impact. The initiatives must go beyond tier-I and tier-II cities and extend to tier III towns and rural areas too.

The DPDP Act and draft Rules also provide for penalties on Data Fiduciaries for non-compliance. The funds collected through these penalties should be utilised in accordance with the 'cy pres' doctrine, ensuring that the resources serve the next best

use in advancing data protection objectives. This could include directing funds to public interest organisations that work on consumer education, digital rights awareness, and grievance redressal support, thereby strengthening the overall data protection ecosystem in India.

c. Exploring more exemptions under the Fourth Schedule of the Act

CUTS recently conducted a study on the regulation of behavioural monitoring and targeted advertisements directed at children to understand the role of personalisation in the digital lives of children.[32] Findings from the study reveal that the internet plays a vital role in children's education, social interactions, and access to information, with personalised content enhancing their online experience. Personalisation offers significant benefits, such as free and relevant content, inclusivity for diverse linguistic and socioeconomic backgrounds, and accessibility tools for children with disabilities. It also fosters safe online spaces, shields children from harmful content, and empowers young creators.

A depersonalised internet could lead to irrelevant content exposure, increased security risks, and a shift to subscription-based models, disproportionately impacting financially disadvantaged children. Policymakers must adopt a balanced approach that maximises personalisation benefits while implementing strong safeguards to mitigate risks.

However, we recognise that without adequate safeguards, personalisation can pose significant risks, including privacy violations, manipulative advertising, and the reinforcement of biases. Additional concerns include the targeting of age-restricted products at children, excessive screen time, and the potential for unauthorised transactions.

Based on our findings (included in Annexure I), we recommend incorporating additional exemptions for service providers that meet specific safeguards, ensuring both child protection and access to beneficial digital experiences. These exemptions could be considered under the Part B of Fourth Schedule, and subject to the provisions of Clause 9(5) of the DPDP Act. The regulator may consider the following factors when granting exemptions:

- Age-Differentiated Approach – The developmental needs of young children (8 years and below), tweens (9-12 years), and teenagers (13-17 years) vary significantly.

[32]CUTS International. (2025). Regulation Of Behavioural Monitoring and Targeted Advertisements Directed at Children: Ensuring Personalisation Benefits Children. https://cuts-ccier.org/pdf/regulation-of-behavioural-monitoring-and-targeted-advertisements-directed-at-children-ensuring-personalisation-benefits-children.pdf

Exemptions should reflect these differences, ensuring that age-appropriate services, including personalised educational and recreational content, are not unduly restricted.

This has also been recognised globally, with different jurisdictions limiting the age of children to ages like 13 or 16 years olds.

- Transparency and Control – Service providers who offer clear, age-appropriate privacy information, ensuring children understand how their data is used. Privacy settings should be easy to navigate, and children should have accessible tools to exercise their data rights. Platforms that fulfil these transparency requirements may be considered for exemptions.
- Risk-Based and Proportionate Regulation – Exemptions may be granted where monitoring provides tangible benefits, such as safety, digital well-being, and educational personalisation. Service providers implementing robust safeguards against misuse—such as data minimisation, parental controls, and clear opt-out mechanisms—may be considered for exemptions.
- The Regulator can also collaborate with the industry, experts, and civil society to develop parental oversight tools that fit the priorities of the government while preserving the services provided by the platform. However, the proposed parental controls must align with data protection Rules, ensuring they follow the principles of proportionality, transparency, and security.
- Industry Best Practices and Accountability – Service providers that adhere to high privacy and security standards, avoid manipulative design (dark patterns), and implement strong accountability mechanisms may be considered for exemptions. These conditions ensure that exemptions do not compromise child safety but rather create a balanced approach to digital participation.

We have also suggested changes for the Fourth schedule below.

CUTS' Rule-by-Rule Suggestions and Rationale

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
3. (a)	be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary;	be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary; **(i) if any other information is made available by the data fiduciary to the data principal, such information must also be in clear, plain and understandable language.**	The disclosure principles laid out for the notice should be applicable to all communication from data fiduciary to data principal. A basic minimum standard needs to be set so that the data principal is able to take informed and active decisions.
3. (b)	give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum,— (i) an itemised description of such personal data; and (ii) the specified purpose of, and an	give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum,— (i) an itemised description of such personal data; and (ii) the specified purpose of, and an itemised description of the goods or	The requirement to provide a notice independently of any other information is a positive and commendable step. It sets standards for consent notices issued by Data Fiduciaries, but the specific methods for delivering these notices are left to their discretion. This raises concerns that Data Fiduciaries may not adequately inform Data Principals about the data they are consenting to share. Clear and informed consent is essential for any effective data protection framework. Further,

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	itemised description of the goods or services to be provided or uses to be enabled by, such processing; and	services to be provided or uses to be enabled by, **the specific purpose served, or goods or services provided or use enabled, corresponding to each data item, should be disclosed, to the extent possible; and** **(iii) specify that the collection and processing of personal data shall be strictly limited to the specified purpose and be limited to such personal data as is necessary for such specified purpose; and** **(iv) the Most Important Terms and Conditions (MITC) should be prominently displayed.**	the provision assumes that Data principals are both aware and capable of reading and making informed decisions about data collection and processing. CUTS' user perception study highlights that most individuals do not read privacy policies, primarily due to their excessive length.[33] To address this, we recommend that all notices be clear, and easily understandable to an average Data principal. Data Fiduciaries should disclose the specific purpose served, the good or service provided, or the use enabled by each data item collected. This transparency allows Data Principals to clearly understand the linkage between their personal data and its intended use, facilitating informed, data-item-specific consent. Additionally, it helps prevent the practice of "take-it-or-leave-it"

[33]Data Privacy and Consumer Welfare in India: Consumer Perception Analysis, available at: https://cuts-ccier.org/cdpp/

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			services, ensuring that individuals are not coerced into consenting to excessive data collection. To this end, service providers should offer basic services with only the necessary information from Data principals, while collecting additional data only for optional features. Currently, consent mechanisms function in an all-or-nothing manner, forcing Data principals to either share all requested data or be denied access to the service entirely. This choicelessness has also been observed in one of the CUTS studies titled, "My data or yours?" Unravelling Multi-Party Privacy (MPP) among Consumers of Digital Credit in India.[34] Furthermore, the current draft Rules do not explicitly require Data Fiduciaries to limit personal data collection to specified purposes, as outlined in the Act. Section 6(1) of the Act states, "The

[34]"My data or yours?" Unravelling Multi-Party Privacy (MPP) among Consumers of Digital Credit in India, available at: https://cuts-ccier.org/pdf/my-data-or-yours-unravelling-multi-party-privacy-among-consumers-of-digital-credit-in-india.pdf

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose." In contrast, the Rule 3 merely mandates an itemised format for presenting data processing details, rather than enforcing clear limitations on collection. This contrasts with global best practices, such as the GDPR, which includes a structured test to determine whether consent was freely given. We recommend amending the Rule to include the provision for limiting the use of consent obtained.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
3 (c)	**New clause**	**(c) The notice may be presented in various forms, including but not limited to privacy labels, modelled on the lines of nutrition labels or energy labels, which are a multilingual/ info-graphic communication tool to provide clear, transparent and necessary privacy information to Data Principals.**	CUTS advocates for the adoption of privacy labels, akin to nutrition and energy labels,[35] by data fiduciaries. The effectiveness of these labels can be evaluated through regulatory sandboxes, which have been recognised as a controlled mechanism for fostering innovation while enabling evidence-based regulation. Further, the regulator must prescribe that Most Important Terms and Conditions (MITC) should be prominently displayed. This has been required in the RBI's digital lending guidelines.[36] In the electricity sector, energy efficiency labels, such as the "Star Labels" in India, help consumers identify energy-efficient appliances.[37] While the food and nutrition labels are increasingly being recognised to build consumer awareness on their dietary habits.[38]

[35]Brochure-Information Labels for Consumers, available at: https://cuts-ccier.org/pdf/Brochure-Information_Labels_for_Consumers.pdf and Enabling developing countries to seize eco-label opportunities, available at: https://cuts-citee.org/enabling-developing-countries-to-seize-eco-label-opportunities/
[36]Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps, 18 November 2021, available at: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189
[37]Star Label | BUREAU OF ENERGY EFFICIENCY, Government of India, Ministry of Power, available at: https://beeindia.gov.in/en/star-label
[38]FSSAI's "Har Label Kuch Kahta Hai": A Step Towards Enhanced Food Safety Awareness, available at: https://www.slurrp.com/article/fssais-har-label-kuch-kahta-hai-a-step-towards-enhanced-food-safety-awareness-1730819217001

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
3 (d)	the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given;	the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given, **ensuring that the withdrawal process is as easy as to give consent and free from penalties, undue burdens;** **(ii) not face restrictions or diminished service quality that discourage her from withdrawing her consent.**	Data Principals should be able to withdraw consent without facing penalties or diminished service quality. This means that ease of providing and withdrawing consent should be the same and without imposing restrictions that discourage Data principals from opting out. However, in practice, Data Principals may have limited agency, particularly when attempting to revoke consent for processing their digital personal data. While the Act mandates that withdrawing consent should be as easy as giving it, Section 6(5) introduces vague and discretionary consequences for withdrawal.[39] This ambiguity could enable Data Fiduciaries to implement deterrent mechanisms, making it difficult for Data principals to withdraw—even when they have privacy concerns about an application or platform.

[39]Section 6(5) of the Digital Personal Data Protection Act, 2023 mentions, "The consequences of the withdrawal referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal."

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			To strengthen protections, the draft Rules could incorporate provisions from Brazil's data protection law, which places the responsibility on the data controller to prove that consent was lawfully obtained in compliance with the regulations. Further, the draft Rules do not require Data Fiduciaries to limit personal data collection to specified purposes, as outlined in the Act. Rule 3 only mandates presenting these details in an itemised format. It could have been drawn from the GDPR, which includes a test to assess whether consent for data processing was freely given.
3 (e)	**New Clauses**	**(e) clearly state that the Data Fiduciary bears the burden of proving that consent was lawfully obtained;**	The requirement for the Data Fiduciary to bear the burden of proving that consent was lawfully obtained is essential to uphold the principles of fairness, accountability, and transparency in data processing. Given the inherent power asymmetry between Data Fiduciaries and Data Principals, particularly in digital environments where consent is often obtained through standardised and

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			complex privacy policies, it is crucial to ensure that consent is not presumed but demonstrably valid.
3 (f)	**New Clause**	**(f) (i) Clearly inform the Data Principal of their right to refuse the collection, recording, or use of their personal data for specific purposes beyond what is strictly necessary for the provision of the requested service.** **(ii) Ensure that such refusal by the Data Principal does not result in denial or degradation of essential services, where the collection, recording, or use of personal data is not necessary for the core functioning of such services.**	Data processing should not continue without valid justification and must respect privacy boundaries. When personal data has fulfilled its original purpose or when that purpose no longer exists, continued processing becomes unnecessary and potentially intrusive. For example, when a Data principal calls a helpline for inquiries or to report a grievance, the call is recorded, and these recordings are now being used to train chatbots. However, clear and explicit consent is not obtained; callers are simply informed that "this call may be recorded for training purposes." As a result, Data principals have no real choice but to allow the collection of their personal data, which is then used for AI training. However, helpline and grievance redressal services should be accessible even if a Data principal refuses call recording.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			Since recording is not essential for grievance redressal, Data principals should have the right to deny the collection of their personal data while still receiving customer support. This prevents data fiduciaries from repurposing collected data for new uses without explicit consent and ensures that data processing remains tied to its original legitimate purpose. This temporal limitation aligns with the principle of data minimisation.
4 (1)	A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website	A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website; **(a) In the event of any inconsistency between the DPDP Rules and sector-**	A publicly accessible registry of approved consent managers should be established and maintained, allowing Data principals to verify legitimate providers. This registry should include details on services and compliance status and be regularly updated. This should also include a trust mark that the Consent Manager must display at all times to assure regulators of its legitimacy and prevent fraudsters from impersonating consent managers to deceive customers or data principals. The trust mark should be developed by the Data Protection

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		specific regulations, the sector regulator and the Data Protection Board shall consult and issue harmonised requirements to ensure regulatory consistency. **(b) A publicly accessible registry of approved Consent Managers shall be established and maintained, allowing Data principals to verify legitimate providers. This registry shall include details on services, compliance status, and regular updates. Approved Consent Managers must display a designated trust mark, as issued by the Board, at all times to ensure regulatory legitimacy and prevent fraud.**	Board in consultation with the industry, experts, think tanks, civil society, and other relevant stakeholders. While integration with consent managers is currently voluntary, companies should be encouraged or required to accommodate Data principal preferences for managing consent through these platforms. Regulatory overlap is another concern, as the Rules fail to clarify how consent managers should navigate sectoral regulations or resolve overlaps and gaps between compliance requirements. Thus, in case of any inconsistency between DPDP Rules and sector-specific regulations, the sector regulator and the Data Protection Board must coordinate to establish consistent requirements.
4 (4)	If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under	If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule,	A clear deadline for corrective measures ensures timely compliance and prevents prolonged risks to Data principals. Without a set timeframe, a

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	this rule, it may, after giving an opportunity of being heard, inform the Consent Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence.	it may, after giving an opportunity of being heard, inform the Consent Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence, **not exceeding 30 days unless specifically justified**; and	Consent Manager could delay necessary changes, allowing non-compliance to persist. For example, if a CM fails to obtain proper Data principal consent before sharing data, an indefinite correction period means Data principals' data could continue to be misused, undermining privacy rights. A fixed deadline ensures violations are addressed promptly, minimising harm and reinforcing accountability. Data principals must also be informed when a CM is non-compliant, especially if their data has been mishandled. Transparency is essential for trust, and individuals have the right to know if their personal information was improperly accessed, shared, or used. Without mandatory user notification, violations could be corrected, eroding trust in the consent framework. Setting a clear timeframe for corrective measures and requiring user notification in cases of non-compliance would better protect Data principal rights, strengthen

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			accountability, and enhance regulatory effectiveness.
4(5)	The Board may, if it is satisfied that it is necessary so to do in the interests of Data Principals, after giving the Consent Manager an opportunity of being heard, by order, for reasons to be recorded in writing,— (b) give such directions as it may deem fit to that Consent Manager, to protect the interests of the Data Principals	If the Board, after providing the Consent Manager an opportunity to be heard **within 15 working days of receiving the notice**, **finds that such action is necessary to protect the interests of Data Principals**, it may, by a **reasoned order recorded in writing**.	A reasoned order recorded in writing would ensure transparency, accountability, and procedural fairness in regulatory decision-making. When the Data Protection Board takes action against a Consent Manager, it must justify its decision with a clear, well-documented rationale. This prevents arbitrary enforcement and provides a basis for review or appeal, ensuring that regulatory actions are proportionate and justified. Providing the CM with an opportunity to be heard within 15 working days before a decision is made allows for due process, ensuring that the CM can present its case and clarify any compliance issues. If the Board ultimately determines that action is necessary to protect Data Principals' interests, it must document its reasoning in writing. Moreover, clause (b) empowers the Data

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			Protection Board to issue directions to a Consent Manager as necessary to protect Data Principal' interests. While intended to safeguard users, the provision grants broad discretionary powers without clearly defining when and how such directions can be issued. Without a well-defined scope, this could lead to overregulation, subjecting Consent Managers to unpredictable and excessive compliance burdens. Undefined regulatory powers create uncertainty for businesses, discourage innovation, and make compliance subjective rather than principle-based.
4, [Read with the Part B of the Schedule 1]	2. The Consent Manager shall ensure that the manner of making available the personal data or its sharing is such that the contents thereof are not readable by it. 3. The Consent Manager shall maintain on its platform a record of	**2.** The Consent Manager shall ensure that, the manner of making available the personal data or its sharing is such that the contents thereof are not readable by it. **Consent records should be stored in secure and encrypted manner** **3. The Consent Manager shall maintain**	The provision in Part B of the First Schedule imposes an inherent contradiction on Consent Managers. On one hand, they are required to ensure that the contents of the personal data they facilitate access to remain unreadable to them (Clause 2). On the other hand, they must retain consent and data-sharing records for at least seven years (Clause 4), which arguably requires

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	the following, namely:— 4. The Consent Manager— (c) shall maintain such record for at least seven years, or for such longer period as the Data Principal and Consent Manager may agree upon or as may be required by law.	**on its platform a record of the following in a format that does not require access to the contents of the personal data being shared, namely:—** **4. The Consent Manager—** **(c)** shall maintain such record for at least **three** years, or for such a longer period as the Data Principal and Consent Manager explicitly agree upon or as may be required by law. **Consent for the retention period must be taken separately from consent for other actions.**	some level of accessibility to personal information. However, this apparent conflict can be resolved by explicitly stating that the Consent Manager cannot access Personally Identifiable Information. Additionally, all records it maintains should be securely encrypted to minimise the risk of data breaches. Further, while maintaining transparency and accountability, the extended retention requirement may place a disproportionate compliance burden on smaller Consent Managers. Requiring Consent Managers to retain consent records for at least seven years imposes an excessive compliance burden without clear justification. Moreover, retaining data beyond three years increases security risks, as prolonged storage of consent records—albeit in a non-readable format—still presents potential vulnerabilities. A shorter retention period aligns with the principles of data minimisation and

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			necessity under global frameworks on privacy laws. Given the evolving nature of digital transactions, a three-year retention period is more reasonable and proportionate.
5 (1)	The State and any of its instrumentalities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or to issue to her any subsidy, benefit, service, certificate, licence or permit that is provided or issued under law or policy or using public funds.	**The State and any of its instrumentalities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or to issue to her any subsidy, benefit, service, certificate, licence or permit that is provided or issued under law or policy.**	The Rule introduces terms and conditions that do not find explicit mention in the Act, which raises concerns regarding legislative overreach. Specifically, the reference to "public funds" in Rule 5(1) is not defined within the Act, and its inclusion in the Rules without legislative sanction is problematic. Expanding the scope of personal data processing under such an undefined term risks arbitrary or excessive collection of data under loosely framed justifications. Policies that include data processing should be subject to parliamentary scrutiny to ensure democratic accountability. Allowing executive policies, which have not been laid before the Parliament, to justify personal data processing undermines transparency and parliamentary oversight,

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			bypassing the principles of legal certainty, accountability, and the rule of law.
5(3)	(c) using public funds shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to,— (i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State or the public account of India or the public account of the State; or (ii) in case of any local or other authority within the territory of India or under the control of the Government of India or of any State, the fund or funds of such authority.	**Withdraw the Clause**	This clause stretches the definition of public fund usage beyond direct government expenditures, potentially enabling the processing of personal data under an overly broad interpretation. This provision lacks adequate safeguards and could permit data processing without necessary legislative authorisation. Therefore, this sub-clause should be removed to prevent unchecked data processing.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
6	(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum,— (a) appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data; (b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor; (c) visibility on the accessing of such personal data, through appropriate	(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include,— (a) appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data; (b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor; **(c) such security safeguards shall be determined based on the associated risk, proportionality of the harm, and materiality, corresponding to the nature and sensitivity of the personal**	The current provision mandates security measures that all Data Fiduciaries must implement, regardless of their size, sensitivity or operational capacity. While robust security safeguards are essential for protecting personal data, the uniform application of these minimum requirements could disproportionately burden smaller platforms, leading to high compliance costs, the cost of which may eventually be passed onto consumers. It could also create potential barriers to entry which would hamper innovation in the services. Thus, introducing a threshold mechanism—such as a risk-based or materiality-based approach—would help ensure that security obligations are proportionate to the size, nature, and risk profile of the Data Fiduciary. This aligns with international best practices, where jurisdictions recognise that not all data security incidents have the same level of impact. For instance, loss of access to personal data by a data fiduciary should trigger obligations only if it meets a defined materiality threshold,

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence; (d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of data backups; (e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;	**data processed and the potential harm that may arise from a personal data breach** **(d) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;** **(e) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of data backups;** **(f) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of**	considering factors such as the sensitivity of data, scale of impact, and risk to data subjects. Thus, a risk-based approach should be incorporated, ensuring that security obligations are tailored to the nature and scale of the Data Fiduciary's operations while maintaining strong protection standards.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	(f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and (g) appropriate technical and organisational measures to ensure effective observance of security safeguards.	**such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;** **(g) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and** **(h) appropriate technical and organisational measures to ensure effective observance of security safeguards.**	
6 (2)	**New Clause**	**A Data Fiduciary shall conduct regular independent security assessments or audits to identify vulnerabilities, measure the effectiveness of security measures and ensure ongoing compliance with provisions of the Act,**	Regular security assessments or audits are vital for proactively identifying and mitigating vulnerabilities, thereby ensuring that Data Fiduciaries maintain ongoing compliance with the Act. By mandating the public disclosure of audit reports every six months, this provision enhances

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		and– **(i) publish such reports on a publicly accessible platform every six months;** **(ii) the report shall contain rationale and justification for security measures, along with their performance against established standards.**	transparency and accountability, enabling consumers and civil society to monitor data protection practices effectively. Such regular reporting not only fosters public trust but also incentivises continuous improvement and adherence to evolving regulatory standards.
7 (1)	On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary,— (a) a description of the breach, including its nature, extent and the timing and location of its occurrence;	On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary,— **(a) a description of the breach, including its nature, the categories of data affected, the estimated number of affected Data Principals, the extent of**	The existing provision lacks clarity on the level of detail required for breach disclosures, particularly regarding the extent and timing of the breach. By specifying that Data Fiduciaries must disclose the categories of affected data, the number of impacted Data Principals, and the volume of data exposed, this amendment ensures that affected individuals and regulators can better assess the severity of the breach. Including a timeline of the breach—from when it occurred to when it was detected—ensures transparency and enables affected Data Principals to take timely precautionary measures. This approach also aligns

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		the breach in terms of data volume and exposure, and the timing of its occurrence, specifying when the breach was detected and the period during which the data was vulnerable and location of its occurrence**;**	with global best practices in data breach notification, ensuring that disclosures are neither excessively vague nor burdensome for compliance. Further, the second intimation to the Board under Rule 7(2)(b) should also be provided to Data Principals to ensure that they remain informed of the measures taken by the Data Fiduciary to address the breach. This prevents asymmetry of information and reinforces accountability.
	(b) the consequences relevant to her, that are likely to arise from the breach;	**(b) the consequences relevant to her that are likely to arise from the breach, including any potential misuse of the compromised personal data;**	
	(c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;	**(c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate the risk and prevent recurrence;**	
	(d) the safety measures that she may take to protect her interests; and	**(d) the safety measures that she may take to protect her interests, including recommended steps to safeguard her personal data and mitigate any potential harm; and**	
	(e) business contact information of a	(e) business contact information of a person who is able to respond on behalf	

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal.	of the Data Fiduciary to queries, if any, of the Data Principal.	
7 (2)	On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board,— (a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact;	On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board,— **(a) a description of the breach, including its nature, the categories of data affected, the estimated number of affected Data Principals, the extent of the breach in terms of data volume and exposure, and the timing of its occurrence, specifying when the breach was detected and the period during which the data was vulnerable** and location of its occurrence**;**	Similar to Data Principals, the Board should also be informed about the categories of affected data, the number of impacted Data Principals, and the volume of data exposed, this amendment ensures that affected individuals and regulators can better assess the severity of the breach.
7 (3)	**New Clause**	**In the event of a personal data breach, the Data Fiduciary shall be liable to compensate affected Data Principals for any loss or harm suffered, subject to**	Rule 7, as currently drafted, does not address remediation for affected individuals. This provision introduces a structured approach to determining liability and compensation in case of a personal

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		the following conditions– **(a) where the breach is a result of the Data Fiduciary's negligence, including failure to implement reasonable security safeguards, delayed response, or inadequate risk mitigation measures, the Data Fiduciary shall bear full liability for compensating affected Data Principals for demonstrable financial, reputational, or other material harm;** **(b) where the breach occurs despite the Data Fiduciary having implemented reasonable security measures in accordance with applicable standards and due diligence requirements, liability shall be assessed on a case-by-case basis, considering whether the Data Fiduciary took prompt and appropriate remedial actions to mitigate harm;**	data breach. Differentiating between breaches caused by negligence and those occurring despite reasonable security measures ensures that Data Fiduciaries are held accountable for preventable failures while also recognizing that certain breaches may be unavoidable despite best efforts. Clause (a) ensures that Data Fiduciaries cannot escape liability when their own lapses contribute to a breach, thereby incentivizing them to adopt robust security frameworks. Clause (b) acknowledges that in cases where breaches occur despite due diligence, liability should be assessed proportionately, preventing undue burden on entities that have acted in good faith. The inclusion of insurance and risk pooling mechanisms in Clause (c) allows Data Fiduciaries to manage financial risks while ensuring that affected Data Principals receive timely compensation. Clause (d) further strengthens

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		(c) the compensation framework may include direct payments to affected Data Principals, risk pooling mechanisms, or insurance-based claims, provided that such arrangements do not absolve the Data Fiduciary of its primary obligation to compensate Data Principals in cases of proven negligence; **(d) the Board shall establish guidelines for determining the quantum of compensation based on the nature and severity of harm suffered by the affected Data Principals.**	accountability by requiring the Board to establish clear guidelines on compensation, ensuring consistency and fairness in addressing harm caused by data breaches.
8 (2)	At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that such personal data shall be erased upon completion	(2) At least **30 days and adequate reminders before** the completion of the time period for the erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that their personal data shall be erased unless the	The proposed requirements for sectors such as online jewellery could have significant consequences for businesses and consumers. The rule may increase customer acquisition costs, reduce the effectiveness of personalised services, and hinder fraud prevention efforts. Additionally,

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data.	Data Principal logs into their user account or otherwise initiates contact with the Data Fiduciary to perform the specified purpose or exercises their rights in relation to the processing of such personal data.	data loss could affect service quality and pricing, while ambiguities in determining when data retention is no longer valid may lead to inconsistent practices. To address these challenges, policymakers should establish a framework for assessing data erasure requests on a case-by-case basis, taking into account factors such as context, public interest, and legitimate business needs. The framework should consider the nature and sensitivity of the data, the purpose of its collection, the time elapsed since collection, and the potential consequences of erasure or retention. Furthermore, a mechanism should be created for regularly reviewing and updating these regulations with input from data subjects, controllers, and other stakeholders. This will ensure that the framework evolves in response to technological advancements, changing business practices, and shifting consumer expectations regarding data privacy. These principles should be

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			applied consistently across all sectors, without granting special treatment to any specific industry.
9 (1)	**New Clause**	**The business contact information published shall remain operational and accessible during reasonable business hours and the Data Fiduciary shall ensure timely responses to queries and requests raised by Data Principals regarding the processing of their personal data.** **(a) in the event that the business contact information is found to be non-operational, unresponsive, or otherwise inaccessible without valid justification, the Data Fiduciary shall be deemed to be in violation of the provisions of the Act and may be subject to penalties as prescribed by the Board.**	This amendment strengthens accountability by ensuring that Data Fiduciaries maintain an active and functional point of contact for Data Principals seeking information or redressal regarding the processing of their personal data. This ensures that Data Principals do not face unnecessary hurdles in exercising their rights and reinforces transparency and trust in data processing practices.
10 (1)	Verifiable consent for processing of	Verifiable consent for processing of	CUTS welcomes the ministry's detailed

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	personal data of child or of person with disability who has lawful guardian.—(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to— (a) reliable details of identity and age available with the Data Fiduciary; or (b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued	personal data of child or of person with disability who has lawful guardian.—(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for **checking that the individual using its services is a child, and the individual providing consent is the child's parent,** by reference to– (a) **reliable details of age and relation of parent and child available with the Data Fiduciary**; or (b) **voluntarily provided details of age and relation of parent and child or a virtual token mapped to the same**, which is issued by an entity entrusted by law with the maintenance of such details	explanation on the approaches to obtain verifiable parental consent (VPC). However, one of the primary challenges that may arise in the proposed framework will be in ensuring a seamless and convenient verification and consent process for both parents and children, without creating unnecessary barriers to digital access. Firstly, a key challenge is how platforms will reliably determine users' ages. Even if a user declares themselves an adult, platforms may need to monitor user behaviour to verify whether they are actually an adult or a child. This assumption is also reinforced by the requirement for platforms to exercise due diligence and ensure that information likely to harm children is not accessible to them. (Part B of Fourth Schedule of the draft Rules). This could also result in the collection of data from adults that isn't essential. Additionally, it may also

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.	or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider. **(c) any other reliable method, in compliance with industry standards, based on the specific use case, risk level, and implementation capabilities, and taking into consideration available technology.** **(d) Platforms may establish secure, interoperable protocols for sharing verified parental consent, ensuring compliance with the Act.**	become complicated, especially when depending on the methods proposed by the draft Rules. Insights from CUTS research on economic analysis of these methods (included in Annexure II) shows that methods like self-declaration tools are not the most reliable when it comes to accuracy due to potential for manipulation.[40] On the other hand, Digital Lockers risk revealing sensitive details of the family. This can make it difficult for organisations to obtain parental consent, especially when age is falsely declared. To this end, CUTS recommends that this provision be appropriately amended to include verifying only the age of the user, in the draft Rules to avoid unnecessary confusion. The requirement of identity can be done away with, as it may not be the best privacy preserving approach.

[40]Iqubbal, A. & Jugiani, K. (2025). Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries. CUTS International. https://cuts-ccier.org/pdf/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-on-consumers-and-data-fiduciaries.pdf

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			Secondly, the proposed methods–including reliance on government-authorised digital tokens or existing user data–may not always be the most practical solution. Findings from a CUTS study on methods of VPC mechanisms also suggests that not one method may be fit for every data fiduciary. Many parents may not store identity and age documents in DigiLocker or other digital services, which could hinder their ability to verify their status as legal guardians. This could disproportionately affect families with limited digital access or privacy concerns about centralised data storage. Global practices too allow different verification services depending on risk and use cases, including third-party verification services to streamline this process, ensuring security while maintaining ease of use. As VPC is an evolving area globally, the regulator should encourage innovation and experimentation in verification

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			methods. Further, the absence of interoperability in verification mechanisms, allowing platforms to share verified parental consent, means each service would have to conduct independent verification, creating an administrative and technical burden for both consumers and service providers, increasing costs. These costs arise from operational expenses such as software subscriptions, staff training, data collection (government IDs, financial details), storage, and ongoing verification. This may lead to disproportionate cost burden on smaller data fiduciaries, which will impact competition in providing services to children, innovation in child friendly services, and such costs may also be passed on to consumers. In addition to their costs, these methods have issues with scalability, convenience, and privacy. Both DigiLocker and

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			Government IDs have the potential to reveal other personal information about the user; while obtaining parental consent from users without official identification is a concern. Further, the Digilocker's penetration is limited and may not be able to determine relationships when a guardian, rather than a parent, is providing consent. To address, the Rules should introduce an interoperable, verifiable parental consent framework. Similar to interoperability in telecom and payments, platforms should establish secure protocols for sharing verified consent. This would reduce data collection, ease compliance, and enhance efficiency, particularly for smaller platforms. Standardised protocols would enable secure communication, allowing parents to verify consent once, minimising barriers in regions with limited ID services, digital infrastructure, or literacy.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			We also recommend allowing data fiduciaries to implement verification methods that align with their specific context, considering three primary factors: the nature of the use case, the level of associated risks, and the scope of implementation costs, both direct and indirect. We also recommend framing a mechanism to review the implementation of VPC after a specified period to assess its effectiveness in protecting children's data protection. This review would help identify concerns, challenges, and risks while exploring mitigation strategies to enhance its efficiency. It would also provide an opportunity to evaluate the overall utility of VPC and consider alternative approaches for better online child protection.
11 (3)	**New Clause**	**The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to the processing of**	The proposed exemption under Rule 11(3) ensures a balanced approach between protecting children's data privacy and enabling responsible

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		personal data of a child by Data Fiduciaries that: **(a) Implement age-appropriate design frameworks, ensuring that content and services align with the developmental needs and privacy expectations of children.** **(b) Adopt privacy by design principles, incorporating strong encryption, secure storage, and minimal data collection.** **(c) Follow data minimisation practices, ensuring that only essential data is collected and retained for limited periods.** **(d) Ensure transparency and accountability by filing continuous compliance reports in the public domain, detailing risk assessments, data processing purposes, and mitigation measures.**	innovation. Strict prohibitions under section 9(1) and (3) may unintentionally hinder personalised services that enhance accessibility, inclusivity, and digital participation, such as adaptive learning tools, child-friendly content recommendations, and age-appropriate safety measures. By allowing exemptions for platforms that adopt age-appropriate design, privacy by design, and data minimisation principles, this provision encourages responsible data processing while safeguarding children's rights. Further, imposing transparency and accountability measures, including continuous compliance reporting in the public domain, ensures that platforms remain answerable to regulators, parents, and civil society. This approach prevents exploitative practices while still allowing legitimate and beneficial behavioural monitoring and targeted content delivery. It also reduces compliance burdens on smaller platforms and

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		(e) Provide parental oversight and user controls, enabling informed consent management and the ability to opt out of behavioural monitoring and targeted advertising. **(f) Deploy safeguards to prevent engagement with fraudulent or harmful entities and implement time-based or content-related warnings to mitigate risks like excessive screen time, exposure to harmful content, or data misuse.**	startups by encouraging interoperable and verifiable consent mechanisms, similar to frameworks in telecom and payments. Additionally, this exemption empowers parents and children by ensuring user control over data processing and implementing parental oversight and opt-out mechanisms. The provision further mitigates risks such as fraudulent engagements, exposure to harmful content, and excessive screen time through time-based warnings, risk assessments, and fraud detection safeguards. Overall, this provision supports a nuanced data governance framework, enabling child safety, digital empowerment, and industry responsibility while avoiding blanket prohibitions that could limit access to essential digital services.
12 (1)	A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is	A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is	A well-defined Data Protection Impact Assessment (DPIA) and audit framework is crucial for consistency, accountability, and effective risk

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	notified as such or is included in the class of Data Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the Rules made thereunder.	included in the class of Data Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the Rules made thereunder; **(a) A Data Protection Impact Assessment (DPIA) shall be conducted when a processing activity, particularly one involving new technologies, is likely to pose a high risk to the rights and freedoms of individuals;** **(b) The assessment shall take into account the nature, scope, context, technical infrastructure, security measures, and purpose of the processing; and** **(c) The DPIA shall be documented in a**	mitigation. However, the lack of clear standards leads to inconsistencies in how companies assess and manage risks. Without uniform guidelines, some conduct superficial assessments while others apply rigorous methodologies, creating an uneven regulatory landscape that weakens compliance and enforcement. DPIAs should be mandatory for high-risk processing, particularly when new technologies or large-scale data collection are involved. This includes sensitive personal data such as financial, health, or biometric information, as well as profiling, automated decision-making, and surveillance-based data collection. DPIAs should evaluate the nature, scope, context, and purpose of data processing while considering technical infrastructure, security measures, and potential impacts on privacy, discrimination, and consent. To ensure consistency, DPIAs should follow a format prescribed by the Data Protection Board, allowing regulators to review high-risk cases and,

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		standardised format as prescribed by the Board and made available to the Board and publicly.	if necessary, demand risk mitigation before approval. Evaluations should assess not only technical compliance but also the real-world effectiveness of data protection measures, including the implementation of privacy policies, data security, and the impact on individual privacy rights.
12 (2)	A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit.	A Significant Data Fiduciary shall ensure that the person conducting the Data Protection Impact Assessment and audit submits a report to the Board **while simultaneously uploading a full report in the public domain**, containing significant observations from the assessment and audit.	An effective DPIA and audit framework is essential to prevent oversight from becoming a mere formality. Without clear guidelines on scope, methodology, and implementation, disclosures risks becoming a checkbox exercise rather than a meaningful accountability measure. The current provisions lack detail, limiting their effectiveness in identifying and addressing risks. To ensure transparency and public trust, the assessment report should be submitted to the DPBI and made publicly available. This would enhance accountability by allowing independent experts, civil society, and stakeholders to assess whether

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			data fiduciaries are genuinely mitigating risks. The provision should also require the full DPIA and audit report, along with a summary of significant observations. Allowing companies to disclose only selected findings creates the risk of withholding critical information on privacy risks, algorithmic biases, or compliance gaps. To prevent this, the framework must mandate full disclosure while permitting redaction of truly sensitive proprietary details without compromising public interest.
12 (3)	A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals.	A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals. (a) **The assessment of risks shall be**	The rule lacks clear standards for determining risk levels, making implementation challenging. The Rules also do not specify what due diligence measures an SDF must take to comply with this requirement. To strengthen it, specific risk assessment criteria should be established, considering data volume and sensitivity, training methods, use cases, deployment contexts, and broader consumer impacts. Risk evaluations should be proportionate to data scale, algorithm

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		proportional to data collection, training, and the intended use case, considering evolving global frameworks on AI-related risks. It shall also take into account sector-specific regulatory frameworks being developed.	complexity, sector-specific harm potential, and global AI governance, ensuring higher scrutiny for higher-risk systems. Transparent assessments are crucial. Risk reports should be publicly available in standardised formats for meaningful comparisons, ensuring accountability and allowing Data Principals and regulators to evaluate compliance. The law should incorporate sector-specific considerations, flexibility to align with global AI safety standards, principles for acceptable risk thresholds, and guidance on risk mitigation. Recognising that algorithmic risks vary across industries like healthcare, finance, and transportation, sector-specific frameworks would enhance enforceability while allowing adaptation to evolving global best practices.
12 (4)	A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the	A Significant Data Fiduciary shall undertake measures to ensure that personal data, as specified by the Central Government based on the	The Draft Rules empower the Central Government to determine which types of personal data must be stored exclusively in India, effectively prohibiting their transfer abroad. This is a

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	recommendations of a committee constituted by it is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.	recommendations of a designated committee, is processed with the restriction that such personal data and its associated traffic data shall not be transferred outside India. **(a) The restrictions on the transfer of specified personal data and traffic data outside the territory of India shall be done through a notification and public consultation. The notification shall include a clear rationale, along with a transparent assessment of the costs and benefits of the proposed restrictions as suggested in rule 14 (2).**	departure from the DPDP Act, which does not mandate explicit data localisation. This seems to be an excessive delegation, as the DPDP Act does not mandate the formation of such committees. Additionally, the law or rules do not define the committee's membership, mandate, or decision-making authority, raising concerns about its legitimacy and transparency. The rule seems to extend data localisation requirements to all industry sectors, whereas previously, such restrictions applied only to payment system providers under RBI regulations that too in specific scenarios. Further, different mandates on data storage and transfer, such as those by the RBI, make it impossible to segregate data by mandate, creating operational challenges for businesses, especially data processors and cloud service providers, who would need to reprogram their systems. A CUTS study found that the economic drawbacks of data localisation may outweigh its

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			perceived benefits.[41] Another CUTS study found that implementing data localisation without proper preparation and accountability measures could restrict access to data-driven services, hinder innovation, increase privacy violations and data breach risks, and facilitate censorship.[42] Moreover, it is unclear why a broad restriction on traffic data is necessary, and the provision lacks clear guidance on the rationale and principles for deciding cross-border data flows. Without a well-defined framework, such decisions risk being arbitrary and inconsistent. Therefore, a re-examination is needed to establish clear criteria and ensure alignment with the DPDP Act.
13 (1)	For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager,	For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, shall publish on its	Ensuring that information is available on both the website and the app is essential for universal access. Some Data principals may rely exclusively on websites, while others primarily use mobile

[41]Data Localisation India's Double-Edged Sword, available at: https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf
[42]Consumer Impact Assessment of Data Localisation, available at: https://cuts-ccier.org/pdf/Findings_of_Consumer_Impact_Assessment_of_Data_Localisation.pdf

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	shall publish on its website or app, or both, as the case may be, — (a) the details of the means using which a Data Principal may make a request for the exercise of such rights;	**website and app**, — (a) The details of the means by which a Data Principal may make a request to exercise such rights shall be **easily accessible** and presented in a **clear and understandable format** for all Data principals, including those with disabilities or limited digital literacy.	apps. Requiring availability on both platforms ensures that all Data Principals can exercise their rights regardless of their preferred device. This approach also helps bridge the digital divide, as different demographics have varying levels of familiarity with websites and apps. Additionally, Clause 13(1)(a) does not specify that the information must be easily accessible and presented in a clear and understandable format for all Data principals, including those with disabilities or limited digital literacy. It should also mandate that the information be available in multiple languages to accommodate diverse linguistic demographics, which is crucial in a multilingual country like India.
13 (2)	To exercise the rights of the Data Principal under the Act to access information about personal data and its erasure, she may make a request	To exercise the rights of the Data Principal under the Act to access information about personal data and its erasure, she may make a request to the Data Fiduciary to	When user data is incorporated into an AI model's training, it becomes embedded in the model's structure, influencing its decision-making and outputs even after erasure. This integration makes

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	to the Data Fiduciary to whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars published by such Data Fiduciary for the exercise of such rights.	whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars published by such Data Fiduciary for the exercise of such rights; **(a) Data Fiduciary should provide written reasons for refusing a request for erasure or providing requested information, specifying the grounds for refusal and the mechanism for appeal to the DPBI; and** **(b) The Data Fiduciary shall notify any third party in possession of the personal data about the erasure request. The notification shall include a description of the request and the grounds for erasure.**	precise data erasure difficult, as extracting specific data points can disrupt the model's functionality. Additionally, removing data from active models requires assessing both technical feasibility and the potential impact on performance. While an individual can request erasure of explicitly identifiable information, their characteristics and patterns may still influence broader groups to which the individual belongs. For example, if an AI system associates a neighbourhood with specific health risks, deleting one person's data does not exclude them from that group-level analysis. AI relies on patterns across groups rather than individual cases, making complete erasure complex.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
13 (3)	Every Data Fiduciary and Consent Manager shall publish on its website or app, or both, as the case may be, the period under its grievance redressal system for responding to the grievances of Data Principles and shall, for ensuring the effectiveness of the system in responding within such period, implement appropriate technical and organisational measures.	Every Data Fiduciary and Consent Manager shall publish on its website or app, or both, **the time frame of 7 days for addressing grievances from Data Principals**. To ensure the effectiveness of the grievance redressal system, they shall **implement appropriate technical and organisational measures to respond within this specified period**; **Any person who has suffered harm as a result of a contravention of this law shall have the right to receive compensation and/ or repartition from the Data Fiduciary for the harm suffered; and** **Data Fiduciaries shall implement alternative dispute resolution mechanisms, such as online dispute resolution and consumer assistance**	The draft Rules do not specify the maximum time for Data Fiduciaries and Consent Managers to address grievances. Without a clear timeframe for grievance resolution, the rights of data principals under the DPDP Act may be weakened. In line with the Consumer Protection Act 2019, a timeline of no more than 60 days could be set for resolving complaints at the Data Protection Board. The draft Bill may also introduce mediation mechanisms, similar to CUTS Grahak Sahayata Kendra. To make grievance redressal accessible, effective, and Data principal-friendly, the draft rule should require service providers to offer alternative mechanisms, including online dispute resolution and consumer assistance centres. The draft Rules may also consider defining types of grievances, such as privacy violations, unauthorised data processing, harms, and data breaches, similar to the IT Rules. Initiatives like CUTS' Grahak Sahayata Kendra should be adopted, as they can mediate

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		centres, to expedite grievance redressal; **A Consumer Protection Fund shall be established with contributions from Data Fiduciaries to compensate Data Principals affected by violations of their data rights. If identifying specific victims is impractical or impossible, the Fund may be used to support grassroot organisations engaged in data protection awareness, advocacy, and redressal efforts. The governance, administration, and utilisation of the Fund shall be prescribed by the Board to ensure transparency and accountability.**	between consumers and Data Fiduciaries. Data Principals should be able to file complaints or seek clarifications via toll-free numbers, online portals, emails, or in person. To build consumer capacity, local information providers, such as community radio and multilingual newspapers, should be involved. The draft Rules should include the right to compensation for consumers harmed by Data Fiduciaries violating the law, and provide clarity on the definition of harm. Data Principals should have the right to involve consumer organisations for assistance in claiming compensation. Furthermore, Data Principals should be able to file complaints for contravention of the Act, regardless of whether harm occurred. The procedure for seeking compensation must be accessible and understandable. A CUTS study showed many consumers unaware of grievance redress options after a data breach or privacy violation, highlighting the need for consumer assistance

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			centres to build capacity and facilitate grievance resolution.[43]
14 (1)	Transfer to any country or territory outside India of personal data processed by a Data Fiduciary— (a) within the territory of India; or (b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India, is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any	Transfer to any country or territory outside India of personal data processed by a Data Fiduciary— (a) within the territory of India; or (b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India, is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State; and	The Digital Personal Data Protection Act allowed cross-border data transfers, except to countries specifically restricted by the government. However, the current Draft Rules do not specify which countries will be blacklisted. Instead, they require Data Fiduciaries to comply with "general or special order" issued by the central government when transferring personal data abroad, suggesting a shift towards data localisation. While section 43 of the DPDP Act empowers the central government to issue orders, that is only in certain circumstances, and may not qualify for specifying requirements for data transfer. Further, the law or rules do not define the committee's membership, mandate, or decision-making authority, raising concerns about its legitimacy and transparency.

[43]Consumer Support Centre (Grahak Sahayta Kendra), available at: https://cuts-cart.org/consumer-support-centre-grahak-sahayta-kendra/

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	agency of such a State.	(c) **The restrictions on the transfer of specified personal data outside the territory of India shall be done through a notification and public consultation. The notification shall include a clear rationale, along with a transparent assessment of the costs and benefits of the proposed restrictions as suggested in rule 14 (2).**	Thus, this needs to be relooked and ensure that the draft rule is aligned with the DPDP Act.
14 (2)	**New Clause**	**Before issuing any notification under subsection 14(1), the Central Government, in consultation with the Board, shall undertake the following steps:** **(a) A cost-benefit analysis shall be conducted using transparent standards, considering the level of data protection in the destination country, the ability of consumers to exercise their rights, efficiency gains for Data**	The CUTS Consumer Impact Assessment study highlighted the unintended consequences of data localisation (DL), including reduced uptake of certain data-driven services, limited service availability, and stifled innovation. The study also pointed out that DL could increase the risks of privacy violations, cyber-attacks, and data breaches. CUTS' study on the impact of Data Localisation on Digital Trade found it would negatively affect trade and innovation while raising compliance costs. Before defining

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		Fiduciaries, law enforcement concerns, and strategic and foreign policy considerations; **(b) conduct a public consultation inviting all relevant stakeholders to provide input; and** **(c) record reasons in writing for excluding any countries or territories outside India.**	territories for personal data transfer restrictions, CUTS recommends that the Central Government, in consultation with the Board, conduct a Cost-Benefit Analysis (CBA).[44] This will ensure that the costs of restrictions do not outweigh the potential benefits for consumers and other stakeholders, such as service providers. The findings of this CBA should be made publicly available to maintain transparency and trust. This should include transparent standards, including the level of data protection in other countries, consumer rights, efficiency gains for Data Fiduciaries, law enforcement concerns, and strategic or foreign policy considerations for transferring data outside India.
15	The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried	The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in	The provision does not define research or statistical processing. Without clear definitions, entities could broadly interpret these terms to claim exemption from data protection

[44]Regulatory Impact Assessment (RIA), available at: https://cuts-ccier.org/regulatory-impact-assessment/

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	on in accordance with the standards specified in Second Schedule.	Second Schedule **and appropriate safeguards.** **(a) Research entities shall publish annual transparency reports detailing the nature, scope, and purpose of personal data processing conducted under this exemption.**	requirements. It is also unclear whether this exemption applies to AI model development. Given the global discourse on regulating artificial intelligence and automated decision-making, these provisions must be examined in the context of commercial AI applications relying on personal data. The Act exempts publicly available personal data if made public by the data principal, such as an artist displaying contact details on a personal website, or disclosed under a legal mandate, such as government-published lists of licensed medical practitioners. It also permits processing personal data for research or statistical purposes with minimal restrictions. The exemption is broad, with one key limitation: if processing leads to a decision directly affecting the data principal, the Act's provisions still apply. In most jurisdictions, data protection laws do not explicitly exempt the processing of personal data for research purposes. Instead, they treat research as a secondary use, meaning it can rely on the same lawful basis as the

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			original data collection or, in some cases, allow non-consensual processing under specific conditions. For example, the EU's GDPR permits the secondary use of personal data for archiving, statistical, or scientific research purposes, provided that appropriate safeguards are in place to protect the rights of data subjects.[45] While a well-defined exemption could facilitate the creation of high-quality datasets, it is essential to establish clear technical and ethical standards to prevent privacy harms.
16 (1)	The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of	The Central Government shall constitute a Search-cum-Selection Committee to ensure the independence of the Board. This Committee shall include the **independent expert**, the **Chief Justice of India or their nominee**, and a	To protect the independence of the DPBI and ensure transparency in the appointment process, the draft Rules should establish clear principles including merit for selecting Board chairperson and members, their terms and conditions, and the process for removing the Chairperson and

[45]General Data Protection Regulation GDPR, available at: https://gdpr-info.eu/

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	Legal Affairs and the Ministry of Electronics and Information Technology and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as Chairperson.	representative from **civil society**. The Committee will recommend individuals for appointment as Chairperson and members of the Board. The committee shall provide reasons for the decision**;** **(a) The final selection process should be livestreamed and conducted before a parliamentary committee when making a decision under Rule 16(3).**	members. These principles should be developed in consultation with judicial representatives, subject-matter experts, and civil society members. The Joint Parliamentary Committee in 2021 recommended including the Attorney General and an independent expert in the selection committee to safeguard the Board's independence. The Justice Srikrishna Committee also suggested including the Chief Justice of India or their nominee to ensure impartiality in the board. An example from the Competition Act, 2002, is its approach to appointing the Chairperson and members of the Commission through a single selection committee. This committee includes the Chief Justice or their nominee, technical experts, and members of civil society from relevant domains. Given that the DPBI is an adjudicating body, its independence is crucial. Since, its adjudicatory role is also relatively limited, necessitating clear safeguards to prevent undue influence is necessary. This independence is at risk

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			due to excessive executive control. As the State is the largest data processor, it is essential that the regulatory body remains fair, transparent, and free from governmental influence. In this regard, similar to the Monetary Policy Committee under India's Financial Code, the selection criteria, the list of shortlisted candidates, and the rationale behind the final recommendation should be made publicly available to ensure accountability. The final recommendation of the committee should be subject to review or confirmation by a parliamentary committee to enhance accountability and prevent undue executive control over appointments.
16 (3)	The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee,	The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the	The Central Government should appoint the Chairperson or other Members, as the case may be, based on the suitability of individuals recommended by the Search-cum-Selection

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	appoint the Chairperson or other Member, as the case may be.	Chairperson or other Member, as the case may be. **(a) The selection process shall be guided by clear merit-based principles to ensure transparency and independence.** **(b) The Search-cum-Selection Committee shall include judicial representatives, subject-matter experts, and civil society members.**	Committee. The selection process should be guided by clear merit-based principles, ensuring transparency and independence. The Search-cum-Selection Committee should include judicial representatives, subject-matter experts, and civil society members, in line with recommendations from the Joint Parliamentary Committee (2021) and the Justice Srikrishna Committee, to safeguard the Board's autonomy. Given the adjudicatory role of the DPBI, safeguards shall be in place to prevent undue executive influence and maintain the Board's fairness, impartiality, and accountability.
16 (4)	No act or proceeding of the Search-cum-Selection Committee specified in sub-Rules (1) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution.	Withdraw the clause.	The provision stating that no act or proceeding of the committee can be questioned due to a vacancy, absence, or defect in its constitution raises concerns about accountability and legitimacy. While such a clause ensures procedural continuity, its broad framing creates governance risks. The absence of a quorum requirement means key decisions could be made by an

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			incomplete committee. If a crucial member, such as an expert with specialised knowledge, is absent, decisions may lack necessary expertise, leading to unsuitable outcomes. The clause also allows decisions to stand despite procedural irregularities or defects in the committee's formation. This includes cases where members are improperly appointed, do not meet eligibility criteria, or if political influence skews the process. By preventing legal challenges on these grounds, the provision shields flawed appointments from scrutiny, reducing accountability. If the committee operates with only government officials due to expert vacancies, it risks concentrating decision-making power within the executive, sidelining independent voices and weakening fairness. This undermines the selection process and erodes public trust in the Board's independence. Thus, provision should be reconsidered.
18 (8)	The Chairperson or any Member of	The Chairperson or any Member of the	Introducing procedural safeguards ensures that

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
	the Board, or any individual authorised by it by a general or special order in writing, may, under her signature, authenticate its order, direction or instrument.	Board, or any individual authorised by it through a general or special order in writing, may, under her signature, authenticate its order, direction, or instrument. **(i) Any such general or special order shall be issued in accordance with established guiding principles that ensure necessity, proportionality, and transparency.** **(ii) The Board shall maintain a publicly accessible record of such orders, including their rationale, scope, and intended application, subject to reasonable confidentiality requirements.**	the issuance of general or special orders by the Chairperson or Members of the Board is consistent, justified, and not arbitrary. Adopting principles of necessity and proportionality prevents overreach, while transparency in maintaining a public record fosters accountability. These measures uphold regulatory predictability, safeguard against misuse of authority, and enhance public trust in the Board's decision-making processes.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
18	**New Clauses**	**(10) The Board shall publish the agenda of its meetings at least 24 hours prior to the scheduled time of the meeting;** **(a) Such minutes shall be published on the official website of the Board and any other appropriate public platform, in a manner that is easily accessible to the general public.** **(11) The Board shall make minutes of its meetings publicly available within 24 hours of the meeting;** **(a) Such minutes shall be published on the official website of the Board and any other appropriate public platform, in a manner that is easily accessible to the general public.** **(12) The Board shall publish a quarterly report on its website, providing anonymised and aggregated data on;** **a) The number and nature of matters heard, including complaints received**	Ensuring transparency and accountability in the Board's functioning is essential for maintaining public trust and procedural fairness. To this end, the Board should publish minutes of its meetings in a clear, concise, and easily comprehensible format. Making these minutes accessible in summarised versions and regional languages will further enhance inclusivity, enabling broader public awareness and participation. Advance publication of meeting agendas promotes stakeholder engagement by ensuring that relevant parties are informed and prepared. Quarterly and annual reports provide critical oversight, reinforcing the consistency, fairness, and proportionality of the Board's decisions and enforcement actions. Transparent reporting on data breaches and penalties serves as both a deterrent and a means to highlight the Board's regulatory priorities. Additionally, maintaining a publicly accessible repository of anonymized

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		and resolved. **b) The number of decisions issued, categorised by type of relief granted.** **c) The number of decisions overturned or upheld in appellate forums.** **d) Other matters of public interest transacted during Board meetings.** **(13) The Board shall also publish an Annual Transparency and Compliance Report, detailing;** **a) A summary of its key activities, including significant decisions made.** **b) Data breach reports received and penalties imposed, along with the rationale thereof.** **c) A business plan for the upcoming year, outlining priorities and expected areas of focus.** **(14) The Board shall maintain a publicly accessible repository of past decisions, anonymised where necessary**	decisions enhances legal predictability, mitigates arbitrary decision-making, and fosters accountability. Collectively, these measures strike a balance between institutional transparency and operational efficiency, ensuring the Board functions as a fair and responsive regulatory body.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		(15) The inquiry by the Board shall be completed within six months from the date of receipt of the intimation, complaint, reference, or direction under Section 27 of the Act, unless extended for reasons recorded in writing, for a further period not exceeding three months at a time.	
20 (3)	**New Clause**	**The Board shall establish a transparent and merit-based process for the appointment of its officers and employees;** **(i) the selection criteria, evaluation process, and final appointments shall be made publicly available on the official website of the Board and any other appropriate public platform**	The appointment of officers and employees by the Board is critical to ensuring its effective functioning under the Act. However, the current provision lacks explicit safeguards to promote transparency, fairness, and accountability in the recruitment process. To uphold the principles of good governance, it is essential that the Board establishes a well-defined, transparent mechanism for hiring personnel. This should include publicly accessible criteria for selection, competitive recruitment procedures, and mechanisms to

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			prevent conflicts of interest. Furthermore, a structured and transparent process for determining the terms and conditions of service is necessary to maintain institutional integrity. The Board should formulate clear policies regarding remuneration, tenure, and performance evaluation, aligning them with best practices and standards applicable to regulatory bodies. Additionally, any deviations from standard procedures should be justified and documented, ensuring accountability. Incorporating these safeguards within the rule would strengthen the Board's institutional framework, fostering efficiency and public confidence in its operations. All Such mechanisms and conditions shall be made publicly available on the official website of the Board and any other appropriate public platform. This would enhance public trust in the Board's independence and credibility while ensuring that only qualified individuals are appointed to carry

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			out its functions.
21 (1)	An appeal, including any related documents, by a person aggrieved by an order or direction of the Board, shall be filed in digital form, following such procedure as may be specified by the Appellate Tribunal on its website.	An appeal, including any related documents, by a person aggrieved by an order or direction of the Board, shall be filed **through digital means, including but not limited to written, audio, or video submissions, or via assisted appeal filing mechanisms. The Board shall ensure the development and availability of such accessible online measures and provide necessary assistance for the ease of filing appeals and complaints. The appeal shall be filed** following such procedure as may be specified by the Appellate Tribunal on its website.	Many citizens, especially those in rural areas or with limited digital literacy, may not have reliable access to digital infrastructure or the necessary technical expertise to navigate online submission processes. Thus, we recommend the provision be amended to include accessible digital appeal mechanisms, such as audio and video submissions, and assisted filing systems. The Board should also make the necessary investments to develop and maintain accessible appeal mechanisms. This can enhance procedural fairness, accessibility, inclusivity, and access to justice while maintaining the Act's digital-first approach.
22, read with Seventh	Calling for information from Data Fiduciary or intermediary.—(1) The Central Government may, for such	Calling for information from Data Fiduciary or intermediary.—(1) The Central Government may, for such purposes of	The existing provision under this Rule and the Seventh Schedule grants the Central Government broad and undefined powers to access personal

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
Schedule	purposes of the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person.	the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person. **(a) Any such request shall be subject to prior approval by a competent judicial authority.** **(b) The request must clearly state specific and legitimate grounds for**	data from Data Fiduciaries and intermediaries under the pretext of "sovereignty," "integrity," and "security of the State." The lack of precise legal definitions for these terms allows for arbitrary interpretation and overreach, raising concerns about excessive data collection, mass surveillance, and being privacy intrusive. This directly contradicts Justice K. S. Puttaswamy v. Union of India (2017) ruling,[46] which established the right to privacy as a fundamental right and required that any state intervention in personal data must meet principles of legality, necessity, proportionality, and adequate safeguards. The provision's lack of oversight further exacerbates the issue, as it enables the government to designate any authority to request personal data without requiring judicial approval, creating significant potential for misuse. Additionally, the clause avoids disclosing

[46]Justice K S Puttaswamy (Retd.) and Another vs. Union of India and Others SC WP(C) No. 494 of 2012.

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
		requiring the personal data and such requests shall avoid excessive collection of data. **(c) The request shall be subject to the principles of necessity and proportionality.** **(d) The government shall publish annual reports on the number, nature, and purpose of such data access requests, in a timely manner.** **(e) A right to appeal shall be available to Data Fiduciaries or intermediaries before the jurisdictional High Court.**	information about such government requests, shielding these actions from public scrutiny and undermining citizens' trust in digital governance. The provision's vague language also permits data access for broadly defined purposes such as performing functions under any law, which could justify large-scale data collection without proportionality. To address these risks, it is essential to introduce safeguards such as judicial oversight, and a necessity-based threshold for data requests. Moreover, transparency mechanisms, including mandatory periodic reports on government data requests, should be introduced to uphold public accountability while balancing national security interests. MeitY can upload such reports on its website. To this end, CUTS recommends amending the clause to introduce clear limitations on the scope of data access, mandatory judicial or independent

Rule	Draft Digital Personal Data Protection Rules, 2025	Suggested Amendments	CUTS Comments and Rationale
			oversight for all government data requests, a necessity and proportionality test for such requests, and transparency measures such as periodic public disclosure of aggregated data access reports. These safeguards will ensure that data protection principles are upheld while balancing legitimate state interests with individual privacy rights. We also recommend including the provision for right to appeal in the High Court. It will ensure due process and accountability, preventing arbitrary or excessive data access requests. It allows Data Fiduciaries and intermediaries to challenge unjustified demands, safeguarding privacy and proportionality in government surveillance.

Suggested additions to the
FIRST SCHEDULE - PART B

New Clauses

9. The Consent Manager shall–

(a) Avoid conflict of interest with Data Fiduciaries, including in respect of their promoters and key managerial personnel.

(b) Disclose mechanisms it uses to prevent conflict of interest with Data Fiduciaries. The information will be disclosed on website, mobile application, key policies, and half-yearly reports to the Data Protection Board of India.

(c) Clearly and upfront disclose all its fees and charges collected, in any form whatsoever, from Data Fiduciaries to Data Principals.

(d) Whenever engaging with a new data fiduciary, or when terms of engagement with an existing data fiduciary changes, shall disclose how such new engagement cannot be considered as a conflict of interest.

10. The Consent Manager shall–

(a) have in place measures to ensure that no conflict of interest arises on account of its directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries, or having a material pecuniary relationship with them.

(b) Disclose mechanisms it uses to prevent conflict of interest with Data Fiduciaries. The information will be disclosed on website, mobile application, key policies, and half-yearly reports to the Data Protection Board of India.

(c) Clearly and upfront disclose all its fees and charges collected, in any form whatsoever, from Data Fiduciaries to Data Principals.

(d) Whenever engaging with a new data fiduciary, or when terms of engagement with an existing data fiduciary changes, shall disclose how such new engagement cannot be considered as a conflict of interest.

11. The Data Protection Board shall monitor the functioning of Consent Managers, in particular compliance with clauses 9 and 10, and publicly disclose names of Consent Managers found to be in conflict of interest with Data Fiduciaries.

Suggested additions to the 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.	Class of Data Fiduciaries	Conditions
(1)	(2)	(3)
1.	A Data Fiduciary who is a clinical establishment, mental health establishment or healthcare professional	Processing is restricted to provision of health services to the child by such establishment or professional, to the extent necessary for the protection of her health**, while ensuring user anonymity and data minimisation.**
2.	A Data Fiduciary who is an allied healthcare professional	Processing is restricted to supporting implementation of any healthcare treatment and referral plan recommended by such professionals for the child, to the extent necessary for the protection of her health**, while ensuring user anonymity and data minimisation.**
6.	**A Data Fiduciary offering age-estimation services**	**Processing is restricted to age estimation solely for the purpose of verifying whether an individual meets the age requirements for access to a service–** **(a) with appropriate security measures and transparency to teenagers and to parents of tween and young children, regarding the methodology, accuracy, and limitations of the age-estimation process.**
7.	**A Data Fiduciary providing digital services for children**	**Processing is restricted to:** **(a) Delivering safe personalised content and recommendations for tween and teenager, provided such personalisation is**

S. No.	Class of Data Fiduciaries	Conditions
		transparent, does not exploit behavioural profiling, and remains in the best interests of the child. **(b) Allowing teenagers to exercise greater control over their data, including the ability to access, modify, or delete their personal information in line with their evolving autonomy and digital participation rights, and choose the type and category of personalised content and advertisements which can be suggested or shown to her.** **(c) Prohibiting targeted advertising and profiling-based recommendations for young child** **(d) Ensuring that any tracking directed at tweens is age-appropriate, non-exploitative, and aligned with child welfare principles, with integrating parent's perspectives** **(e) Ensuring that any tracking directed at teenagers is age-appropriate, non-exploitative, and aligned with child welfare principles.**

Note: In this Schedule—

(a) "Young child" means individual who has not completed the age of eight years;

(b) "Tween" means an individual who has completed the age of eight years but has not completed the age of thirteen years.

(c) "Teenager" means an individual who has completed the age of thirteen years but has not completed the age of eighteen years.

Suggested additions to the FOURTH SCHEDULE - PART B

Purposes for which provisions of sub-sections (1) and (3) of section 9 shall not apply

S. No.	Purposes	Conditions
(1)	(2)	(3)
4.	For ensuring that information likely to cause any detrimental effect on the wellbeing of a child is not accessible to her	Processing is **permitted** to the extent necessary to ensure that such information is not accessible to the child**, provided that following conditions are met**– **(a) adopt security by design principles, embed privacy protections at every stage of data collection and processing, ensuring minimal data collection, strong encryption, and secure storage;** **(b) collecting only essential behavioural data, with time-bound retention;** **(c) providing clear and accessible controls to teenagers and to parents of tweens and young children to manage data preferences and opt out of them;** **(d) publish periodic compliance reports in the public domain, detailing their adherence to child protection standards, data collection practices, and risk mitigation measures.**
6.	**A Data Fiduciary providing personalised digital services for content delivery**	**Processing is restricted to offering personalised recommendations to the extent necessary for availability of the content, adopting appropriate measures for detecting and preventing harmful interactions, exposure to harmful content, or predatory behaviour, or anything that harms well -being of the child.**

Annexure - I

Regulation of Behavioural Monitoring and Targeted Advertisements Directed at Children: Ensuring Personalisation Benefits Children[47]

The internet has become an integral part of children's lives, playing a crucial role in their education, social interactions, and access to information. The growth of personalised internet, enabled by behavioural monitoring and targeted advertising, has significantly shaped children's online engagement, tailoring content to their needs and interests. It offers opportunities for enhanced learning, provides tailored health and well-being resources, and fosters inclusive and safe online communities. It helps enhance the relevance of content considering diverse linguistic, cultural, and socioeconomic backgrounds.

Further, personalisation ensures free content availability, which is crucial for maintaining digital rights, especially for children from economically constrained backgrounds. It also fosters inclusivity and accessibility, particularly in diverse countries like India, by addressing varying linguistic, cultural, and socioeconomic needs. It aids children with disabilities through tools like voice interactions and eye-tracking and helps shield them from harmful content while promoting positive behaviours like financial literacy and public health awareness. Additionally, personalisation aids in empowering young creators by allowing them to engage meaningfully with their audience, and leverage the potential of the digital economy.

When done wrong though, personalisation carries significant risks. Excessive collection of sensitive personal data increases the risk of data breaches and privacy violations, while manipulative advertising practices can exploit children's evolving critical reasoning skills. It can promote excessive screen time, leading to adverse physical and mental health outcomes. Unregulated behavioural monitoring can inadvertently stereotype children based on their online activities, reinforcing biases and limiting their exposure to diverse viewpoints. Without proper standards and safeguards, risks like exposure to inappropriate content, commercial targeting of children, and privacy violations can emerge.

[47]CUTS International. (2025). Regulation Of Behavioural Monitoring and Targeted Advertisements Directed at Children: Ensuring Personalisation Benefits Children. https://cuts-ccier.org/pdf/regulation-of-behavioural-monitoring-and-targeted-advertisements-directed-at-children-ensuring-personalisation-benefits-children.pdf

The UK's Information Commissioner's Office framework recommends using personalisation to deliver appropriate content to children while also cautioning against its inaccurate application.[48]

Benefits of personalisation done right and risks of personalisation gone wrong[49]

Rights of children	Benefits of personalisation done right	Risks of personalisation gone wrong
The inherent right to life and survival. Their physical and emotional development should not be impeded.	Promotes positive health behaviours and online safety tools	Exposes children to unsuitable content (for example age-inappropriate products, self-harm or inaccurate health information)
Right to information from a diversity of digital media sources, and in particular those that promote their social well-being and general health.	Results in targeting news information in the best interests of the child	Exposes children to information not in their best interests (for example misinformation)
Right to be protected from all forms of physical or mental violence, abuse, maltreatment or exploitation.	Provides access to safe and child-appropriate content	Exposes children to violent or abusive content
Right to the highest attainable standards of health, and access to health care information and services online.	Promotes public health messaging and advice	Exposes children to inaccurate health information.
Children have a right to be protected from economic exploitation of all forms.	Targets content that promotes financial literacy, skilling and safe online behaviour.	Target adverts and service features that generate revenue for children (for example loot boxes or in-game purchases), using on-by-default settings, without adequate transparency or safeguards. Leads to fraudulent or misrepresented products.

[48]Profiling for content delivery and service personalisation, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/profiling-for-content-delivery/

[49]Personalisation goes wrong when it is done without necessary principles, safeguards, standards, and oversight, prioritising commercial gains over children's well-being and exposing them to content that may not be in their best interests.

Rights of children	Benefits of personalisation done right	Risks of personalisation gone wrong
Children have a right to be protected from the illicit use of drugs and age-restricted substances	Promotes information that protects children from drug abuse.	Target age-restricted products to children (for example alcohol)

There are various sector specific benefits, risks, and good practices of personalisation, which have been summarised below.

Behaviour Monitoring Use Cases: Benefits, Risks, and Recommendations

Use Case	Benefits	Risks	Recommendations
Education	Enhanced learning, higher student engagement, prediction of student performance, insights into curriculum and policy improvements, and personalised support for differently abled children.	Privacy and consent concerns due to tracking without appropriate safeguards, the potential to worsen existing inequalities in access to technology, and potential neglect of essential social and emotional skills.	● Implement graded exemptions for behavioural monitoring based on age. ● Ensure data is collected and processed only for service delivery. ● Implement robust data security measures.
Health & Well-being	Personalised health information, interventions, and support; access to sensitive information on topics like sexual health and mental well-being, early detection of mental health issues, timely intervention, and access to resources.	Potential decrease in self-regulation, reduced in-person social interactions, internet addiction, exposure to inaccurate health information and vulnerability to harmful content, and data security concerns with health data collection.	● Allow behaviour monitoring for mental health and well-being purposes with transparency and disclosures. ● Implement age appropriate exemptions. ● Promote digital literacy on health information and critical evaluation skills. ● Ensure robust data security and privacy measures for sensitive health data.
Safe spaces for marginalised communities	Community building, connecting individuals with similar interests, particularly for	Exposure to hate comments, harassment and abuse, misinformation, and	● Permit behavioural monitoring for credible dedicated platforms focused on providing

Use Case	Benefits	Risks	Recommendations
	marginalised groups, access to online spaces for LGBTQIA+ youth, children in abusive situations, and other vulnerable situations.	trolls, Misuse of platforms through impersonation, exploitation, and abuse of safe spaces intended for vulnerable communities.	services to marginalised communities. ● Implement strict safeguards to prevent misuse, impersonation, and online predation. ● Ensure robust safety and security standards and restrict data processing.
Age estimation services	Enables tailored age-appropriate content and features, improved options for parental monitoring and management of children's online activities, and facilitates safety & security through geolocation for monitoring children's movements and ensuring their safety.	The effectiveness of age estimation methods may be limited in certain contexts, privacy risks due to the collection of large amounts of sensitive data for age estimation, potential for reinforcing stereotypes and discriminating against children based on their online behaviour.	● Test age estimation technologies in a controlled environment (e.g., regulatory sandbox). ● Implement exemptions for verified age-estimation solutions with robust safeguards against data misuse and discrimination. ● Promote transparency and user control over age-related data collection and processing.
Social media	Helps users discover relevant content and trends, personalised feeds; enhances connection with friends and communities, provides platforms for children to express themselves, build communities, and unlock opportunities to monetise their talents.	Risk of data misuse, exploitation, and manipulation through targeted advertising, filter bubbles, limited exposure to diverse perspectives, potential influence on opinions and worldviews, negative psychological effects with concerns about addiction, self-image issues, and peer pressure.	● Empower users with transparency and control over personalisation algorithms. ● Implement age-appropriate safeguards against data misuse and manipulation. ● Promote media literacy and critical thinking skills to navigate social media responsibly. ● Address mental health concerns and provide support resources for online interactions.

Use Case	Benefits	Risks	Recommendations
Gaming	AI-driven player profiling detects cheating and ensures a fair environment, content filtering, and AI-powered detection of predatory behaviour, enhanced gameplay through matchmaking and engagement tracking for improved user experience.	Potential for excessive gaming and negative impacts on physical and mental health, concerns about the collection and use of player data for unintended purposes, and in-app purchases can lead to financial risks.	● Allow behaviour monitoring for safety and fairness purposes in gaming. ● Implement robust safeguards against data misuse and addiction. ● Promote responsible gaming practices and provide parental control tools. ● Regulate in-app purchases and protect children from financial exploitation.
Music & Podcasts	Personalised recommendations help users discover new music and podcasts, algorithms curate content based on user preferences, and platforms for creating and accessing podcasts on various topics.	Risk of encountering harmful or age-inappropriate music and podcasts, concerns about the collection and use of listening data for unintended purposes, filter bubbles and potential narrowing of musical tastes.	● Allow personalisation while ensuring data is processed responsibly and not misused. ● Implement age-appropriate content filtering.

A complete prohibition on behaviour monitoring and targeted advertisements, as proposed under section 9(3) of the Digital Personal Data Protection (DPDP) Act may deprive children of personalised internet benefits. Without personalisation, children may encounter irrelevant or harmful content, including material promoting self-harm, violence, or misinformation. This could jeopardise their online safety, diminish their digital experience, and restrict access to innovative services.

A depersonalised internet experience would also resemble traditional media, lacking the tailored experiences that digital platforms offer. The relevant content may go behind a paywall, limiting opportunities and investment in innovation, and children migrating to unregulated platforms, increasing security risks. The economic model of the internet could also undergo significant shifts, leading to subscription-based services, potentially excluding children from financially disadvantaged backgrounds,

deepening digital inequities. Thus, there is a need to adopt a nuanced approach to balance personalisation benefits with strong safeguards to prevent negative impacts.

A core recommendation is implementing age-appropriate frameworks that cater to the varying developmental needs of children and teenagers. Younger children under eight often struggle to discern commercial content, requiring robust protections and parental oversight to safeguard against targeted advertising and inappropriate material. In contrast, older children and teenagers (ages 13–17) have a more nuanced understanding of online interactions and the trade-offs between personalisation and privacy. Consequently, younger children (below eight) need strong protection from targeted advertising and inappropriate content through parental oversight. Tweens (ages 9–12) and Teenagers (ages 13–17), on the other hand, should be proportionately empowered to make informed choices, with clear disclosures on data use and privacy settings.

Thus, transparency and agency around behaviour monitoring and targeted advertisements become vital. Platforms must provide age-appropriate explanations of data collection and usage, enabling children and guardians to make informed decisions. Teenagers should be taught how personalisation algorithms work and how their choices influence the content they see. Platforms should offer tools for children and parents to control data-sharing preferences and opt out of unnecessary monitoring. Exemptions under the DPDP Act must consider age differences, ensuring tweens and teenagers are provided tools for transparency, algorithmic control, and accessible, age-appropriate information.

A risk-based framework is necessary to assess behavioural monitoring and targeted advertising practices. Policymakers should differentiate between beneficial and exploitative practices, allowing exceptions for services that benefit children. Purpose-specific data policies can limit monitoring to ethically sound uses. Platforms should also conduct regular Data Protection Impact Assessments (DPIAs) to identify and mitigate risks and also ensure that personalisation technologies are inclusive and equitable. They should prioritise accessibility features, such as multilingual support and tools for differently-abled users. Platforms must safeguard against misuse, including impersonation, trolling, and data exploitation, especially for marginalised groups.

Purpose distinction is essential for determining the ethical scope of behavioural monitoring. Monitoring for safety and well-being purposes, such as detecting cyberbullying, grooming, or mental health risks, should be clearly defined as permissible. However, high-risk automated processing, such as profiling children for

targeted advertising, must be strictly prohibited. Platforms must demonstrate evidence of benefit versus harm, showing that data collection is necessary and proportionate for fulfilling the intended purpose.

Privacy by design and default must be central to all platforms catering to children. Platforms must build privacy settings into the architecture of the product and implement high-privacy settings by default. They should also limit personal data collection to essential needs and require active consent for personalisation from children or parents/guardians. Measures like data anonymisation and shorter retention periods should be adopted to further protect sensitive information while enabling ethical personalisation.

Digital literacy for parents and children is also crucial for ensuring safe online environments for children. Parents should have tools to guide children's online interactions while respecting their privacy. For teenagers, digital literacy programmes are essential to build awareness about risks, privacy rights, and responsible technology use. Digital literacy programmes for teenagers must go beyond theoretical knowledge, equipping them to navigate personalisation algorithms practically and safely, in collaboration with schools, civil society, and industry. Policymakers should encourage collaboration between platforms and schools to integrate digital literacy into curricula, preparing children for the digital world.

Regulatory sandboxes are valuable for testing personalisation technologies in controlled environments. Platforms can test age-estimation, algorithmic transparency, and data minimisation practices before implementation at scale. Policymakers should use these outcomes to create robust, evidence-based regulations that prioritise children's safety and well-being. Policymakers must craft frameworks to nudge platforms toward safer consumer experiences, offering clear metrics for permissible tracking, including privacy protection, psychological impacts, and parental satisfaction.

The findings highlight the need for a balanced approach to regulating behavioural monitoring and targeted advertising, to ensure personalisation benefits children. Policymakers should adopt an evidence-based approach that ensures transparency, accountability, and inclusivity, fostering a safe and ethical digital ecosystem, while envisaging scenarios to allow behaviour monitoring and targeted advertisements, as provided under sections 9(4) and 9(5) of the DPDP Act. It is also crucial to explore more exemptions under the Fourth Schedule of the DPDP Rules, which are use-case specific. Such exemptions could be differentiated by age groups, aligned with principles of safe, ethical, and responsible data processing, and guided by a risk-based framework.

International examples emphasise the importance of both protecting children and empowering them to make informed online choices, offering valuable lessons for India. This approach will enable children to benefit from technology in a safe, enriching environment that supports their growth and development while ensuring their rights are protected.

Annexure - II

Economic Analysis of Verifiable Parental Consent Mechanisms[50]

Key Findings

The Digital Personal Data Protection (DPDP) Act, 2023, emphasises on individual consent, enhancing user control over personal data. It includes specific protections for children under 18, with Section 9 mandating data fiduciaries to obtain verifiable parental consent (VPC) from parents of the child. The recently released draft DPDP Rules propose that data fiduciaries verify parental identity and obtain parent's consent and propose two methods. 1) using existing platform data for current users, 2) through government-authorised entities or virtual non-user tokens.

This report analyses these proposed and other methods available for obtaining VPC and aims to present frameworks for policymakers and platforms to foster innovation while ensuring child safety and data protection. While regulatory intent is legitimate, factors such as parental digital literacy, privacy, security, and the financial costs of implementing VPC must be carefully considered.

VPC implementation costs are significant, involving expenses such as recurring software subscriptions, staff training, data collection, storage, and ongoing verification. Estimates from other countries, such as the U.S., suggest initial infrastructure costs of around $35,000 and ongoing annual costs of $70,000–$120,000.[51] Given that 29.9% of internet users are aged 0–17,[52] mandatory VPC systems could significantly impact a wide range of digital services, particularly those designed for children, making affordability and feasibility key concerns.[53]

The analysis of various VPC methods highlights that the DPDP draft Rules' prescribed verification mechanisms—using existing platform data or government-authorised services like Digital Locker—may not be optimal in terms of security, cost, or efficiency.

[50]Iqubbal, A. & Jugiani, K. (2025). Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries. CUTS International. https://cuts-ccier.org/pdf/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-on-consumers-and-data-fiduciaries.pdf
[51]Recent Developments In Privacy Protections For Consumers Hearing Committee On Commerce House Of Representatives, available at: https://www.govinfo.gov/content/pkg/CHRG-106hhrg67635/pdf/CHRG-106hhrg67635.pdf
[52]Digital 2024: India — DataReportal – Global Digital Insights, available at: https://datareportal.com/reports/digital-2024-india
[53]Singh, M., Nishant, Sachdeva, G., Tewari, A. (2024). Balancing Consent & Customisation. Youth Ki Awaaz, available at: https://www.youthkiawaaz.com/dpdpsurvey/

More flexible alternatives could enhance security for both minors and parents while reducing operational burdens.

No single verification method is accurate across all key parameters—cost, privacy, convenience, accuracy, and scalability. Some methods, like self-declaration and SMS consent, are cost-effective and scalable but lack accuracy and robustness, making them suitable for low-risk scenarios. Conversely, methods such as government ID verification or video consent offer higher accuracy but can be costly and inconvenient, making them more appropriate for high-risk contexts.

Estimated Costs of different methods (for 1,000,000 annual verifications)[54]

Method	Infrastructure/Setup Cost (A)	Operational Costs (B)	Storage Costs (C)[55]	Total Cost (A +B +C)	Total Cost (Average)	Cost Scale (Low To High)[56]
Self Declaration	10,000	818 – 996	260	11,078 – 11,256	11,167	Low
Age Estimation (AI/ML)	7,800	494,618[57]	260	502,678	502,678	High
Government-Issued ID	10,000	5,882 – 176,471	260	16,148 – 186731	101,440	Medium
DigiLocker	10,000	35,176	260	45,436	45,436	Low
Credit cards	10,000	5,294	260	15,554	15,554	Low
KBA	10,000	800,000	260	810,260	810,260	High
Third-Party Verification	10,000	235,294[58]	260	245,554	245,554	Medium
Email based consent	10,000	1,506 – 10,864	260	11,766 – 21,124	16,445	Low

[54]All the costs are in US$ and rounded off

[55]For simplicity, US$260, the average storage cost discussed above, has been taken.

[56]**Low**: Below US$50,000, **Medium**: Between US$50,000 and US$500,000, **High**: Above US$500,000.

[57]US$494,118 for annual 1,000,000 verifications and average annual subscription fees of US$500.

[58]The cost has been calculated based on a single verification, but service providers have indicated that it will decrease significantly as the user base grows. However, the exact amount can only be determined once the Rules come into effect.

Method	Infrastructure/Setup Cost (A)	Operational Costs (B)	Storage Costs (C)[55]	Total Cost (A +B +C)	Total Cost (Average)	Cost Scale (Low To High)[56]
Video consent	10,000	1,294 – 67,059	23,852[59]	35,416 – 100,911	68,164	Medium
SMS based consent	10,000	1,941	260	12,201	12,201	Low
ZKP	23,640	26,588	260	50,458	50,458	Medium
Operating System/ App store	25[60]	1,764 – 3,727[61]	260	2049 – 4012	3,031	Low
Interoperable VPC	10,000	Shared between platforms	260	10,260	10,260	Low

Key Features of different methods

Method	Privacy	Convenience	Accuracy	Scalability
Self Declaration	High because of minimal data collection	High because of its simplicity and accessibility	Very low due to lack of proof and potential for manipulation	Highly effective for low-risk use cases and on a larger scale
Age Estimation (AI/ML)	Low, due to continuous data collection and monitoring	High, as users may not be even aware	Moderate but prone to errors for near-age thresholds (e.g. 17 and 18)	Moderately scalable
Government -Issued ID	Low because of the risk of exposure to sensitive data	Low because it is time-consuming and can exclude users without official IDs	High accuracy when implemented with additional checks	Low, difficult to scale, especially in resource-constrained areas

[59]The average storage costs for the video file discussed above have been taken.

[60]for Google Play Store.

[61]Includes US$99 annual fee for Apple.

Method	Privacy	Convenience	Accuracy	Scalability
				and populations without IDs
DigiLocker	Low, because of the potential to reveal other details like name	Low, because of limited penetration	High as Aadhaar KYC is already used in the financial sector	Moderate because DigiLocker may not have universal access
Credit cards	Low, as limited threat of exposure of sensitive financial data	Moderate, as it is simple but excludes families without access to cards	Moderate, has risks in case of children having access to joint cards	Low due to limited card penetration in countries like India
KBA	Moderate to high privacy risks if knowledge about personal data is assessed	Moderate and avoids the need for additional hardware, but users may face frustration due to a set of personal questions	Moderate since it is vulnerable to generic or inaccurate answers	Low, costly and challenging to scale
Third-Party Verification	Low privacy and potential data overexposure to external entities.	High convenience but requires trust in third-party services	High but varies with implementation quality	Medium scalability but resource-intensive
Email based consent	High, collects limited data but is vulnerable to spoofing	High, easy to implement, relies on a common communication method	Low due to susceptibility to circumvention by tech-savvy minors	Moderate as it can scale efficiently with optimised delivery systems; however, it assumes that most people will have email IDs
Video consent	High privacy risk from facial and identity data	Low as it requires digital literacy and is invasive, too	High due to direct verification	Low, resource-heavy due to the need for a large staff, limits scalability

Method	Privacy	Convenience	Accuracy	Scalability
SMS based consent	High, relatively private, and avoid excessive data collection	Very high, quick and simple	Low since it risks circumvention in case of children having access to OTP	Very high scalability with robust SMS infrastructure
ZKP	High, preserving privacy through cryptographic proofs	High, easy to use	High precision depends on verifier and algorithm integrity	Moderate, requires advanced infrastructure and resources
Operating System/ App store	Moderate, relatively private, integrates with parental controls	Moderate, dependent on parents' understanding of digital platforms	Moderate depends on parental literacy and diligence	Highly scalable due to integration into existing ecosystems
Interoperable VPC	High, because of avoidance of repeated identity verification	High, easy to implement as parents' identity has already been established	High because one platform has already done the due diligence	High, as platforms can access already established identity through interoperable mechanisms

A market-driven approach—where platforms choose and transparently disclose their verification methods—would encourage competition, fostering more effective, user-friendly solutions. This flexibility would be particularly beneficial for smaller platforms, allowing them to adopt cost-effective yet secure verification processes, while larger platforms could implement more comprehensive systems based on their resources.

We recommend that the DPDP Rules should avoid rigid, one-size-fits-all approaches to VPC to encourage innovation and experimentation. A non-prescriptive, risk-based approach should be adopted, allowing service providers to choose verification methods based on use case, risk level, and implementation capabilities. Lower-risk activities like viewing general content can rely on simple self-declaration, whereas high-risk activities such as accessing age-restricted content or financial transactions require robust verification.

Additionally, an interoperable VPC framework should be incorporated, similar to interoperability in telecom and payments, enabling platforms to share verified consent

securely. This would reduce data collection, ease compliance burdens, and enhance efficiency, particularly for smaller platforms. For instance, if a parent is already verified on one platform, their verified identity should be usable by another platform, minimising the need for repeated verification and improving digital accessibility.

To balance innovation and child protection, an independent advisory group of consumer organisations, technical experts, and child development specialists should be established. This group would develop standards, manage grievances, assist small businesses, and promote responsible data handling by suggesting minimal data collection, restricted biometric processing, and user anonymity. Over time, it would assess VPC implementation, identify risks, propose mitigations, and educate policymakers, service providers, and parents to ensure safety, privacy, and accessibility remain central to the system's evolution.

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org , Web site: www.cuts-international.org
Also at Lusaka, Nairobi, Accra, Hanoi, Geneva, Delhi, Calcutta and Washington, D.C