CENTRE FOR COMMUNICATION GOVERNANCE AT

NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY ON THE DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in

Published by

Centre for Communication Governance
National Law University Delhi
Sector 14, Dwarka, New Delhi – 110078

Patrons: Professor (Dr.) G.S. Bajpai (Vice Chancellor, NLUD), Professor (Dr.) Ruhi Paul (Registrar, NLUD)

Faculty Director, CCG: Dr. Daniel Mathew

Executive Director, CCG: Jhalak M. Kakkar

Authors: Angelina Dash, Fawaz Shaheen, Nidhi Singh, Tejaswita Kharel and Tithi Neogi (in alphabetical order)

Editing and Review: Jhalak M. Kakkar and Shashank Mohan

Acknowledgements: This policy input was made possible by the generous support we received from the National Law University Delhi (NLUD). The Centre for Communication Governance (CCG) would therefore like to thank our patrons, the Vice Chancellor Professor (Dr.) G.S. Bajpai and the Registrar Prof. (Dr.) Ruhi Paul of NLUD for their constant guidance. CCG would also like to thank our Faculty Director Dr. Daniel Mathew for his continuous direction and mentorship. Special thanks to the ever-present and ever-patient Suman Negi and Preeti Bhandari for the unending support for all the work we do at CCG. Lastly, we would also like to thank all members of CCG for their invaluable inputs and feedback.

Suggested Citation – Centre for Communication Governance, 'Comments on the Draft Digital Personal Data Protection Rules' (2025)

TABLE OF CONTENTS

RULE 1: SHORT TITLE AND COMMENCEMENT

Rule 1 lays down a staggered timeline for implementation of the DPDP Rules. The Rules lay down a phased approach which prioritises the formation of the Data Protection Board of India.

A staggered timeline for implementation will allow Data Fiduciaries to incorporate and operationalise the provisions of the Act. However, when published the rules should provide a clear timeline for all provisions of the Act to reduce confusion and a risk of prolonged delay which will leave Data Principals without any mechanism for exercising their rights, despite the enactment of the DPDP Act. Ambiguity over the timelines for notification creates implementation challenges for all stakeholders, and adds to business uncertainties. Data Fiduciaries need to invest into creating a data protection architecture which is in consonance with the DPDP Act and the pursuant Rules.

A definite date laying out when specific parts of the Rules will come into force will provide certainty and allow Data Fiduciaries to plan their compliance measures and build appropriate capacity. This is in line with global standards, where other data protection instruments such as the GDPR laid down a two-year timeline for its implementation.[1]

[1] European Data Protection Supervisor, 'The History of the General Data Protection Regulation', <https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 28 February 2025.

RULE 3: NOTICE GIVEN BY DATA FIDUCIARY TO DATA PRINCIPAL

Rule 3 lays down the requirements for providing notice under Sections 5 and 6 of the DPDP Act.[2] However, the current Rule has significant limitations.

1. **Lack of granular consent:** The Rule lacks mechanisms for obtaining granular consent, forcing users to either share all requested data or forgo services entirely. This differs from the 2018 Data Protection Bill[3] and international standards like EU's GDPR,[4] Korea's PIPA,[5] and China's PIPL,[6] which allow for granular consent options. Using granular consent also supports the principle of data minimisation, by ensuring that users only have to share information which is required to obtain services.[7] The inclusion of granular consent mechanisms is critical in upholding the principles of free, specific, and informed consent and enabling user autonomy in digital spaces.[8]

---

[2] Sections 5 and 6 of the DPDP Act mandate that notices must be provided in clear language and separate from other information, including an itemised description of personal data to be processed, processing purposes, description of goods or services provided, and communication links to withdraw consent, provide access and file complaints.

[3] Section 18, Personal Data Protection Bill, 2018 (India) <https://prsindia.org/files/bills_acts/bills_parliament/1970/Draft%20Personal%20Data%20Protection%20Bill,%202018%20Draft%20Text.pdf> accessed 28 February 2025.

[4] General Data Protection Regulation, 2018 (European Union) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> accessed 23 February 2025.

[5] Article 4(2), Personal Information Protection Act, 2011 (South Korea) <https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=KOR> accessed 28 February 2025.

[6] Personal Information Protection Law, 2021 (China), <https://personalinformationprotectionlaw.com/> accessed 28 February 2025.

[7] CCG, UNDP Guide- Drafting Data Protection Legislation: A study of regional frameworks, p 46 <https://www.undp.org/sites/g/files/zskgke326/files/2023-04/UNDP%20Drafting%20Data%20Protection%20Legislation%20March%202023.pdf> accessed 28 February 2025.

[8] Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting a Digital India* (2018), p 35 <https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf> accessed 25 February 2025; Data Empowerment And Protection Architecture - Draft for Discussion (2020), p 33 <https://www.niti.gov.in/sites/default/files/2023-

2. **Best practice to ensure informed consent:** The current iteration of the Rules omit certain crucial aspects which should be added to a notice to ensure informed consent. Global best practices include adding legal basis for processing,[9] retention requirements,[10] data transfer circumstances,[11] and security measures[12] within the text of the notice.

3. **Ambiguous guidance to users on rights:** Another concern is the ambiguous implementation guidance. While Rule 3 provides access links for users to exercise their rights, it does not require explaining what those rights are or how to exercise them.[13] We recommend that notices should also contain an itemised list of user rights along with the mechanisms to operationalise them.

4. **Handling of legacy data:** A notable omission in the current rules is guidance on handling legacy data - personal information shared before the Act's commencement. Although Section 40(2)(b) of the DPDP Act empowers the government to make rules for this situation, the current rules do not address it. This leaves a significant gap in protecting previously collected personal data and ensuring the exercise of retroactive rights. We recommend that the requirements for provision of notice under the Rule be extended to legacy data as well.

03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf> accessed 28 February 2025.

[9] Section 23, Personal Data Protection Act, 2018 (Estonia) <https://www.riigiteataja.ee/en/eli/523012019001/consolide> accessed 28 February 2025.

[10] Article 15(4) Personal Information Protection Act, 2011 (South Korea); Section 23 Personal Data Protection Act, 2018 (Estonia).

[11] 13(1)(f) General; Article 28-8 Korea

[12] Section 29(f), Data Protection Act, 2019 (Kenya) <https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf> accessed 28 February 2025.

[13] Section 29 Data Protection Act, 2019 (Kenya) and Article 13 of the General Data Protection Regulation (2016) require the notice to contain a description of the rights of a user.

5. **Model formats for notice:** We recommend that the Rules should contain model templates/formats for notice which are user-friendly and avoid technical jargon.[14] These formats need not be mandatory and can act as a guide on how notice shall be provided. They should comply with accessibility standards for various groups such as those under the Rights of Persons with Disabilities Rules, 2017.[15] This standardisation would help ensure consistent implementation and better understanding across all organisations and user groups.

[14] The Report of the Joint Committee on the Personal Data Protection Bill, 2019 had mooted the idea of a model format that is easily comprehensible, even for laypersons, so that they can make informed choices before giving consent (pg. 265) <https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf> accessed 5 March 2025. The EU guide on implementing the GDPR also provides a model notice template <https://gdpr.eu/privacy-notice/> accessed 5 March 2025.

[15] Rights of Persons with Disabilities (Amendment) Rules, 2023 (India) <https://cdnbbsr.s3waas.gov.in/s3e58aea67b01fa747687f038dfde066f6/uploads/2023/11/20231129153 3057741.pdf> accessed 20 January 2025; Rule 15, Rights of Persons with Disabilities Rules, 2017 (India) <https://upload.indiacode.nic.in/showfile?actid=AC_CEN_25_54_00002_201649_1517807328299&type=rule&filename=Rules_notified_15.06.pdf> accessed 2 February 2025.

RULE 4: REGISTRATION AND OBLIGATIONS OF CONSENT MANAGER

The DPDP Act and Rules establish Consent Managers as registered entities serving as single points of contact for Data Principals to manage their consent through accessible, transparent, and interoperable platforms.[16] However, the current framework faces several significant challenges and limitations.

1**. Lack of operational clarity:** The Rule lacks operational clarity as it doesn't clarify the extent of data collection and sharing and the pricing structure applicable to consent managers. For instance, there are no obligations that specifically bar the consent managers from collecting excessive data, or specific details on the requirements that have to be met to showcase that conflict of interest is prevented. The ambiguity in data collection and exchange mechanisms creates risks of excessive data processing and potential misuse. Additionally, the lack of a defined pricing model raises concerns about financial barriers for Data Principals. The development, implementation, and maintenance of these systems involve substantial costs that may be passed down to the Data Principals. To address these challenges, the Rules should establish clear obligations limiting data collection (including metadata), and define sustainable pricing models where fiduciaries and processors primarily bear costs while easing the burden of cost on Data Principals.

2. **Lack of technical guidelines balancing transparency and data security:** Consent managers will have to develop interoperable platforms that can be used by a wide array of Data Fiduciaries without compromising data security and transparency principles. The current framework does not provide any technical guidelines for the implementation of such interoperable platforms, balancing transparency with data protection. It is unclear how consent managers can remain "data blind" when they are

[16] This framework builds upon existing architectures like the Data Empowerment and Protection Architecture (DEPA), and sectoral initiatives like the Account Aggregator framework in banking and the Ayushman Bharat Digital Mission (ABDM) in healthcare.

required to retain metadata of all the notices received, consents given and data shared with Data Fiduciaries We recommend the creation of detailed guidelines on technical aspects of the framework.

3**. Interoperability with existing consent management frameworks:** It is also important for the Consent Manager frameworks to fit into the broader information ecosystem. Consequently, Consent Managers under the DPDP Act must allow for interoperability with existing consent management systems such as the HIE-CM[17] in the ABDM and the Account Aggregator Framework.[18] This will allow for cross-sector interoperability, ensuring standardised and scalable frameworks.

4. **Classifying Consent Managers as Significant Data Fiduciaries ("SDFs"):** We recommend classifying Consent Managers as SDFs to ensure a higher standard of accountability due to the volume and sensitivity of data handled by them. This would subject them to stricter compliance measures, including mandatory data audits, Data Protection Impact Assessments, and the appointment of Data Protection Officers.

While the introduction of Consent Managers shows potential for enabling meaningful consent, the excessive minimisation of transactional friction in sharing of data can cause systematic desensitisation of users to privacy harms. To prevent consent from becoming a mere formality, the consent management framework must ensure that consent remains a deliberate and informed choice. It is crucial to strengthen oversight mechanisms and ensure regulatory enforcement for successful and meaningful implementation of this framework. This can be done by laying down clear technical guidelines that are consistent with data protection principles like transparency and data minimisation. Classifying Consent Managers as SDFs will also provide greater oversight and ensure a higher standard of accountability.

---

[17] Ministry of Health and Family Welfare, Health Information Exchange- Consent Manager, <https://abdmbeta.abdm.gov.in:8081/uploads/HIE_CM_58b5f555d2.pdf> accessed 26 February 2025.

[18] Account Aggregator (Reserve Bank) Directions, 2016 (India) <https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=10598> accessed 28 February 2025.

RULE 5: PROCESSING FOR PROVISION OR ISSUE OF SERVICES BY THE STATE OR ITS INSTRUMENTALITY

Rule 5 relates to the processing of data under Section 7(b) of the DPDP Act.[19] Rule 5(2) provides that such processing will follow the standards specified in the Second Schedule of the Rules.[20]

1. **Expanding the scope of "legitimate use" under DPDP Act:** Rule 5(3)(b) provides that data may be processed by the Central or State Government under any policy in exercise of their executive powers. The language of the Rule goes beyond merely enabling the processing of personal data by the executive in pursuance of a legislative purpose, and makes it subject to discretionary power as well. The overbroad phrasing covers agencies and officials involved in everything from building permits to driving licenses.

Rule 5(3)(c) takes this even further to include processing for use of any public funds by the Central or State Governments or any other local authority. This effectively means that any State agency or official could process personal data without the consent of the Data Principals, as long as it can be tied to the use of public funds. The Rules must provide detailed operative guidelines to ensure proper implementation of 7(b) of the DPDP Act. The current phrasing is overbroad which enables excessive discretionary power..[21] It also dilutes the critical safeguards included in the Second Schedule (such as use for lawful

[19] Section 7(b) of the DPDP Act provides for legitimate use of personal data available with the State or its instrumentalities for the provision of benefits to a Data Principal.

[20] These include requirements that the data must be processed lawfully, that it must be limited to purposes specified in the DPDP Act and retained only for a limited time. Where data is being used for purposes specified under Section 7(b) of DPDP Act or Rule 5(2) of the DPDP Rules, it also requires the state or its instrumentality to provide the data principal with an intimation of the same. This intimation must include contact information of the person who can answer questions about such processing, as well as other means through which the data principal can exercise their rights under the DPDP Act.

[21] The current phrasing provides broad discretionary powers without specifying the purposes or limits for which it may be used. This effectively means that any State agency or official, as well as private entities engaged by them, will be able to process personal data without the consent of the Data Principals, as long as it can be tied to the use of public funds in any way.

purpose, storage limitation, and providing intimation to Data Principals) of the DPDP Rules, since any use of public funds can be shown as a lawful purpose within the meaning of Rule 5(3)(c).

2. **Insufficient Safeguards**: The safeguards provided under the Second Schedule are limited, and do not adequately consider constitutional protections for privacy. Apart from the requirement of lawfulness included in the draft, the Second Schedule also needs to incorporate necessity and proportionality laid down by the Supreme Court in the *Puttaswamy* judgement.[22]

3. **Failure to define "State or its instrumentalities":** Finally, the word "instrumentalities" has not been defined and can be construed to mean any person or body corporate associated with the State to carry out a function. This could include private entities like corporations and NGOs acting as implementing agencies, partners, service providers or subcontractors in carrying out welfare schemes and programs of the State. Therefore, the word "instrumentalities" must be clearly defined to include only those entities which are covered under the meaning of "State" or "other authorities" under Article 12 of the Constitution of India.

[22] *Justice K.S. Puttaswamy vs. Union of India* AIR 2017 SC 4161, <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors> accessed 27 February 2025.

RULE 6: REASONABLE SECURITY SAFEGUARDS

Rule 6 lays down security measures that the Data Fiduciary must adopt under Section 8(5) of the DPDP Act to protect personal data. However, the Rules need to provide further clarity for Data Fiduciaries to effectively operationalise these safeguards.

1. **Failure to define key terms:** While Rule 6(1)(a) recommends the use of technologies such as encryption, obfuscation and masking, they are not defined in the parent Act or the Rules, which leads to operational uncertainty. The Rule also provides for the use of virtual tokens as a form of security safeguard.[23] However, the Rule lacks operative guidance on what would be considered as virtual tokens, and how they will be mapped to personal data. We recommend that the Rules should define these terms to provide more clarity.

2. **Periodic guidance on specific security measures:** The Rules set broad standards of reasonableness and appropriateness for security safeguards. We recommend that Rules should mandate that the Board must provide periodic guidelines on specific security measures, similar to the European Data Protection Board. This will ensure that the security standards provided in the Rules stay up to date with technological developments.

3. **Context specific security safeguards:** The Rule does not consider sensitivity of data while providing standards for security. Singapore's PDPA[24] recommends opting for context specific safeguards, for example, providing higher security standards for confidential information such as employee appraisals as opposed to generic project-related information. We recommend that similar context specific security standards be built into Rule 6.

---

[23] The use of virtual tokens, or tokenization, refers to a data security practice where sensitive data is converted into a digital replacement, also called a token, which can be used to safely store the sensitive data.

[24] Personal Data Protection Commission (PDPC), 'Advisory Guidelines on Key Concepts in the PDPA', Singapore (17 May 2022) <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf> accessed 28 February 2025.

RULE 7: INTIMATION OF PERSONAL DATA BREACH

The obligation on a Data Fiduciary to notify the Board and the affected Data Principal regarding any personal data breach arises out of Section 8(6) of the DPDP Act. Rule 7 provides clarity on the details that a Data Fiduciary must provide to both the relevant Data Principals and the Board while intimating about the breach.

This Rule allows the affected parties to be informed of potential risks, enabling them to take necessary steps to mitigate harm. It also reinforces accountability among Data Fiduciaries by mandating transparency in their handling of data breaches.

1. **Specific time period for notification:** While the Rule provides clarity on the form and manner of intimation of the personal data breach, the Rule does not specify the time period within which the personal data breach is to be notified. The use of the term "without delay" is vague and may enable misuse. We recommend that the Rule clearly state a specific time period (for example 72 hours) to provide intimation of breach. This will ensure that Data Principals are provided timely notification of such breach. When Data Principals are informed, they will be able to implement measures to mitigate possible harms that may arise as a consequence of the breach.

2. **Providing notifications in an accessible manner:** In order to ensure that Data Principals are aware of the data breach, the Rule provides that the notification be made in a "concise, clear and plain manner". The inclusion of this language aims to ensure that the Data Principals understand the contents of the intimation. The Rules should also include provisions mandating accessibility as per the standards laid out in Rule 15(1)(c)(iii) of the Rights of Persons with Disabilities Rules, 2017.[25] The said Rule requires that products and services which are based on information and communication

[25] Rights of Persons with Disabilities (Amendment) Rules, 2023 (India) <https://cdnbbsr.s3waas.gov.in/s3e58aea67b01fa747687f038dfde066f6/uploads/2023/11/20231129153 3057741.pdf> accessed 20 January 2025; Rule 15, Rights of Persons with Disabilities Rules, 2017 (India) <https://upload.indiacode.nic.in/showfile?actid=AC_CEN_25_54_00002_201649_1517807328299&ty pe=rule&filename=Rules_notified_15.06.pdf> accessed 2 February 2025.

technology shall comply with Bureau of Indian Standards' IS 17802 (Part 1 & 2): 2021 and 2022.[26] Integrating these standards will ensure that all individuals, regardless of their abilities, can effectively exercise their rights, thereby ensuring accessibility to Data Principals' rights.

[26]Bureau of Indian Standards, Accessibility for the ICT Products and Services, IS 17802 (Part 1): 2021 <https://broadbandindiaforum.in/wp-content/uploads/2022/08/IS-17802_1_2021.pdf>; Bureau of Indian Standards, Accessibility for the ICT Products and Services, IS 17802 (Part 2): 2022 <https://broadbandindiaforum.in/wp-content/uploads/2022/08/IS-17802_2_2022.pdf>.

RULE 8: TIME PERIOD FOR RETENTION

Rule 8 and the corresponding Third Schedule lay down the period of retention and erasure for specific classes of Data Fiduciaries.

1. **Including sensitivity of data as a criterion for classification:** The current mechanism for classification is over reliant on the number of users and only covers three classes of Data Fiduciaries, namely e-commerce platforms, social media intermediaries and gaming websites. We recommend the inclusion of the sensitivity of personal data being processed as a criterion for determining the period of retention. For example, an e-commerce entity selling sexual wellness products or an online dating app should be subject to the safeguards under Rule 8 based on the sensitivity of data, irrespective of the number of users. Further, a longer retention period can make data more susceptible to breaches which may have dire implications due to the sensitive nature of the information.

2. **Global best practices on safeguarding sensitive data:** Accounting for additional safeguards based on sensitivity of personal data is informed by global best practices such as Council of Europe's Convention 108+[27] and the GDPR.[28] Convention 108+ allows for processing of special categories of personal data only if adherence to appropriate safeguards is ensured. This is because the processing of sensitive data may increase the risk of discrimination and curb fundamental freedoms and rights.[29] Similarly, Recital 51 of the GDPR also acknowledges that sensitive personal data warrants additional safeguards since its processing could significantly limit fundamental rights and freedoms.[30] In line with these provisions, the Rules should provide an additional level of safeguards for the retention and processing of sensitive personal data. This can include

[27] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+), ETS 108, 28 January 1981 <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> accessed 28 February 2025.

[28] General Data Protection Regulation (2016).

[29] Article 6, Convention 108+ (1981).

[30] Recital 51, General Data Protection Regulation (2016).

specific time periods for classes of Data Fiduciaries and purposes of processing which involve sensitive personal data.

3. **Defining sensitive personal data:** Sensitivity can be interpreted as per definitions formerly provided under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,[31] and previous iterations of the DPDP Bills, including the Personal Data Protection Bill, 2019,[32] the Personal Data Protection Bill, 2018,[33] and the Srikrishna Committee Report.[34] The scope of sensitive personal data could include passwords, financial information, health and medical data, data relating to sexual orientation, and biometric information.

[31] Rule 3, The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (India).

[32] Clause 2(36), The Personal Data Protection Bill, 2019 (India).

[33] Clause 3(35), The Personal Data Protection Bill, 2018 (India).

[34] Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting a Digital India* (2018) p 31 <https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf> accessed 28 February 2025.

RULE 9: CONTACT INFORMATION OF PERSON TO ANSWER QUESTIONS ABOUT PROCESSING

The obligation on a Data Fiduciary to provide the contact information of the Data Protection Officer, or a person who is able to answer on behalf of the Data Fiduciary arises out of Section 8(9) of the DPDP Act. Rule 9 provides that the contact information shall be published prominently on its website or app and shall be shared as a response to any communication for the exercise of the rights of a Data Principal.

The Rule empowers Data Principals by facilitating accessible communication channels to exercise their rights and seek clarifications regarding the processing of their personal data. However, even though the Rule provides clarity on when and where the contact information is to be shared, it does not provide any guidance on how such information is to be made accessible to all.

In order to ensure accessibility, the Rule should include provisions mandating accessibility in the website or app as per the standards laid out in Rule 15(1)(c)(iii) of the Rights of Persons with Disabilities Rules, 2017.[35] The said Rule requires that products and services which are based on information and communication technology, shall comply with Bureau of Indian Standards' IS 17802 (Part 1 & 2): 2021 and 2022.[36] Integrating these standards ensures that all individuals, regardless of their abilities, can effectively exercise their rights, thereby ensuring accessibility to Data Principals' rights.

---

[35] Rights of Persons with Disabilities (Amendment) Rules, 2023 (India) <https://cdnbbsr.s3waas.gov.in/s3e58aea67b01fa747687f038dfde066f6/uploads/2023/11/20231129153 3057741.pdf> accessed 20 January 2025; Rule 15, Rights of Persons with Disabilities Rules, 2017 (India) <https://upload.indiacode.nic.in/showfile?actid=AC_CEN_25_54_00002_201649_1517807328299&ty pe=rule&filename=Rules_notified_15.06.pdf> accessed 2 February 2025.

[36] Bureau of Indian Standards, Accessibility for the ICT Products and Services, IS 17802 (Part 1): 2021 <https://broadbandindiaforum.in/wp-content/uploads/2022/08/IS-17802_1_2021.pdf>; Bureau of Indian Standards, Accessibility for the ICT Products and Services, IS 17802 (Part 2): 2022 <https://broadbandindiaforum.in/wp-content/uploads/2022/08/IS-17802_2_2022.pdf>.

RULE 10: VERIFIABLE CONSENT OF PARENTS OR LAWFUL GUARDIAN FOR PROCESSING

Rule 10 operationalises the processing of personal data for children and persons with disabilities under Section 9 of the DPDP Act.

Rule 10(1): Processing Personal Data of Children

1. **Uncertainty regarding presumption of majority:** Rule 10 does not prescribe the standard for presumption of minority, i.e. whether Data Fiduciaries should assume all users are children or adults unless specified otherwise, leading to operational uncertainty. Global best practices include the development and use of age assurance mechanisms in countries like Australia[37] and the USA,[38] and the guidance on 'age checks to protect children online'.[39]

2. **Differentiating standards based on likelihood of harm:** These mechanisms also follow a tiered system with higher thresholds for certain digital services based on the likelihood of use by children, and potential harm. Services which have been established as likely to be accessed by children, and services allowing pornography, are required to comply with the children's risk assessment duties like age verification.[40] Similarly, Recital

---

[37] eSafety Commissioner, *Age assurance* (eSafety Commissioner 2024) <https://www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1732247092556> accessed 23 April 2025; Age assurance refers to a set of technologies and mechanisms used to verify the age of an individual, typically to ensure compliance with regulations relating to online services, content access, or data processing.

[38] Federal Trade Commission, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' (June 2017) <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business> accessed 27 February 2025.

[39] Ofcom, 'Age checks to protect children online' (*Ofcom*, 16 January 2025) <https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online/> accessed 27 February 2025.

[40] ibid.

38 of the GDPR[41] and the Children's Online Privacy Protection Rule (COPPA)[42] specify that age verification must be done particularly in the case of services being offered directly to a child. This means that mandatory age verification (as well as other stringent obligations) only becomes a requirement for digital services likely to be used by children, instead of becoming a burden on all operators. We recommend including comparable specificity in the Rules regarding the scope of age verification to provide operational clarity for data fiduciaries.

3. **Excessive data collection due to VPC:** The Rules also introduce a Verifiable Parental Consent (VPC) mechanism, but do not provide sufficient clarity on how to establish a parent-child relationship. The VPC mechanism contravenes the principle of data minimisation by collecting excessive data. The Rules should lay down a tiered approach for VPC mechanisms to use IDs only for certain categories based on risk and accessibility assessments.[43] Criteria for assessments can include volume and proportion of children's data and possibility of harm to the child.[44] Data Fiduciaries must also delete such identification from their records after the completion of verification.[45]

Rule 10(2): Processing Personal Data of Persons with Disabilities

1. **Uncertainty due to clubbing Persons with Disabilities and Children:** Clubbing persons with disabilities with children infantilises them by equating the role of the lawful guardian with that of the parent.[46] It also creates uncertainties in terms of

---

[41] Recital 38, General Data Protection Regulation (2016).

[42] Section 312.3, Code of Federal Regulations, Title 16 <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312> accessed 28 February 2025.

[43] UK Information Commissioner's Office, 'Age appropriate design: Age Appropriate Application' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/> accessed 27 February 2025.

[44] Clause 16(3), The Personal Data Protection Bill, 2019 (India).

[45] Section 312.5(b)(v), Code of Federal Regulations, Title 16.

[46] Angelina Dash and Tithi Neogi, 'Persons with Disabilities vis-à-vis the Digital Personal Data Protection Act, 2023', (2024) Centre for Communication Governance at National Law University Delhi <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/persons-with-disabilities-vis-a-vis-the-digital-personal-data-protection-act-2023-709.pdf> accessed 27 February 2025.

whether provisions of Rule 10(1) relating to children will also apply to persons with disabilities. For instance, it is unclear whether the system of virtual tokens relating to children's data mentioned in Rule 10(1)(b) would also be applicable to persons with disabilities. Further, Rule 10(2) requires Data Fiduciaries to observe due diligence while obtaining verifiable consent from lawful guardians of persons with disabilities. However, it does not lay down appropriate specifications for a mechanism to obtain such verifiable consent. It is unclear whether the system of virtual tokens relating to children's data mentioned in Rule 10(1)(b) would also be applicable to persons with disabilities. We recommend including detailed guidance on the applicability of consent and virtual tokens under Rule 10(2).

2. **Lack of illustrations under Rule 10(2):** We recommend the inclusion of illustrations for operationalising verifiable consent collection for persons with disabilities under Rule 10(2), informed by principles like limited guardianship under the Rights of Persons with Disabilities Act, 2016.[47]

[47] Section 14, The Rights of Persons with Disabilities Act, 2016 (India); Limited guardianship is a system of joint decision-making between the person with disability and their lawful guardian. The system is grounded in mutual trust and its operation is limited to specific decisions, specific periods and on the basis of the will of the person with disability.

RULE 11: EXEMPTIONS TO OBTAINING PARENTAL CONSENT FOR PROCESSING CHILDREN'S DATA

Rule 11 and the Fourth Schedule create exemptions to the obligation of collecting parental consent for processing children's data. This obligation is provided under Section 9(1) and (3) of the DPDP Act, which also includes a ban on tracking, behavioral monitoring and targeted advertising to children. The Fourth Schedule lays down classes of Data Fiduciaries that are exempted from the obligation to collect parental consent as well as the bar on targeted advertisement.

1. **Exemptions for educational institutions:** Entry 3, Part A of the Fourth Schedule includes exemptions for educational institutions that create scope for promoting commercial interests such as the use of targeted advertising by coaching institutes. We recommend that commercial applications should be excluded from the exception provided for educational activities.

2. **Geolocation tracking and behavioural monitoring of children:** Entries 4 and 5, Part A of the Fourth Schedule also allow geolocation tracking and behavioural monitoring for certain classes of Data Fiduciaries. This is extremely sensitive data which can be misused by bad actors. Continuous tracking and monitoring of children's activities may be overall detrimental and hinder the development of their identity.[48] We recommend that both parents and children should be provided a notice in respect of tracking and monitoring data. The notice should also allow for parents to opt out of the processing or request the deletion of such information collected. This is in line with best practices from COPPA which requires a notice to be provided to parents for processing for the purpose of children's safety.[49]

---

[48] UK Information Commisioner's Office, 'Age appropriate design: Geolocation' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/> accessed 27 February 2025; A lack of transparency concerning location tracking may also contravene children's privacy under Article 16 of the United Nations Convention on the Rights of the Child, 1989.

[49] Section 312.3(b)(5), Code of Federal Regulations, Title 16.

3. **Barring access to information for children:** Entry 4, Part B of the Fourth Schedule creates exemptions to bar children's access to information likely to have a "detrimental effect" on their well-being. This broad phrasing may result in Data Fiduciaries being overcautious and undertaking practices like shadowbanning to limit the information available to children on sensitive subjects like sexuality, reproductive health and mental health. This would dilute children's right to access information under the freedom of expression.[50]

We recommend that the Fourth Schedule include more procedural safeguards to ensure that the rights of the child and their best interest are being balanced against the provisions of Rule 11. It should also include mechanisms to make details of data collected and the purpose of processing available to the parents. A lack of transparency to parents can curb their ability to make decisions in the best interests of their child.[51]

4. **Applying verifiably safe standards instead of broad exemptions:** Section 9(5) of the DPDP Act allows the exemption of specific Data Fiduciaries from obtaining parental consent after verifying their safety standards. The exemptions under Rule 11 should adopt a similar limited approach based on "verifiably safe standards" instead of the broad exemptions laid down in the Fourth Schedule. For instance, instead of providing broad exemptions for all educational institutions, the Rules could exempt only those institutions that can demonstrate appropriate safety standards being applied by them.

[50] Article 17, United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) UNGA Res 44/25, 1577 UNTS 3 <https://www.ohchr.org/sites/default/files/crc.pdf> accessed 28 February 2025.

[51] Preamble, United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) UNGA Res 44/25, 1577 UNTS 3.

RULE 12: ADDITIONAL OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARIES

Rule 12 lays down additional obligations on SDFs to conduct annual audits, assess privacy risks of algorithmic software and undertake Data Protection Impact Assessments (DPIA), in consonance with Section 10 of the Act.

1. **Prescribed format for DPIAs:** The Rule does not lay down a prescribed format for DPIAs or mandate the process to be followed to conduct one. While there is no universally accepted format of a DPIA, France's CNIL lays down methodology for conducting DPIAs which classifies the process into four steps, namely context, controls, risks and decision.[52] This method lays down a detailed mechanism which can be used by Data Fiduciaries to ensure compliance with the data protection law, and demonstrate their implementation of data protection principles. Conversely, the GDPR and the UK ICO lay down a more prescriptive framework for DPIAs. For instance, Article 35 of the GDPR lays down a list of minimum requirements that must be contained in a DPIA. It includes necessity and proportionality of processing, and potential risks and mitigation.[53] The UK ICO similarly lays down necessity and proportionality assessments and compliance with privacy principles that must be included in a DPIA.[54] We recommend that the Rules also lay down mechanisms to provide more detailed guidance on the methodology and contents of the DPIAs.

2. **Audit of algorithmic systems:** The mandate to conduct audits on algorithmic systems deployed by SDFs as per Rule 12(3) should also be brought within the ambit of

---

[52]Commission Nationale de l'Informatique et des Libertés (CNIL), 'PIA Methodology' (2015) <https://www.cnil.fr/sites/cnil/files/typo/document/CNIL-PIA-1-Methodology.pdf> accessed 28 February 2025.

[53] Article 35, General Data Protection Regulation, (2016)

[54]Information Commissioner's Office (ICO), 'Data Protection Impact Assessments' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/> accessed 28 February 2025.

the DPIA. This ensures that such an audit would be conducted annually and also be reported to the Board.

3**. Publication of DPIA:** We recommend that Rule 12(2) create an obligation on the Data Protection Board to publish the DPIA and the algorithmic audit reports with appropriate safeguards to uphold transparency and accountability towards Data Principals. For instance, the UK's ICO publishes the executive summary of a completed audit on its website. The WP29 Guidelines on DPIA[55] suggest publishing a statement on the completion of the DPIA in case the complete report could reveal commercially sensitive information.

4. **Lack of clarity on cross-border data flows:** Finally, Rule 12(4) allows for restrictions on cross-border data flow for "specified personal data" as recommended by a committee constituted by the Central Government. This is a vague and overbroad application of the powers under Section 16(1) of the DPDP Act. The Rules should include more details regarding the kinds of data which may be restricted and the composition of the committee which would make these recommendations. This would allow for operational clarity and for stakeholders to provide nuanced feedback on the composition of the committee and the categories of personal data affected by this provision.

[55] European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (2017) <JUSTICE AND CONSUMERS ARTICLE 29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)>, accessed 28 February 2025.

RULE 13: RIGHTS OF DATA PRINCIPALS

Rule 13 mandates that Data Fiduciaries and Consent Managers must publish mechanisms for operationalising the rights of Data Principals. However, the provision lacks sufficient detail which may affect its implementation.

1. **Time period for responding to Data Principal's request:** Rule 13 does not prescribe the period to respond to a Data Principal's request, rather it delegates this to be notified by Data Fiduciaries and Consent Managers instead. Frameworks in other jurisdictions such as Canada's Privacy Act[56] and the EU's GDPR[57] prescribe a period of 30 days for the Data Fiduciary to respond. Similarly, the Rules should codify the time period for response instead of delegating this further, to avoid potential delays in grievance redressal for the Data Principals.

2. **Format for requesting enforcement of rights:** The Rules do not provide a mechanism and format for requesting access to information made by the Data Principals. Jurisdictions like the Philippines publish formats for access, rectification and erasure request forms.[58] We recommend that the Rules should provide formats for such request forms to enable easier access of rights by Data Principals.

3. **Providing reasons for denial of a request to access information:** The Rules do not provide clarity on the process to be followed in case of denial of a request to access information. We recommend that the Rules include an obligation on Data Fiduciaries to provide reasons in writing when refusing such a request. This should be accompanied with details on how a Data Principal can subsequently file a complaint before the Board.

---

[56] Section 14, The Privacy Act, 1983, (Canada) <https://laws-lois.justice.gc.ca/PDF/P-21.pdf> accessed 3 March 2025.

[57] Article 12(3), General Data Protection Regulation (2016).

[58] National Privacy Commission, 'NPC Advisory 2021-01' (2021) <https://privacy.gov.ph/wp-content/uploads/2021/02/NPC-Advisory-2021-01-FINAL.pdf> accessed 28 February 2025.

4. **Operationalising right to correction and erasure of personal data:** Section 12 of the DPDP Act provides Data Principals with the right to correct and erase personal data, but the Rules do not give effect to these rights. The Rules should include detailed guidelines to operationalise the right to erasure or delisting. The European Data Protection Board's guidelines on delisting[59] provide grounds for a delisting request and exceptions to the right to erasure. The Rules are a missed opportunity to codify the law of erasure in India which has been evolving in the Indian Judicial system for the last few years.[60]

5. **Additional transparency requirements for Data Fiduciaries:** We recommend adding additional transparency mechanisms to Rule 13, which mandate Data Fiduciaries to publish periodic transparency reports containing details of the number of requests and their outcomes in the form of reasoned responses of the Data Fiduciaries. These should include all requests for access, erasure, correction or nomination filed by Data Principals. Providing nuanced data under each category of requests will also help stakeholders and the Board assess compliance of Data Fiduciaries with the Act.

[59] European Data Protection Board, 'Guidelines on the Right to Be Forgotten in the Search Engines Following the Google Spain Judgment' (2019) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf> accessed 28 February 2025.

[60] Srija Naskar, Sukriti, and Nidhi Singh, 'Right to Erasure', Centre for Communication Governance at National Law University Delhi (2024), p 13 <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-right-to-erasure-710.pdf> accessed 28 February 2025.

RULE 15: EXEMPTION FROM ACT FOR RESEARCH, ARCHIVING OR STATISTICAL PURPOSE

Rule 15 is meant to operationalise Section 17(2)(b) of the DPDP Act. This section provides exemptions from the provisions of the Act where processing of personal data is required for research, archival, and statistical purposes. While the Second Schedule of the Rules provides important safeguards for individuals or entities claiming this exemption, the scope of the provision raises several significant concerns.

1. **Ambiguity due to lack of clear definitions:** The scope of the Rules is ambiguous due to the lack of clear definitions for "research," "archiving," and "statistical purposes". Defining these terms in the the definitions clause of the Act would ensure a clear scope of the application of these terms enabling legislative clarity and preventing an expansion in the scope of the provision.

2. **Absence of journalistic exemptions:** Another oversight under the Act and Rules is the continued absence of exemptions for journalistic activities.[61] We recommend bringing journalistic research within the scope of the term “research” used in Rule 15 and Section 17(2)(b) of the DPDP Act.

3. **Strengthening safeguards:** The Second Schedule provides an important list of safeguards and standards for processing of personal data by individuals and entities claiming exemption under Rule 15. These include requirements of lawfulness, purpose limitation and storage limitation that must be followed by the State or its instrumentalities while processing any data. While the Schedule has introduced some guardrails, it does not fully engage with constitutional safeguards which must be adhered to while limiting the right to privacy. The introduction of “lawfulness test” is a positive step in this direction, however additional safeguards for “necessity” and “proportionality”

[61] Shashank Mohan, ‘New data law, a barrier to journalistic free speech’ *The Hindu* (16 April 2024) <https://www.thehindu.com/opinion/op-ed/new-data-law-a-barrier-to-journalistic-free-speech/article68068923.ece> accessed 27 February 2025.

must also be added in accordance with the Supreme Court's mandate in the *Puttaswamy* case.[62]

4. **Intimating Data Principals when their data is processed for research, archival, and statistical purposes:** Clause (g) of the Second Schedule mandates providing an "intimation" to the Data Principals, when their data is being processed under Section 7(b) of the DPDP Act, for provision of benefits by the State. However, it does not extend to the data which is collected under Section 17(2)(b) of the Act for research, statistical and archival purposes. We recommend that this provision in the Second Schedule be expanded in scope to cover both sections to provide holistic safeguards for Data Principals.

5. **Defining "intimation" under the Second Schedule:** Finally, the term "intimation" is not defined in the DPDP Act or the Rules, which may lead to ambiguity in the enforcement of this intention. While the Second Schedule does provide some guidelines about what should be contained within such an intimation, it is very narrow in scope and does not contain essential information such as the purpose for data processing. Consequently, the intimation to be given under the Second Schedule should be expanded to include the purpose of processing as well.

[62] *Justice K.S. Puttaswamy vs. Union of India* AIR 2017 SC 4161, <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors> accessed 27 February 2025.

RULE 16: APPOINTMENT OF CHAIRPERSON AND OTHER MEMBERS

Rule 16 lays down the procedure for selection of the Chairperson and other members of the Data Protection Board of India, pursuant to Section 19 of the DPDP Act. The Rule clarifies the composition of the search-cum-selection body which will be composed of members of the executive and two expert members to be appointed by the Central Government.

The powers of the Board include administrative as well as quasi-judicial functions, therefore, it is recommended that the search-cum-selection body should also include a judicial representative to ensure fair and balanced decision making. Having a balance of executive, independent experts, and judicial members in the search-cum-selection body will also improve the independence of the Board itself. This will act as a necessary check-and-balance system, improving the overall functioning of the Board.

RULE 18: PROCEDURE FOR MEETINGS OF BOARD AND AUTHENTICATION OF ITS ORDERS, DIRECTIONS AND INSTRUMENTS

Rule 18 lays down the procedure for the meetings of the Board. The procedures laid down under Rule 18 take a crucial first step towards providing operational clarity for many of the provisions listed under chapters V and VI of the DPDP Act. While the Rules provide some guidance, they do not lay down proper guidelines for the disposition of inquiries.

Rule 18(9) establishes basic timelines (six months, extendable by three months at a time) for the completion of an inquiry, but it does not lay down any specific procedures for the investigation itself. This could lead to ambiguity in the implementation of the process. It is important for the Rules to lay down a comprehensive procedure to deal with an "inquiry" under Section 28 of the DPDP Act, in order to give effect to the rights of Data Principals. For instance, Section 14 of the Protection of Human Rights Act, 1993 and National Human Rights Commission (Procedure) Regulations, 1994 lay down the procedure to be followed by the National Human Rights Commission on receipt of a complaint.

We recommend that the Rules should direct the Board to lay down the process for filing a complaint and the procedure to be followed thereafter. To ensure understanding and accessibility this should be published prominently in plain and clear language on their website. It should also lay down the steps that must be followed to conduct an inquiry and a mechanism which allows the Data Principal to follow the progress of the inquiry.

RULE 19: FUNCTIONING OF THE BOARD AS A DIGITAL OFFICE

Rule 19 echoes Sections 28(1) of the DPDP Act and talks about the Board functioning as a "digital office". However, the Rules lack any substantial guidelines on how this would be implemented. We welcome the introduction of a digital office; however, a fully online design raises certain concerns.

1. **Concerns around accessibility of digital office:** Accessibility to the internet and digital literacy rates vary throughout the country, with people having differing levels of internet access. Moreover, there is uncertainty about the implementation of this design since no adjudicatory body of such a wide scale and scope has yet been completely digital in design and functioning in the country. A completely digital model may end up catering to predominantly urban populations with high levels of digital literacy, ignoring the challenges faced by people in remote areas with low levels of digital literacy.[63]

2. **Hybrid mode of functioning:** For these reasons, the Rules should include a delayed hybrid model that initially focuses on setting up the physical presence of the Board and then builds its digital presence. The Rules can lay down a gradual transition from a more traditional physical model to a digital model to ensure that the Board has enough time to scale up. As the Board is expected to handle a large volume of complaints, the Rules should focus on building internal capacity to deal with a large number of cases while developing administrative and adjudicatory mechanisms for gradual digital adoption.

[63] For a more detailed discussion on the challenges of a fully digital model, and how they can be mitigated by a more decentralised and gradual approach, please refer to 'RECONFIGURING DATA GOVERNANCE: Insights from India and the EU', (Tilburg Institute for Law, Technology and Society (Netherlands), the Centre for Communication Governance at the National Law University Delhi, and the Centre for Internet & Society), p 28 <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/reconfiguring-data-governance-final-525.pdf> accessed 26 March 2025.

3. **Decentralised approach catering to remote populations:** Recognising the disparity in the level and quality of internet access across the country, the Rules must lay down procedures to allow for alternative mechanisms to access the Board. This could include setting up regional physical presence as well as mechanisms to file complaints through letters or at physical locations.

RULE 22: CALLING FOR INFORMATION FROM DATA FIDUCIARY OR INTERMEDIARY

Rule 22 creates a wide ambit for the State to call for information from Data Fiduciaries and intermediaries without appropriate checks and balances. The Seventh Schedule specifies the purpose for which this power may be exercised. The first entry allows the State or its instrumentalities to act in the interest of sovereignty and integrity of India or security of the State. While maintaining the security of the State is an important function this must be balanced with the fundamental rights of citizens. The wide powers of the State to carry out its sovereign functions must be accompanied by constitutional safeguards.

1. Absence of Procedural Safeguards: The State has expansive powers under Section 69 of the Information Technology Act, 2000 (IT Act) to monitor, intercept or decrypt any digital information that is necessary to protect India's sovereignty, security, and public order. Section 69(1) of the IT Act specifies that any order under this section must be made for reasons recorded in writing. The IT Rules, 2009 further clarify who is authorised to make such orders. Further, interception orders made under Section 5 of the Telegraph Act or Section 69 of the IT Act must be reviewed by a Review Committee composed of senior government officials constituted under 419A of the Telegraph Rules. These provisions have been criticised for providing expansive powers to the executive accompanied by insufficient procedural safeguards. Rule 22 and the Seventh Schedule effectively override these provisions, allowing for authorities to call for information without even the minimal constitutional and legal safeguards applicable under the IT Act.[64] We recommend that the first entry in the Seventh Schedule should be made subject

[64] The constitutionality of Section 69 of the IT Act has also been challenged before the Supreme Court for being violative of the right to privacy (M L Sharma v Union of India WP (Criminal) 1 of 2019). For more on this, see the discussion on Section 69 of the IT Act in 'The surveillance law landscape in India and the impact of Puttaswamy', CCG, Pg 44 <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-surveillance-law-landscape-in-india-and-the-impact-of-puttaswamy-476.pdf> accessed 05 March 2025.

to at least the procedural safeguards incorporated under Section 69 of the IT Act.[65]

2. **Excessive powers given to public officials:** The second entry in the Seventh Schedule empowers the State or its instrumentalities to call for information in performance of any function or obligation under any law, without specifying which authority may exercise this power. Instead, it extends this power to be exercised by any person authorised under an applicable law. This is the broadest possible framing of the purpose for which the power to call for information may be utilised, making it susceptible to abuse. For instance, an officer carrying out address verification could use this provision to track an individual's cell tower location in the name of verifying their physical location. We recommend that the power given under the second entry should be limited to specific purposes which must be outlined in the DPDP Rules.[66]

3. **Assessment of SDFs:** The third entry allows the State to call for information to carry out an assessment for notifying any Data Fiduciary as a Significant Data Fiduciary. We recommend that the provision should specify the authority that will carry out such assessment and clarify that the data collected for this purpose shall not be used for any other reason

[65] In *PUCL vs. Union of India* [(1997) 1 SCC 301], when looking at the constitutionality of interception powers under the Telegraph Act, the Supreme Court stressed on the necessity of laying down procedural safeguards to satisfy the standard of 'just, fair and reasonable' under Article 21. See also <https://privacylibrary.ccgnlud.org/case/pucl-vs-union-of-india?searchuniqueid=207618> accessed 27 February 2025.

[66] The Srikrishna Committee Report also discussed at length the need for balancing data protection and privacy requirements with the necessity of ensuring State security. It had recommended that in order to protect against abuse of the power by State authorities, the power to intercept and call for information must be limited to the purpose of protecting the sovereignty and integrity of India or security of the State.

Centre for Communication Governance

National Law University Delhi

Sector 14, Dwarka

New Delhi – 110078

011- 28031265

ccgdelhi.org

privacylibrary.ccgnlud.org

twitter.com/CCGNLUD

ccg@nludelhi.ac.in