Submission on the draft Digital Personal Data Protection Rules, 2025

We thank the Ministry of Electronics and Information Technology (MeitY) for the opportunity to give feedback on the draft Digital Personal Data Protection Rules, 2025 (the Rules) to be made under the Digital Personal Data Protection Act, 2023 (the Act).

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence and expertise based in over 20 countries across six continents, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.

Access Now engages with a global community of individuals from over 162 countries in our annual RightsCon summit series, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We have special consultative status at the United Nations.[1]

In India and globally, Access Now has consistently engaged with stakeholders including governments and regulatory authorities on matters pertaining to digital rights,[2] including data protection,[3] content governance,[4] cybersecurity, internet shutdowns,[5] surveillance and digital security.

Rule-wise comments and recommendations

1) Rule 3: Notice

   We welcome the specific items mentioned in Rule 3 which need to be provided in a notice to the Data Principals and the emphasis on clarity. Rule 3 must be enforced as soon as possible without delay as it does not place an undue burden on the Data Fiduciaries, who are already aware of data they are collecting and how they are using such data. This Rule is central to the Act as it gives Data Principals essential information about how their personal data is being used. Without a notice, the Data Principal is unable to exercise any rights over their data.

---

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, *No liberty, no safety: Sri Lanka must withdraw the Online Safety Bill*, https://www.accessnow.org/press-release/sri-lanka-must-withdraw-the-online-safety-bill/.
[3] Access Now, *Joint submission on the Bangladesh Draft Data Protection Act 2023,* https://www.accessnow.org/wp-content/uploads/2023/10/Submission-on-the-Bangladesh-Data-Protection-Act-2023-Access-Now-and-Tech-Global-Institute.pdf.
[4] Access Now, *Submission on the draft Broadcasting Services (Regulation) Bill, 2023,* https://www.accessnow.org/wp-content/uploads/2024/01/Access-Now-Submission_Broadcasting-Services-Bill_January-2024.pdf.
[5] Access Now, *Shrinking democracy, growing violence: Internet shutdowns in 2023*, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf.

We recommend that Rule 3 and the obligation to provide a detailed notice to Data Principals be enforced immediately without delay.

2) Rule 4: Consent Managers

We recommend clarifying the operational framework of consent managers to explain whether, and what circumstances, it is mandatory for Data Fiduciaries to work with consent managers; how the flow of consent, and the burden of proof in respect of having obtained valid consent, would work in the interaction between the Data Principal, the Data Fiduciary and the consent manager; how Data Principals can obtain redress when engaging with a Data Fiduciary as well as a consent manager. Further consultations should be held to detail the extent of information that would be shared with consent managers and the baseline of strong security measures for how such managers must safeguard the data to ensure that they do not become a centralised database of personal information vulnerable to attacks and breaches. The measures taken in this regard should be made clearly and transparently available to Data Principals, and individuals must have the choice to decide not to engage with a particular consent manager. In all cases, there must be clear procedures for redressal with actionable rights for affected parties.

We recommend further consultation on the role and responsibilities of consent managers with participation from the general public to ensure a rights-respecting framework for management of consent.

3) Rule 5 and the Second Schedule

Some of the standards in the Schedule need to be clarified for meaningful implementation.

We recommend that standard (a) in the Second Schedule be clarified to specify that processing must be carried out in a "lawful, fair, and reasonable manner".

Standard (b) is not needed as the rule derives from Section 7(b) and Section 17(2)(b) of the Act and processing must first be in conformity with those sections in order to attract the standards in the Second Schedule.

We recommend that standard (b) in the Second Schedule be omitted for clarity.

We welcome the inclusion of a necessity standard in (c) which promotes the principle of data minimisation and purpose limitation. For clarity and to ensure that the standard is followed, it can be modified slightly.

We recommend that standard (c) in the Second Schedule be clarified to state that processing should be limited to such personal data as is "strictly necessary" for the uses or purposes in Section 7(b) or Section 17(2)(b).

We welcome the inclusion of an obligation to ensure accuracy in standard (d).

We recommend that standard (d) in the Second Schedule be retained.

We welcome the time-limitation on retention of personal data in standard (e). However, we note that this standard conflicts with Section 17(4) of the Act which exempts the State and its instrumentalities from the obligation to erase personal data once it no longer serves the purpose for which it was collected and processed.

We recommend that standard (e) in the Second Schedule be retained and Section 17(4) of the Act be removed, and that it be clarified that the State and its instrumentalities are not exempt from the erasure requirement when they process data under Section 7(b) of the Act.

We welcome the requirement that reasonable security safeguards must be implemented by the State and its instrumentalities as this is essential for keeping personal data protected against unauthorised access. However, the rule needs to be clear as to what safeguards must be implemented in order to ensure compliance. Without clarity, different instrumentalities and entities may follow different and inadequate standards, leading to an overall weakening of data protection.

We recommend that standard (f) in the Second Schedule be clarified to state that the reasonable security safeguards under Rule 6 must be implemented for processing under Section 7(b) and Section 17(2)(b) of the Act.

We welcome the requirement that processing by the State or any of its instrumentalities under Section 7(b) will require intimation to the Data Principal that such processing is occurring; provision of a contact to answer the Data Principal's questions about the processing; and intimation of the means by which the Data Principal may exercise their rights. These are essential for transparency in processing personal data and for accountability of the State.

However, condition (iv) in paragraph (g) of meeting "such other standards" as may be applicable to personal data processing does not clarify whether this includes the reasonable security standards prescribed in Rule 6. The rules have an opportunity to explain which standards, exactly, will be applicable to the personal data processed by the State under Section 7(b). Without specifying which standards are applicable, it is impossible for either the Data Protection Board of India or any affected Data Principal to measure and assess whether there has been a breach of the standards.

We recommend that standard (g) in the Second Schedule be clarified to state the policies or laws which should be followed for processing by the State or its instrumentalities under Section 7(b) and that the standards include the reasonable security safeguards prescribed in Rule 6.

We welcome the inclusion of an accountability standard in (h) recognising that the official(s) in charge of the personal data processing should be answerable. However, the absence of any clear mechanism for holding such officials answerable could lead to this remaining on paper.

We recommend that the person(s) who determine the purpose and means of processing of personal data under Section 7(b) be required to submit quarterly reports of the number of persons whose personal data has been processed, the purposes of such processing, the intimations provided under standard (g), the number and details of requests by Data Principals have sought to exercise their rights through the link under standard g(ii) and the status of such requests; and the compliance with other standards under standard g(iii). This report should be submitted to the Board and published by the relevant State instrumentality.

4) Rule 6: Reasonable Security Safeguards to be followed by Data Fiduciaries under Section 8(5) of the Act

We welcome the obligation on all Data Fiduciaries to maintain the seven minimum reasonable security safeguards listed in rule 6(1). This provision is at the core of data protection and cybersecurity, and requires immediate implementation. These measures are the key to preventing data breaches, whether through access for illegal means by a person having control of the computer system where the personal data is stored, or through unauthorised access by a third-party through a compromise of the security system. Adoption of measures like encryption mentioned in the rules are important positive steps towards protecting personal data.

Studies indicate that more than a majority of companies in India follow unsafe data practices.[6] This is borne out by the occurrence of data breaches at major companies with serious consequences for privacy and economic losses. For example, a data breach at Star Health Insurance leading to the personal data including PAN, date of birth, and medical records of 31 million people being put up for sale online.[7] The average cost of a data breach in India in 2024 was estimated to be INR 19,50,00,000 (19.5 crores).[8] These facts demonstrate the urgent need for all Data Fiduciaries to undertake minimum security safeguards at the earliest. Many of the measures listed in Rule 6(1) are in sync with national and international norms for cybersecurity and data protection, and are already followed by many Data Fiduciaries. In this context, there is no justification for private companies to

[6] Business Standard, *Over 60% companies in India follow problematic data practices: Study*, https://www.business-standard.com/industry/news/over-60-companies-in-india-follow-problematic-data-practices-study-124083001307_1.html.
[7] India Today, *Star Health insurance hack led to personal data of 31 million customers being compromised*, https://www.indiatoday.in/technology/features/story/star-health-insurance-hack-led-to-personal-data-of-31-million-customers-being-compromised-story-in-5-points-2615354-2024-10-11.
[8] IBM, *IBM Report: Escalating Data Breach Disruption Pushes Average Cost of a Data Breach in India to All-Time High of INR 195 Million in 2024*, https://in.newsroom.ibm.com/2024-07-31-IBM-Report-Escalating-Data-Breach-Disruption-Pushes-Average-Cost-of-a-Data-Breach-in-India-to-All-Time-High-of-INR-195-Million-in-2024.

seek an additional 18-24 months to comply with the data protection regime.[9] Permitting such an extended period for compliance will result in further breach of people's personal data and more incidents of cybercrime and economic loss which must be prevented at the earliest.

We recommend that Rule 6 be enforced as soon as possible and in any case before the 18-24 month timeline sought by some private sector stakeholders.

5) Rule 7: Form and manner of intimation in case of a data breach under Rule 8(6) of the Act

We welcome the clarity in Rule 7(1) as to the information which must be provided to each affected Data Principal in case of a personal data breach. The inclusion of information including the nature of the breach, the consequences which could occur to the Data Principal, the steps being taken by the Fiduciary to mitigate risk, and the steps that a Data Principal may take as well as provision of contact information for further inquiry are all key to creating an accountable and person-centric data protection regime. The requirement that Data Fiduciaries provide this information in a "concise, clear and plain manner and without delay" is also welcome as it will help to ensure that Data Principals understand and can act on the intimation.

However, there is a discrepancy between the open-ended timeline of "without delay" in Rule 7(1)(a) and the time limit in Rule 7(2)(b), which provides the Data Fiduciary with seventy-two hours to update the Data Protection Board of similar information. If the "without delay" requirement is read to mean a timeline shorter than 72 hours, it is possible that Data Principals may receive incomplete or unhelpful information. In order to harmonise the rules and give Data Principals relevant information without overwhelming them with multiple notifications, the same timeline can apply to intimations to the Principals as well as to the Board.

We recommend that the intimation to Data Principals under Rule 7(1)(a) be made without delay, and in any case within 72 hours of becoming aware of the breach.

6) Rule 8: Erasure of personal data

The limitation on retaining personal data is an important protection in Section 8(7) of the Act, reflecting the principle of purpose limitation and the principle of data minimisation. Mandatory erasure is key to comprehensive data protection, preventing the unnecessary storage of large volumes of personal data which can be breached and misused. Section 8(7) of the Act requires that all Data Fiduciaries must erase personal data not only when consent is withdrawn but also when it may be reasonably assumed that the specified purpose is no longer being served. This latter requirement is an enforcement of the principle that data processing should be fair and reasonable: even if the Data Principal does not herself withdraw consent, the Data Fiduciary must not continue to process her personal data when unnecessary for the Principal.

[9] Business Standard, *DPDP Act: Social media, telcos, startups lobby for 18-24 months to comply*, https://www.business-standard.com/industry/news/social-media-telcos-lobby-for-18-24-months-to-comply-with-dpdp-act-123100100635_1.html.

We welcome the specification in the rules to help determine when it may be reasonably assumed that the purpose is no longer being served. However, the rule appears to significantly limit section 8(7) and the principle of minimisation only to three limited categories of Data Fiduciaries listed in the Third Schedule: e-commerce entities, online gaming intermediaries, and social media intermediaries, with further conditions for application based on the volume of registered users of these intermediaries.

Section 8(7) and Section 8(8) do not limit the application of the data erasure requirement. Harms from indefinite data retention are not limited to these three types of Data Fiduciaries. Vast amounts of personal data are collected by all types of Data Fiduciaries — for example, researchers found that even a flashlight application was collecting location data from users.[10]

Rule 8, in its present form, is imposing a limitation beyond the legislative intent in Section 8(8) which states that "... different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes."

We recommend that Rule 8(1) be modified to remove the words "who is of such class and is processing personal data for such corresponding purposes as are specified in Third Schedule" or, in the alternative, that an entry number 4 be added to the Third Schedule to impose a time limit applicable to residual Data Fiduciaries beyond which they must follow the obligation to erase personal data under Section 8(7) and 8(8).

7) Rule 12(1) and 12(2): Data Protection Impact Assessments and audits

We welcome the requirement in Rule 12(1) that the Data Protection Impact Assessments (DPIAs) and audits required under Section 10(2)(c) of the Act by Significant Data Fiduciaries (SDFs) must be an annual exercise, and further the requirement in Rule 12(2) that "significant observations" from the DPIA and audit must be furnished to the Board. However, increased scrutiny is required to ensure that SDFs are complying with their obligations and that the Board is exercising its powers appropriately in case of non-compliance.

We recommend that SDFs be required to publish and give the Data Protection Board of India full copies of the annual reports of Data Protection Impact Assessments (DPIAs) and audits required under Section 10(2)(c) of the Act so that Data Principals, experts, and other stakeholders can also scrutinise their compliance with the Act and Rules.

8) Rule 12(3): Algorithmic software and risks to Data Principals' rights

We welcome, in principle, the measure in Rule 12(3) which addresses the potential risk to Data Principals' rights by the use of algorithmic software. However, the rule needs clarifications to determine how and when it will apply to meaningfully protect Data Principals' rights.

[10] NBC News, *A shock in the dark: Flashlight app tracks your location*, https://www.nbcnews.com/technolog/shock-dark-flashlight-app-tracks-your-location-1b7991120.

i. The term “algorithmic software” is not defined in the Act and requires specification. For example, “automated decision-making” should be explicitly included in the scope of Rule 12 as an activity which can adversely affect Data Principals’ rights, as recognised under other data protection frameworks including the European Union’s General Data Protection Regulation.

ii. It is not clear whether the risk to Data Principals’ rights must be calculated based on the mere deployment of the software or the overall processes being employed by the SDF.

(iii) The rule should include accountability mechanisms by which the Board or Data Principals can verify and evaluate the due diligence measures taken by SDFs. The rules should clearly outline if this is part of the DPIA or audit under Section 10(2)(c).

(iv) The rule does not clearly prohibit SDFs from using algorithmic software which poses a risk to Data Principals’ rights. This should be clear from the rules, in order to prevent risk rather than take a post-facto fine or penalty approach.

We recommend that Rule 12(3) include clarity on how risks are to be measured, a prohibition on the use of algorithmic software which poses a risk to the rights of Data Principals, and specific mechanisms for accountability and verification of measures taken.

9) Rule 12(4): Data localisation

Under the guise of imposing obligations on SDFs to protect data, Rule 12(4) creates a new power for the Central Government to require, entirely at its discretion, that personal data and traffic data relating to the flow of such personal data is kept within the territory of India.

Data localisation is not a prerequisite for comprehensive and privacy-respecting data protection. The data protection rights of Indian residents must apply no matter where their data may flow, and entities must accordingly be subject to legal requirements. Section 16(1) of the Act already provides that the Central Government may restrict the flow of personal data to “such country or territory outside India” by notification. There is no need for Rule 12(4) which does not derive from Section 16. Section 16(2) also clearly protects the data localisation mandates under any other law in force, accounting for sector-specific protections such as the RBI’s regulations on payment systems data,[11] IRDAI regulations on maintenance of policy and claims records,[12] and SEBI’s guidelines for cloud adoption.[13]

Broadness of the provision and lack of clear categorisation of SDFs will lead to abuse of localisation mandate: Neither the Act or the Rules is clear as to who may be classified

[11] Reserve Bank of India, *Storage of Payment System Data*, Circular DPSS.CO.OD.No 2785/06.08.005/2017-18, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.
[12] Insurance Regulatory and Development Authority of India, *IRDAI (Maintenance of Insurance Records) Regulations, 2015*, https://irdai.gov.in/document-detail?documentId=604674.
[13] Securities and Exchange Board of India, *Framework for Adoption of Cloud Services by SEBI Regulated Entities, 2023*,https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html.

as an SDF or the factors to be considered for classification. The factors listed in Section 10(1) are broad and inexhaustive.

Since the power to classify a Data Fiduciary as an SDF is extremely broad, the conditions imposed on SDFs must be measured and proportionate to the purpose sought to be achieved. The purpose of protecting personal data by not transferring it to certain countries or territories can already be achieved under Section 16.

Rule 12(4) does not clarify how this power will be exercised, specifically:

(a) The types of personal data and related traffic data which must be kept within India;
(b) Any reference to an objective sought to be achieved or the factors on the basis of which the Central Government will specify types of personal data and related traffic data must be kept within India;
(c) The composition of the committee, introduced here for the first time, which will recommend the personal data and related traffic data which must be kept within India; and
(d) Whether this condition will apply to all SDFs, regardless of the reason why they have been notified as an SDF and the relevance of this personal data to the services they provide.

The risks of rules with an undefined scope of application (Section 10) combined with mandatory localisation requirements is that an excessive amount of personal data (including traffic data) becomes easy for the State, including its investigating agencies, and private actors with malicious motives to access. In the absence of independent oversight of surveillance powers, transparency of surveillance orders, and accountability for misuse of such powers, the proposed personal data localisation mandate in Rule 12(4) will infringe rather than protect people's personal data. Since sector-specific and country-specific localisation mandates are already permitted, a residual discretionary power to demand data localisation does not serve any privacy purpose.

The provision could lead to the fragmentation of the internet: Personal data localisation hurts people's connection to the rest of the world, affecting the range of services they can access.

We recommend that Rule 12(4) be omitted.

10) Rule 13: Rights of Data Principals

In order for the rights articulated in the Act to be meaningfully enjoyed and exercised, it is essential that the mechanism for exercising rights is accessible as widely as possible. Rule 13 should include more specific measures to ensure that Data Principals are able to exercise their rights easily and without having to undertake excessive steps.

(i) The means by which Data Principals can exercise their rights under the Act should be available and information about the means (as described in Rule 13(1)(a) and (b)) should be published on all platforms through which the Data Fiduciary or Consent Manager

provides services. To illustrate, the Data Fiduciary or Consent Manager must not restrict requests to be made through an app if it also provides goods or services through a website.

We recommend that Rule 13(1) clearly state that the means of making a request for the exercise of rights under the Act be available on all platforms through which the Data Fiduciary or Consent Manager provides goods or services.

(ii) Section 13(2) of the Act provides that the Data Fiduciary or Consent Manager must respond to grievances within a period which may be prescribed, but Rule 13(3) fails to prescribe such a period or even lay down conditions for the time period which should be adopted. The period adopted is relevant since in case there is no response or inadequate response from the Data Fiduciary or Consent Manager, the Data Principal has the right to approach the Board. There must be a clear and reasonably short deadline for response.

We recommend that Rule 13(3) indicate a clear and reasonably short deadline for a response to the grievances of Data Principals.

11) Data localisation: Rule 14

Rule 14 appears to be a blanket power to the Central Government to issue a general or special order with requirements to be met by a Data Fiduciary with respect to making personal data available to a foreign State, a person or entity "under the control of" a foreign State, or an agency of a foreign State. Rule 14 does not derive from Section 16 or any other provision in the Act, and is dangerously overbroad in its scope.

We recommend that Rule 14 be omitted.

12) Rule 16(1) and 16(2): Composition of the search-cum-selection committees

Rule 16(1) and Rule 16(2) set up search and selection committees to appoint the chairperson and members of the Data Protection Board of India. Both committees include two experts "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*" which gives the Central Government excessive discretion to determine the fields and is inconsistent with the Act itself.

The two expert members of the search and selection committees should have expertise in the areas already identified in the Act as relevant to the purposes of the Act. Section 19(3) of the Act provides that members of the Board should have special knowledge or practical experience in the following fields.

- Data governance
- Administration or implementation of laws related to social or consumer protection
- Dispute resolution
- Information and communication technology
- Digital economy
- Law (at least one member must be an expert in law)

- Regulation or techno-regulation
- Any other field which in the opinion of the Central Government may be useful to the Board

It is therefore neither necessary nor appropriate for Rule 16(1) and 16(2) to use only the broad language of "the opinion of the Central Government" as seven other specific areas in which Board members should have expertise are already clearly identified in the Act.

We recommend that Rule 16(1) and Rule 16(2) be amended to replace "which in the opinion of the Central Government may be useful to the Board as members" with "listed in Section 19(3) of the Act".

13) Rule 16: Composition of the search-cum-selection committees and appointment of the Board.

The Data Protection Board of India has a statutory duty to function "as an independent body" under Section 28(1) of the Act. The Board is the central body which will be empowered with enforcing and upholding the Act. It will function as the primary adjudicatory body hearing complaints in the first instance. Independence is crucial for the Board to be able to apply the law impartially. The state as a major Data Fiduciary must be subject to enforcement processes under the Act for meaningful and universal data protection, as is the case in other jurisdictions. For example, the General Court of the European Union recently fined the European Commission for transferring personal data in violation of the General Data Protection Regulation (GDPR).[14]

The manner of appointment of the Board can help to ensure its independence from the state, but Rules 16(1), (2), and (3) provide a procedure by which the Board's appointment is effectively controlled by the Central Government. As an adjudicatory body, it is crucial for the Board to be composed of persons who are chosen through a transparent and reliably independent process.

We recommend that both the search-cum-selection committees under Rule 16(1) and Rule 16(2) also include at least one additional independent member.

The appointment of the Board should also be done as per the recommendation of the committees rather than by the Central Government. Rule 16(3) provides the Central Government additional discretion to appoint the Board "after considering the suitability of individuals" recommended by the committees. Given that the committees consist of high-ranking members of the state and experts in the fields relevant for data protection, their recommendations should be implemented without interference. The Central Government may instead retain a conditional, limited power to request the committees to reconsider any candidate, for specific reasons of unsuitability, with transparency mechanisms in place.

[14] The General Court, *Judgment in Case T-354/22 Thomas Bindl v. European Commission*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=294090&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=397223; Reuters, *In a first, EU Court fines EU for breaching own data protection law*, https://www.reuters.com/world/europe/first-eu-court-fines-eu-breaching-own-data-protection-law-2025-01-08/.

We recommend that Rule 16(3) be amended to read: "The Central Government shall, on the public recommendation of the Search-cum-Selection Committee, appoint the Chairperson and other Members within a month of such recommendation having been made. The Central Government may, for reasons to be recorded in writing, request the Committee to reconsider any recommendation but the Committee's decision in this regard shall be binding on the Central Government."

14) Rule 21: Appeal only digitally

Rule 21(1) provides that appeals from an order of the Board must be filed in "digital form" to the Appellate Tribunal, which is the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). This restriction on filing appeals through physical mode is unjustified, as the TDSAT has a comprehensive existing procedure and rules for filing appeals and petitions which allows for physical as well as online filing.[15] There is no reason why the same manner of filing should not be applicable to all proceedings before the TDSAT and other appellate bodies. Limiting the manner in which appeals may be filed will unreasonably restrict access to justice and enforcement of data privacy rights.

We recommend that Rule 21 permit appeals to be filed in either digital or physical format to promote access to the appellate mechanism.

15) Rule 22: calling for information

Section 36 of the Act must be limited to calling for "information" and not personal data, for data protection and not for collecting information for any other purpose. S. 36 does not delegate any power to the Central Government to expand purposes for which information may be called or the conditions under which it may be collected. The section is self-limiting by referencing the purposes of the Act itself.

Rule 22 enlarges the scope of Section 36 significantly by making it applicable to "personal data" and not simply "information". Further, Rule 22 seeks to expand the purposes of the Act and prohibit the disclosure of the fact of exercise of power by the Central Government under the Section. The Seventh Schedule in the rules seeks to include as purposes under the Act personal data use by the State or any of its instrumentalities (i) "in the interest of sovereignty and integrity of India or security of the State"; (ii) for the performance of functions under law or for disclosure of information for fulfilling any legal obligation; and (iii) Assessment for notifying Significant Data Fiduciaries.

The processing of personal data by the State for carrying out its duties in the interests of India in accordance with the Constitution in (i) and (ii) cannot also be a *purpose* under the Act. This is both redundant and beyond the scope of a data protection regime to implement the fundamental right to privacy. Rule 22 and the Seventh Schedule seek to create an extremely broad data access regime for the State. This expansion of powers is

[15] https://tdsat.gov.in//admin/introduction/uploads/TDSAT%20Procedure2022.pdf.

incompatible with the basis of the Act and the fundamental right to privacy, and must be removed.

With respect to item (iii), the Central Government does not need access to the actual personal data being processed by a Data Fiduciary to notify SDFs. SDFs can be notified with respect to the class and volume of data they process without reference to the personal details thereof. Rule 22 and the Seventh Schedule are essentially creating a backdoor for the State to access people's personal data in the guise of classifying SDFs, which undermines rather than protects people's privacy and is not contemplated under the Act.

We recommend that Rule 22 and the Seventh Schedule be omitted as they are beyond the scope of the Act and are incompatible with the fundamental right to privacy and the principles and purpose of data protection.

We remain committed to continuing to engage with this important process to promote a rights-respecting data protection framework in India.

Yours sincerely,

Shruti Narayan
Asia Pacific Policy Counsel
shruti@accessnow.org

Namrata Maheshwari
Senior Policy Counsel and Encryption Policy Lead
namrata@accessnow.org

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org