# THE DIGITAL PERSONAL DATA PROTECTION ACT- AMBIGUITIES, LIMITATIONS AND RECOMMENDATIONS

## Wadhwani Centre for Government Digital Transformation (WGDT)

**Authors:**
**Nivedita Krishna**
**Dr. Arun Teja Polcumpally**
**Alok Gupta**

**December 2023**
A Policy Paper by Wadhwani Centre for Government Digital Transformation (WGDT)

# Acknowledgements

In the course of developing this policy paper, we have had the privilege of engaging in insightful consultations with a cadre of distinguished experts from various sectors. We extend our heartfelt gratitude to Mr. Prakash Kumar, Prof. Indranath Gupta, Prof. Krishna Deo Singh, Mr. Ketan Mukhija, Ms. Deepa Ojha, Mr. Rodney Ryder, Mr. S Chandrasekhar, Ms. Chitra Iyer, Ms. Nidhi Sudhan, Mr. Nikhil Naren, Mr. Shashank Mohan, Dr. Akanksha Natani, Mr. Siddharth Deb, Mr. Prashant Ranjan Verma, and Ms. Aparna Mehrotra. Their collective wisdom, diverse perspectives, and invaluable contributions have been pivotal in shaping the recommendations and insights presented in this policy paper on data protection and privacy. We express our sincere appreciation for their time, expertise, and commitment to advancing the discourse on this critical subject.

# Table of Contents

# 1. Overview

The Digital Personal Data Protection Act, 2023 ["**the Act**"] was passed by the Parliament in August 2023. It provides the guard rails for collecting and processing digital personal data which is either collected within India or processed outside India for offering goods and services in India. While the Act, formalized after extensive deliberations, multiple stakeholder meetings, committee reviews, and recommendations, establishes a comprehensive framework for personal data management, it requires the support of specific rules or operational guidelines. These are essential to ensure a clear and unambiguous interpretation and implementation of the Act.

This paper thoroughly examines select sections of the current Act to identify areas of concern and ambiguity, explores best practices from other jurisdictions that could provide solutions, and offers recommendations for resolving these ambiguities. The initial section addresses issues such as specifying the format for consent notices, defining 'reasonable security safeguards,' and elucidating what qualifies as 'sufficient grounds of enquiry' for investigations under the Act. These aspects could be effectively clarified through rules established under the Act or through guidelines issued by the Ministry.

The subsequent section highlights concerns that require more substantial measures, such as granting suo motu powers to the Data Protection Board and introducing a specific classification for sensitive personal information. Addressing these issues may necessitate amendments to the Act or rely on judicial interpretations for resolution.

# 2. Section 1

## 2.1 Format, Content and Simplicity of the Consent Notice

### 2.1.1 Position under the Act

The Act states that a person may process personal data of a Data Principal only with her consent, in accordance its provisions, and for a lawful purpose/legitimate uses.[1] Such consent shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.[2]

Section 6(3) states that the request for consent must be in "clear and plain language," and gives the data principal the option to access such a request in "English or any language specified in the Eighth Schedule to the Constitution." Further Section 5 of the Act provides that "every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal ....in such manner as may be prescribed".

Thus, the law drives the requirement of the notice seeking consent to be informed, such that an ordinary layperson can make sense of the notice. This approach is mainly taken to reduce the cognitive load on the data principal and to reduce consent fatigue. However, Section 7(a) also enables data fiduciaries to process data in respect of which the data principal has not expressly indicated lack of consent, thus bringing large amounts of personal data under an opt-out mechanism. Such a provision significantly weakens the assurance of express consent established in Section 6. Moreover, it represents a notable deviation from the standards of the GDPR, which mandates explicit consent for data processing.

Further, currently, there is no standard as to what would constitute "clear and plain language" or what could be a blueprint for a desirable consent framework. This may be notified under the rules (as per the rule-making powers reserved under Section 5(2) of the Act), and the following considerations must be accounted for in developing guidance for a robust and pragmatic consent framework:

[1] Section 4, Digital Personal Data Protection Act, 2023
[2] Section 6, Digital Personal Data Protection Act, 2023

1) **Ambiguity on Using Publicly Available Data:** Section 3(c) of the Act exempts the application of data protection to personal data that is made or caused to be made publicly available by the data principal themselves. This gives external data processers impunity in processing such data without consent. For instance, if a person decides to publish her personal information publicly on a social media website, this would enable other data processors including AI models, to scrape information to train their models.[3]

   Even though personal data is made public for a specific reason, there is no way an individual will ex-ante understand the associated risks. This individual unwittingly shares her personal details, and the companies may use this for completely different purposes. Further, there are number of instances where services are provided only if personal data is shared, making the consent necessary to access certain services. This also makes an individual provide personal data unwittingly. This defeats the purpose of the legislation as personal data may be published online by individuals for specific purposes, but could be used by companies for any other purpose, even those that might be unlawful. This concern is especially poignant as generative AI models are being trained on large troves of publicly available data without explicit consent. Hence, there is a need to define the extent to which such 'publicly available data' may be legally processed. In fact, Justice Kaul, while talking about the importance of having a robust data protection regime in Puttaswamy v Union of India, stated:

   **"***if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it."*[4]

2) **Digital Literacy and Consent Fatigue:** Though a data privacy law must lay the guardrails for consent mechanisms, these initiatives may come a tad too late to the average Indian digital citizen. Digital habits have long been formed. Mechanical, click to accept practices (to access digital services such as email, e-commerce, and government services) have set firmly, resulting in a predominantly data indifferent population. The digital divide in India has created stark disparities in the levels of awareness regarding digital safety among its citizens, particularly among first-generation internet users. While urban areas and younger generations may have relatively higher access to digital resources and information, rural and elderly

[3] https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023/
[4] (2017) 10 SCC 1

populations often struggle to keep pace with the rapidly evolving digital landscape.[5] This discrepancy is further exacerbated by the relative unfamiliarity with the idea of digital privacy. Therefore, when designing privacy consent mechanisms, it is crucial to take into consideration this diverse user base in India. These mechanisms should be user-friendly, language-diverse, and accessible to those with varying levels of digital literacy to ensure that individuals from all walks of life can make informed decisions about their online privacy.

3) **Digital Rights Awareness**: Furthermore, the success of the law hinges on the extent of citizens having their rights to data privacy enforced through the respective data protection officers appointed by the Data Fiduciaries. This means that the spirit of consent and privacy, though envisaged by the Act may not translate into implementation, without an accompanying robust initiative for building citizen awareness of their digital rights under the Act. In this context, specific rather than generic guidance on what constitutes "clear and plain language", and "effective consent" is essential for the effective implementation of the Act. This guidance is needed to ensure that a generic understanding of what constitutes a legally and ethically acceptable consent framework needs to be established.

4) **Electronic Consent is Quasi Consent**: Electronic consent may not fully meet the traditional standards of explicit or unequivocal agreement. Though data principals may care about their privacy, they might agree to data practices that undermine their privacy and expose them to risks. Data Principals may give consent *unwittingly*, meaning they fail to understand the privacy agreement by virtue of it being too long or too technical.[6] The design of consent interfaces, such as pop-ups or checkboxes, can also influence users' decisions. Some interfaces may use pre-selected checkboxes or employ subtle design elements that encourage users to quickly click through without carefully considering the terms. From a business perspective, it may not be the fiduciary's high priority to simplify the contents for a robust understanding by the principals or it might have been designed that way using dark patterns of consent. Hence, a guidance or illustration on "clear and plain language" will help shift consent from 'passive acquiescence'[7] to free and informed consent.

[5] https://iasp.ac.in/uploads/journal/5.%20Socio-Economic%20Determinants%20of%20Digital%20Divide%20in%20India-1669206597.pdf
[6] https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview
[7]https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1567&context=fac_schol

5) **Chain of data flows in Chinese Whispers:** The Act lays down that the personal data of a principal shall only be processed for 'lawful purposes'[8] and that the purpose for processing the data shall be conveyed to the principal in the notice.[9] In order to comply with the law, the purpose as defined by the data fiduciary maybe too broad that it may be used and shared for wide ranges of purposes beyond the principal's knowledge. For instance, a common purpose mentioned by companies, in their privacy policies is to "improve user experience." This is a sweeping definition, and data collected from a principal maybe transferred to an infinite number of third parties that may help the platform "improve its services." Such broad definitions of the purpose may have the tendencies to make the consent mechanism redundant.

6) **Timing of Consent is itself a Problem**: Consent is usually collected from the persons before they get to use and experience the platform. Thus, the persons are tied into various platforms unintentionally, thus undermining the voluntary nature of consent, as users may fear restrictions on access to services if they do not agree.

7) **Concerns on already collected data:** The Act does not have retrospective effect, implying that Data Fiduciaries must provide notice to such Data Principals whose consent was given before the commencement of Act, notifying the Data Principals' rights for withdrawing such consent and redressal of any grievance. Specifying a reasonable timeline for providing such notice to Data Principals is pre-eminent for the effective implementation of the Act.

### 2.1.2 Practices under other jurisdictions

The General Data Protection Regulation of the European Union ["**GDPR**"] mandates that the data controller[10] provide information relating to the processing of data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.[11] The Principle of Transparency, in the context of the GDPR, requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used.[12] Further, if the consent is given in the context of a written

[8] Section 4(1), Digital Personal Data Protection Act, 2023
[9] Section 5(1)(i), Digital Personal Data Protection Act, 2023
[10] Similar to 'data fiduciary' under the Indian Act
[11] Article 12, GDPR
[12] Recital 58, GDPR

declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.[13] This is to prevent the obscuration of the aspects related to consent.

### 2.1.3 Recommendations to Exercise Rule Making Powers on Consent Mechanisms

1) **Amendment to Section 5:** Expand the requirements under Section 5 to include conditions and accountabilities in data transfer with other fiduciaries, duration of retention, data that may be potentially processed by virtue of Section 7(a), etc. would empower data principals by having more information over the data that they are providing for processing.

2) **Propose Model Consent Notices and Notify state governments to publish model notices in official languages**: The government may propose model consent notices based on international best practices, which shall include some minimum defined parameters forming as an integral part of consent notices. Though these model notices may not be binding on the industry, they would establish a basic standard for consent notice, that can be emulated. State governments may publish model privacy notices in their official regional languages, for adoption in respective jurisdictions.

3) **Appoint Sectoral Nodal Agencies to oversee privacy**: Under the residuary power to make rules under Section 40 (2) (z) of the Act, the central government may identify nodal agencies in each sector (for example RBI for banking/finance, TRAI for telecom, National Health Authority for Health and so forth) and these agencies in consultation with the Nodal Department shall develop sector wise guidelines for formulation of model consent frameworks. This approach has been taken in the past too, for example, the Ministry for Corporate Affairs has provided a draft model Articles of Association (AoA) which serves as a guiding document for companies while drafting their own AoA.

4) **Make Notices more accessible:** Issue guidelines for platforms to make consent more accessible, by making in available in various languages, audio-visual formats to suit the needs of persons with disabilities and reading vulnerabilities, and employing ex-ante testing before the notice is rolled out.

[13] Article 7, GDPR

5) **Encourage industry research:** It is crucial to build the academic and industry narrative in the local context To develop privacy consent frameworks specific to the Indian user base that are cognizant of the linguistic diversities, cultural attitudes and wide spectrum of digital literacy level unique to the country. Government and academic funding for research needs to be made available to enable this body of work to be created, based on which the industry responses can take place.

## 2.2 Defining 'Reasonable Security Safeguards' to Govern Data Privacy

### 2.2.1 Position under the Act

Section 8(5) of the Act places an obligation on data fiduciaries to take *reasonable security safeguards* to prevent data breaches, but without defining what would constitute such safeguards. The failure to implement such practices can potentially attract a penalty of up to Rs. 250 crores. Considering that several companies are subject to an extensive data protection regime for the first time, there arises a need for the Government to bring out guidelines/ best practices that such companies may undertake to prevent breach. The power to make these guidelines has not been reserved under the Act, meaning that it remains unclear who would notify the reasonable security safeguards.

Currently, under the IS/ISO/IEC 27001 regulations are identified by the Indian Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as international standards. As such, Indian companies aren't obligated — but are highly advised — to implement these standards,[14] which can help meet the "reasonable security practices" under Indian jurisdiction. In June 2023, the CERT-IN issued guidelines on Information Security practices for government entities in-line with the Government of India's objective to ensure that digital citizens experience a safe and trusted internet.[15] However this constituting "guidance", specific Rules as to the nuances reasonable security safeguards is awaited.

[14] Rule 8(2), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[15] https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

### 2.2.2 Practices under other jurisdictions

Article 40 of the GDPR requires the member states, the European Data Protection Board and the European Commission to encourage sector specific bodies and associations to draw up codes of conduct to ensure the proper application of the Regulation. For instance, Healthcare Employees Association in Poland,[16] Cloud Services Providers in EU[17] etc., have come up with their own codes of conduct. These codes of conduct often recommend that each organization establish security practices compliant with international standards such as ISO 27001/ 27002 etc. The codes of conduct also lay down detailed security objectives that each data fiduciary shall achieve, such as human resources security, encryption etc.

### 2.2.3 Recommendations on Security Safeguards

1) **Appoint Sectoral Nodal Authorities to draw up codes of conduct**: The Government may under the residuary power to make rules under Section 40 (2) (z) of the Act appoint a Nodal Authority in each sector which shall be in charge of laying out codes of conduct for the relevant industry which may be interoperable but cater to sectoral requirements, keeping in tandem with changing realities. The nodal authority shall also oversee data protection related codes of conduct and security standards for that sector, with due regarding to preventing/minimizing entry barriers for industry newcomers. This shall help in pushing industry to voluntarily adopt good data practices as generally compliance with data protection mandates is expensive[18] which delays adoption by the industry. For example, the RBI has devised its own standards of cyber security for banks,[19] which requires banks to undertake certain measures such as undertaking a cyber crisis management plan, setting up security operations centers etc. Such nodal authorities must be pushed to design codes of conduct and safeguards that incorporate privacy by design rather than as an afterthought. Requiring significant data fiduciaries to have higher standards for safeguards will also enable them to comply with their obligations under the Act better.

[16] https://www.dataguidance.com/news/poland-uodo-approves-first-code-conduct-under-gdpr
[17] https://eucoc.cloud/fileadmin/cloud-coc/files/former-versions/European_Cloud_Code_of_Conduct_2.10.pdf
[18] https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf
[19] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

2) **Mandate Nodal Authorities to oversee data protection audits:** Government has proposed Data Protection & Data Security Audit in IndiaAI 2023 document [20] which may be required to be conducted by all data fiduciaries on an annual basis. On similar lines, the sectoral nodal agency may be mandated to ensure that audit reports on specified security parameters are submitted by such data fiduciaries as it determines as (and not just significant data fiduciaries as is currently envisaged) to them. Further, by an amendment to Section 27 (1) of the Act (Powers and Functions of Data Protection Board), each nodal agency should then be required to submit the compliance report in a pre-specified format to the Data Protection Board. These reports may also be encouraged to be made public to build public trust in governance both at the data fiduciary level and the government. Such an audit could be covered under the definition of 'reasonable security safeguards' through a notification. This audit will ensure that compliance is driven top down as well as bottom up. The Audit should not be based on static considerations and must assess whether every change from the original consent requirements have been notified in advance and respond to evolving market practices and technologies.

3) **Appoint Board Members with technical expertise**: Assessing whether a data fiduciary has undertaken reasonable security practices requires a thorough understanding of technical processes and mechanisms that safeguard privacy. The Act provides for members of the Data Protection Board, who *may* have such technical capacity, but this is not mandated.[21] An amendment to Section 19(3) to endow the Board with the necessary technical capacity by appointing at least one such member with expertise to assess the technical soundness of privacy safeguards and practices is crucial to effectively enforce provisions such as Section 8(5).

## 2.3 Processing Minors' Data

### 2.3.1 Position under the Act

Under the new framework, data fiduciaries are expected to take verifiable parental consent before processing any data pertaining to minors (persons lesser than age of

[20] https://indiaai.s3.ap-south-1.amazonaws.com/docs/IndiaAI+Expert+Group+Report-First+Edition.pdf
[21] Section 19(3), Digital Personal Data Protection Act, 2023

18).[22] This makes it onerous for data fiduciaries, as in order to collect a child's data, there will be a higher data collection effort in order to route consent through the parents. This may also have the effect of restricting children's access to the internet. In its current form, the Act does not envisage how the age verification would be done.

Section 9(5) enables the Government to apply differential standards to fiduciaries who process data in a manner that is 'verifiably safe,' but for the effective application of the law, rules/ guidelines will need to clarify how data can be made safe as per the Act's standards for children. Data privacy pertaining to children and children's data is a matter of serious importance, with very few successful attempts at assuring a high level of data privacy for children, across the world. In India until now, a child above the age of 13 can open Google, Facebook, and Instagram accounts. However, age verification of children on the internet is challenging for several reasons:

a. Firstly, the internet allows users to remain largely anonymous, making it difficult to ascertain the age of a user accurately.
b. Secondly, children can easily misrepresent their age when creating online accounts, thereby circumventing age restrictions, and making the parent who consented on their behalf liable for any misrepresentations on their behalf.
c. Thirdly, balancing age verification with children's right to privacy is a delicate issue. Verifying parental consent also involves collecting additional information pertaining to the children. While it is crucial to protect children from harmful content and interactions, it is equally important to respect their privacy and ensure their digital rights are not violated.
d. Fourthly, the use of shared devices in a household can potentially complicate age verification processes for websites aiming to restrict access to certain content or services based on age. In many households, multiple family members, including children and adults, may share a single device and use a common account. Age verification is typically tied to individual accounts, and if everyone is using the same login credentials, it becomes challenging for websites to accurately assess the age of each user. Parents or guardians may have control over the device's settings and permissions, but these controls may not extend to the websites accessed. Children might find ways to access content or services by using incognito modes, alternative browsers, or other methods that circumvent age verification measures.

[22] Section 9, Digital Personal Data Protection Act, 2023

Further, the current framework is hinged on the assumption that parents of minors have the knowledge and capacity to adequately understand the digital ecosystem and can make informed choices on their behalf. However, only 38% of households in India are digitally literate.[23] This number too, is driven by the number of young people. Hence, age verification by itself may not adequately address the various threats that children may be exposed to on the internet.

The hyper-focus on age verification in the Act at the expense of invisibilising other threats to children in the digital space may not be sufficient to address broader concerns related to children's online experiences. Simply verifying a user's age does not control the amount of time spent online or the type of content consumed.

India is considered a significant market where children are increasingly becoming a target demographic for various products and services. Several industries and businesses recognize the potential of this young consumer base, and they tailor their offerings to appeal to children.[24] While the Act prohibits targeted advertising, websites and platforms also use algorithms to personalize content based on user data. This goes beyond targeted advertisements and includes personalized recommendations, which can shape a child's online experience and perspectives, often negatively. Age verification may also not prevent predatory behaviour or online abuse. Abusers can exploit vulnerabilities in the system to gain access to children.

The lack of a clear definition of 'harm' or "detrimental effect on well-being" makes it easier for platforms to be subversive with privacy norms, dark patterns, and behaviour manipulation using children's data consented upon by parents. 3 kinds of harms can be expected:

a. Bad actors abusing and exploiting children through deepfakes, drug peddling, and pornography.
b. Disadvantaged genders being denied tech access based on moralities and cultural fears.
c. Platforms targeting age-specific vulnerabilities through the hyper-personalisation of content, not advertising.

### 2.3.2 Practices under other jurisdictions

Online age verification methods recognized by the European Commission includes:

[23] Oxfam, India Inequality Report 2022: Digital Divide
[24] https://www.theguardian.com/sustainable-business/2015/jul/22/indian-companies-target-children-push-green-messages-sell-products

1) Self-declaration
2) Using credit card (Since most banks issue credit cards only to adults)
3) Biometrics (including facial recognition)
4) Analyzing online usage patterns
5) Offline verification
6) Parental consent
7) Vouching by users (other than parents)
8) Using a digital ID
9) Verification of age through a government licensed app[25]

The CNIL (The French Data Protection Commission), has analysed each of these methods and concluded that none of these meet the three essential standards required: 1) sufficiently reliable verification, 2) complete coverage of the population and 3) respect for the protection of individuals' data and privacy and their security.[26]

Similarly, the United States is also struggling to regulate the domain of a child safe internet. California's Age-Appropriate Design Code Act (CAADCA), a law that requires special data safeguards for underage users online slotted to come into effect in 2024, was stayed by a Federal Judge for likely violating the right to free speech.[27] On the other hand, there has been a frenzy of bills in states including Utah,[28] Arkansas,[29] Texas,[30] Maryland,[31] Connecticut,[32] and New York[33] to make the internet safer for children. The United States' Federal Trade Commission has approved a third-party programme called KidSafe Seal Programme[34] under which the fiduciary has to demonstrate features such as age-appropriate contents, domestic law compliances etc., to obtain a seal.

### 2.3.3 Recommendations for Protection of Minors' Data

1) **Frame model standard practices for age verification:** Considering that no global standard has been evolved for age verification, the Government

[25] https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf
[26] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[27] https://www.reuters.com/legal/judge-blocks-california-law-meant-protect-childrens-online-safety-2023-09-18/
[28] Social Media Regulation Act 2023 (Utah)
[29] Social Media Safety Act 2023 (Arkansas)
[30] Safeguarding Children Online through Parental Empowerment Act 2023 (Texas)
[31] Maryland Online Consumer Protection and Child Safety Act 2022
[32] Amendment No 7796 to Senate Bill No. 3, An Act Concerning Online Privacy, Data and Safety Protections 2023 (Connecticut)
[33] Stop Addictive Feeds Exploitation (SAFE) for Kids Act 2023 (New York)
[34] https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-kidsafe-safe-harbor-program/kidsafe_seal_program_certification_rules_ftc-approved_kidsafe_coppa_guidelines_feb_2014.pdf

may undertake focused research to come up with standard practices for age verification that would minimize the harms while also reducing the chances of circumvention. A system devoid of all flaws might be impractical to achieve with the current advancements in technology, but sufficient standards can be laid down. This could be done keeping in mind, principles recommended by the CNIL such as:[35]

a) Proportionality
b) Minimization (of the amount of data collected and processed)
c) Robustness (hence, self-verification must be avoided)
d) Simplicity
e) Standardization (so that the same practices can be adopted by a wide range of apps and websites
f) Third Party Intervention

2) **Certify websites that are verifiably safe for children:** For the purposes of determining whether the data collection and processing by a fiduciary is 'verifiably safe,' the Government may adopt self-devices or third-party certification programmes which provides a seal or certificate to websites and apps, like United States' Federal Trade Commission.

3) **Appoint a certification body for compliance with protection of minors data**: Keeping in mind that privacy policies and consent notices would be only read as much as any other form of long-form notices, an intermediary certifying body could take over the cognitive load of parsing data privacy nuances for decision-making on behalf of parents/guardians and provide a stamp of approval or a percentage of privacy adherence to warn parents of the nature of data being shared and risks associated with the same. We have examples of the ISI standard for products or FSSAI standard for food.

4) **Limiting the scope of exempted classes under Section 9(4):** Section 9(4) of the Act carves out an exception by certain "classes of data fiduciaries" and for certain purposes which are yet to be notified.[36] Though there is no clarity on the classes of actors that would fall under this exception, considering the proportionality and legitimate aim tests laid down in the Puttaswamy judgement,[37] schools are likely to be an exempted class in view of the large

[35] https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy
[36] Section 9(4), Digital Personal Data Protection Act, 2023
[37] (2017) 10 SCC 1

amount of data collected from children as part of their routine activities as well as their role in enhancing the educational experience of children. However, making such an exemption, is dangerous, since data collected from children has potential to be long-lived, and is prone to be "dangerous long after it has been created and forgotten" since the massive amounts of data collected is not disposable.[38] Hence, it is recommended that government may exercise caution in defining the classes of fiduciaries exempted under the Act such that the minor's data is not adversely impacted. It is recommended that the government's directives extend to period after which the data so collected will be deleted, especially after child leaving the educational institution.

5) **Draw guidelines to specify data processing that may fall under Section 9(2):** Consider the nature and gravity of the breach of minors' personal data at a higher standard,[39] and thereby inviting a higher penalty than other offences. This shall prioritize the safety and privacy of minors and ensure regulatory compliance. The EU AI Act classifies "unacceptable" and "high risk" categories for data governance of minors' data.[40] The DPDP Act currently prohibits certain kinds of practices such as targeted advertising and behavioural tracking,[41] but these do not cover all the threats faced by children in the digital space. Guidelines covering an indicative list of practices that would fall under Section 9(2) of the Act will help place greater obligation and accountability on data fiduciaries in ensuring child protection. This can also inform the Board in assessing the nature and gravity of the offence while determining penalties.[42]

6) **Amend and expand the scope of Section 27:** Expand the powers vested in the Data Protection Board from merely investigative and adjudicatory[43] through amendments to build information literacy for parents and children. The powers of the supervisory authorities in the EU transcend investigation, and adjudication, and permeate to promoting public awareness and understanding on risks, safeguards etc.[44]

[38] https://link.springer.com/chapter/10.1007/978-3-658-39664-0_9#Fn23
[39] As under Section 33(2)(a) of the Act, the nature and gravity of a breach are grounds for determining the penalty.
[40] Title II, Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts
[41] Section 9(3), Digital Personal Data Protection Act, 2023
[42] Section 33(2)(a), Digital Personal Data Protection Act, 2023
[43] Section 27, Digital Personal Data Protection Act, 2023
[44] Article 57. GDPR

7) **Conduct data audits for government and private bodies**: Conducting frequent audits as part of ensuring reasonable security practices for both government and private data processors would help in identifying and mitigating threats to children's privacy. Currently, audits are envisaged only in respect of significant data fiduciaries under the Act.

8) **Draw guidelines to promote privacy by design standard for data fiduciaries and processors, by converging and coordinated efforts across Ministries** : It is crucial to promote privacy by design to ensure that data protection becomes part and parcel of data processing systems without individuals necessarily needing to fully comprehend the often times complex internal data processing practices of controllers.[45] A child centered approach towards privacy by design would entail the design, development and execution of websites, apps etc. used by children with the primary consideration of children's best interests.[46] For instance, the UK Information Commissioner's Office for instance, provides an indicative list of practices that companies may adopt to incorporate children's privacy by design in their products/websites. [47] Bringing out similar guidelines fit to the Indian context would not only further the protection of children under the law, but also even out the responsibility for privacy protection between the companies and users. One way to do this would be to mandate privacy by design as a pre-incorporation licensing requirement for start-up companies which may collect and process data pertaining to minors. This would envisage contemporaneous changes in the Companies Act, 2013 as well as convergence with initiatives of the National and State Commissions for Protection of Children's Rights, under the Ministry of Women and Child, Ministry of Education and Ministry of Corporate Affairs.

9) **Collaborate with civil society organizations**: The government may also leverage the support of civil society organisations in information dissemination and engaging with companies to adopt responsible practices. Civil society plays a crucial role as the guardians of children's safety, especially in the digital realm. Acting as intermediaries, civil society organizations can help alleviate the burden on parents by facilitating a better understanding of the concept of notice, which

[45] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107660
[46] https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf
[47] https://ico.org.uk/about-the-ico/media-centre/events-and-webinars/privacy-by-design-designing-with-children-s-privacy-in-mind/#:~:text=The%20Children's%20code%20is%20a,designed%20with%20them%20in%20mind.

involves providing information to individuals, including parents, about data collection and usage practices.

## 2.4 Sufficient Grounds of Enquiry on Complaints of Data Breach

### 2.4.1 Position under the Act

Upon receiving a complaint of data breach or through reference from the Government, the Data Protection Board of India (DPB) is to ascertain whether there are "*sufficient grounds*" for proceeding with an official inquiry.[48] A pre-requisite for identifying sufficient grounds of action against data breach, is that Members of the Board are technically well versed. In this context, it is to be noted that the Act does not lay down strict qualifications for the Board Members. Hence, there could arise a situation where the Board may consist of non-domain experts with no expert knowledge of data breaches, and this results in limitations of the Board's functioning and initiatives. India's Competition Commission also suffers from very similar capacity shortcomings resulting in delays in matters before it,[49] as well as in keeping pace with quickly evolving technological advancements.

Sec 33 (1) of the Act provides that if the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the person the opportunity to be heard, impose penalty under the Schedule to the Act. Section 33(2) further clarifies that while determining the amount of monetary penalty to be imposed, the Board shall have regard to the following matters:

a) the nature, gravity and duration of the breach
b) the type and nature of the personal data affected by the breach.
c) repetitive nature of the breach
d) whether the data fiduciary, as a result of the breach, has realised a gain or avoided any loss.
e) whether the data fiduciary took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action.

[48] Section 28(3), Digital Personal Data Protection Act, 2023
[49] https://economictimes.indiatimes.com/news/india/india-antitrust-agency-squeezed-by-staff-vacancies-and-workload/articleshow/98508824.cms#

f) whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and
g) the likely impact of the imposition of the monetary penalty on the person.

The specific composition of the Board has not been detailed under the Act, and the same is expected to be notified under the Rules.

### 2.4.2 Practices under other jurisdictions

The California Consumer Privacy Act clearly lays down the two grounds that the Privacy Protection Agency[50] may take into consideration while deciding to not investigate or provide more time to cure/ rectify the alleged violation:

- Lack of intent to violate the legislation.
- Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

### 2.4.3 Recommendations on 'sufficient grounds of enquiry'

1) **Issue Guidelines to Data Protection Board (DPB)on what constitutes "sufficient grounds":** Guidance on what constitutes sufficient grounds of enquiry is necessary for the Board to function effectively. Amending Section 28(3) of the Act or by issuing separate guidelines to the Board to lay out the grounds that lend sufficient basis to initiate an enquiry would enable the members of the Board to take quick action in case of violations of the Act which can be as broad as what is laid down in the California legislation, or as narrow as specific grounds on which inquiry must be initiated. On similar lines, Section 19(3) and 19(4) of the Competition Act 2002, provides the Competition Commission with a list of factors to be considered while undertaking an inquiry into appreciable adverse effects or dominance in the market. Similarly, section 17 of the Prevention of Money Laundering Act 2002 clearly lays down the grounds on which a search and seizure order may be authorized.

2) **Include a charter of purpose for the DDPB** – Drawing a clear mission statement for the Board will help to anchor the purpose for Board and accordingly orient its initiatives, including the determination of indicators to inform whether an inquiry is necessary. Affirmative language suggesting that

[50] Clause 1798.199.45, California Consumer Protection Act 2018

the DPB should take steps and initiatives to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection, will go a long way in framing the DPB as a friend of the data principals, rather than an authoritarian/bureaucratic set-up. This may be done through an amendment to the Act, as devoid of a charter the Board's role may remain undefined for judicial interpretation.

3) **Maintain Board's Independence** – It is important to make provisions to maintain the independence of the Board to mitigate any power or influence that can be wielded by any agency, as has been seen from Ireland's challenges. Since most of the major U.S. tech platforms have their European subsidiaries on the Emerald Isle, Ireland has struggled to emerge as a strict GDPR enforcing jurisdiction and has also recently come under criticism for this.[51] Considering that the Board does not have explicit suo-motu powers under the Act, one concern is that the Board is not vested with sufficient powers to maintain and assert independent oversight in the matter of data protection. Further, it continues to rely on complaints brought before it by aggrieved individuals or the government. This limitation can be overcome by making amendments under Chapter VI of the Act:
    i. permitting certain recognised groups such as civil society initiatives to advocate on behalf of citizen groups before the DPB.
    ii. endowing the DPB with necessary technical capacity to understand the latest technologies is important to ascertain the extent of harm, to inform the need to intervene.
    iii. bifurcating the investigation and adjudication powers among different members of the DPB will help to maintain objectivity and independence.
    iv. strengthening the enforcement capacity of the DPB in respect of orders made by it will help to strengthen the position of the DPB. Currently only the orders of the Appellate Board are enforceable as the decree of a civil court.[52]
    v. DPB should remain an accessible forum which has capacity for swift and appropriate action. When complaints are filed before the DPB, the form of the complaint must be kept simple and accessible for the ordinary citizen, without making the forms for complaint too lengthy or complex to fill in.

[51] https://www.simmons-simmons.com/en/publications/ckucpnrme21dy0a42mwuhhhae/ireland-s-balance-between-big-tech-and-data-privacy
[52] Sec 30(1) of the Act

## 2.5 Provisions on Consent from Persons with Disabilities

### 2.5.1 Position under the Act

The provisions on verifiable parental consent while obtaining data pertaining to children also extends to persons with disabilities. The law provides that the consent of a legally appointed guardian of persons with disabilities, will where available be taken.[53] However, the Act does not shed light on the class of disabled persons to whom these provisions shall apply. The Rights for Persons with Disabilities Act, 2016 envisages a benchmark for disabilities. A person with more than benchmark (more than 40% disabilities) is provided certain accommodations under the said act.

The provision of DPDP Act on consent being routed through a guardian where appointed, seemingly applies to all persons with disabilities. This will have implementation challenges since disability is a broad spectrum that encompasses physical, mental, intellectual or sensory impairments. Further, for a person with a disability, a legal guardian maybe appointed under the National Trust Act,[54] or the Rights of Persons with Disabilities (RPWD) Act.[55] The processes and the specific role of the guardian varies under both the Acts, creating an ambiguity in the interpretation of this section.

The guardian under the RPWD Act is typically appointed for a period of five years, so routing the consent through the guardian may mean that the consent is valid only for a period of five years, making the process of collecting consent of persons with disabilities more cumbersome.

### 2.5.2 Recommendations on Consent Framework for Persons with Disabilities

1) **Issue clarifications on 'Persons with Disability':** It is imperative that the Government, in consultation with the MSJE, issue clarifications on who shall be considered a person with disability for the purposes of the DPDP Act, and whether a person with disability with a legally appointed guardian can be assumed to lack the capacity to consent. Consent frameworks protecting the

[53] Section 9, Digital Personal Data Protection Act, 2023
[54] Section 14, The National Trust Act, 1999
[55] Section 14, The Rights of Persons with Disabilities Act, 2016

rights of persons with disability to share their data securely and to access the internet equitably need to be iteratively built. There is no global standard or principles in respect of consent frameworks for persons with disability pertaining to their right of data privacy, reflecting that a simplistic provision in the DPDP is likely to create challenges in interpretation and implementation.

2) **Convergence in Policies of MEITY and MSJE:** A convergent and coordinated policy jointly driven by the Ministry of Social Justice and Empowerment and the Ministry of Electronics and Information Technology is necessary towards achieving digital accessibility is essential.

3) **Ensure better implementation of the RPWD Act to further digital accessibility :** It remains true that digital accessibility is still a challenge[56] even though the RPWD Act mandates that the Central Government take appropriate measures to ensure that all digital and information and communication technology services are accessible.[57] Thus the implementation of the RPWD Act in letter and spirit is a key milestone, and foundation upon which further digital rights for citizens with disability would be built.

4) **Extend Inclusive Consent Framework across Various Rights under the DPDP Act:** Within the larger effort towards building digital accessibility for persons with disabilities, special efforts towards inclusive and accessible consent frameworks are critical. Alternate mechanisms to provide consent for disabled persons (in formats other than in writing, such as audio-visual, graphic, etc.) must be developed based on consultation with civil society. Inclusive mechanisms must by design also extend to processes and frameworks for revocation of consent once given, requests for deletion of personal data, filing grievances pertaining to data breaches.

5) **Create Awareness and Capacity Building among Persons with Disabilities:** Currently there is little awareness and demand for inclusive information and communication technology from groups of persons with disabilities in India.[58] Further persons with disabilities already face socio-economic barriers in accessing the internet.[59] In this context, narratives of digital personal data protection and data privacy need to be gradually built among the community.

[56] https://vidhilegalpolicy.in/research/making-the-digital-eco-system-disabled-friendly/
[57] Section 42, The Rights of Persons with Disabilities Act, 2016
[58] https://www.broadbandindiaforum.com/media/attachments/2020/08/10/wp-ict-accessibility-report-online---7-aug-2020--v2-1.pdf
[59] https://www.researchgate.net/publication/308171283_%27Disability_and_Social_Media_in_India%27

The implementation robustness of the DPDP Act relies on the individual data principals to enforce their rights under this Act. Thus, it becomes imperative for government to engage in building capacity and awareness as to the rights under this Act, specifically for the marginalized groups such as persons with disabilities.

## 3. Section 2: Overcoming the Ambiguities of the DPDP Act

The ambiguities in the Act can largely be addressed by subsequent rules, notifications, and guidelines. Certain provisions also require review considering best practices from across jurisdictions and the standards laid down in the Puttaswamy judgement.

The lack of a compensatory regime is one such evident shortcoming. Section 43A of the Information Technology Act, 2000, which previously allowed compensation claims for data breaches, has been repealed by the DPDP Act. Compensation provided a means to address various harms individuals face when their personal data is compromised, including financial losses, emotional distress, and privacy violations. While substantial penalties act as deterrents for data fiduciaries, compensation incentivized individuals to report breaches and seek redress. With this avenue closed, there is now less motivation for the public to actively pursue accountability for data breaches. The absence of a compensation mechanism has shifted the burden of seeking justice onto individuals, making it more challenging for them to act when their data is mishandled, which ultimately undermines the overall accountability and security of personal data.

Further, as it stands in the DPDP Act, the Data Protection Board can only act upon a complaint by a data principal or through reference by the Central Government. In cases where individuals might be unaware of their rights or unable to file complaints, *suo motu* powers (if vested in the Board) ensure their interests are safeguarded. This is particularly important for protecting vulnerable groups or individuals who may not be well-versed in data protection laws or have the means to seek legal redressal. Amending the Act to permit the Data Protection Board to act *suo motu* would enable the Boards to take proactive measures to ensure compliance, rather than relying solely on reactive responses to complaints. This proactive approach helps in preventing data breaches and privacy violations.

Similarly, in its report,[60] the Sri Krishna Committee had recommended that for processing of sensitive personal data, an even higher standard of consent than the ordinary one described above must apply. The GDPR[61] for instance, sets higher standards for the processing of personal data that are indicative of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership etc. Amending the Act to define sensitive personal information and setting a higher penalty for its breach, would act as deterrents for data processors in handling such data cavalierly. This becomes poignant in view of the repeal of Section 43A of the Information Technology Act, 2000, as discussed above.

In the current digital landscape, our data protection law provides a robust legal framework for safeguarding digital personal data. However, the effectiveness of any law hinges not only on its existence but also on broader cultural awareness. The data protection authorities under the GDPR, for instance, are specifically tasked with promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.[62] Building a culture of digital privacy awareness is paramount for the seamless operation of the Act. The Data Protection Board must play a pivotal role in instilling and promoting this culture. Hence in India too, the Government should review the mandates of the Board to include awareness building for both businesses and individuals.

[60] https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[61] Article 9, GDPR
[62] Article 57, GDPR

## Appendix: Methodology

The recommendations postulated in this policy paper are derived from the research conducted by the authors. It includes secondary research and expert consultations, which are organised in the form of consultative workshops.

### Design of the consultative workshop

Experts from academia, industry, thinktanks, and former bureaucrats are consulted to understand the existing challenges with the consent mechanism and identify the potential solutions. Below are the details of the experts for 5 consultative sessions.

### I. Format, content and simplicity of the notice under the DPDP Act

*Prof. Indranath Gupta:* Professor and Dean, Data, Innovation and Technology, Jean Monnet Chair (2020- 23), O. P. Jindal Global University.
*Prof. Krishna Deo Singh:* Associate Professor, Jindal Global Law School, O. P. Jindal Global University.
*Mr. Ketan Mukhija:* Partner, Dentons Link Legal (formerly Link Legal)'s.

### II. Defining 'Reasonable Security Safeguards' to Govern Data Privacy under the DPDP Act

*Ms. Deepa Ojha:* Deputy Manager – Policy, Data Security Council of India (DSCI).
*Mr. Rodney Ryder:* Partner, Scriboard, a full-service law firm.
*Mr. S Chandrasekhar:* MD and CEO, K&S Digiprotect Services Pvt Ltd.

### III. Processing Minors' data under DPDP Act

*Ms. Chitra Iyer:* Co-Founder & CEO at Space2Grow.
*Ms. Nidhi Sudhan:* Co-founder of Citizen Digital Foundation.
*Mr. Nikhil Naren:* Chevening Scholar and Assistant Professor at Jindal Global Law School.

### IV. Sufficient Grounds of Enquiry by the Data Protection Board on Complaints of Data Breach

*Mr. Shashank Mohan:* Program Manager, Centre for Communication Governance at National Law University, Delhi.
*Dr. Akanksha Natani:* Assistant Professor at Human Science Research Center (HSRC), IIIT Hyderabad.
*Mr. Siddharth Deb:* Manager, Public Policy, The Quantum Hub (TQH) and Young Leaders for Active Citizenship (YLAC).

### V. Provisions on Consent from Persons with Disabilities Under the Act

*Mr. Prashant Ranjan Verma:* General Secretary at National Association for the Blind Delhi.
*Ms. Aparna Mehrotra:* Litigation Associate, Center for Law and Policy Research.

## About Authors

**Ms. Nivedita Krishna** is a Technology Policy Consultant at Wadhwani Centre for Government Digital Transformation.

**Dr. Arun Teja Polcumpally** is a Technology Policy Analyst at Wadhwani Centre for Government Digital Transformation.

**Mr. Alok Gupta** is Director, Policy and Technology at Wadhwani Centre for Government Digital Transformation.

This report is produced by Wadhwani Centre for Government Digital Transformation, an initiative of the Wadhwani Foundation, a not-for-profit institution focusing on public policy issues. Wadhwani Foundation does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

WADHWANI FOUNDATION

www.wfglobal.org

Wadhwani Foundation is a global not-for-profit with the primary mission of accelerating economic development by driving job creation through large-scale initiatives in skilling, entrepreneurship, government digital transformation and innovation & research. Founded by Silicon Valley entrepreneur, Dr. Romesh Wadhwani, the Foundation today is scaling impact across multiple countries in Asia, Africa, and Latin America through innovative programs that leverage the latest technology and expansive global networks to democratize access to world-class resources needed to improve livelihood and change lives.

ASIA | AFRICA | LATIN AMERICA