December 2024

Persons with Disabilities vis-à-vis the Digital Personal Data Protection Act, 2023

Centre for Communication Governance at National Law University Delhi

॥न्यायस्तत्र प्रमाण स्यात्॥
NLU DELHI
CENTRE FOR COMMUNICATION GOVERNANCE

Image Description of cover page:

The cover page of the policy brief is designed like a front-facing touchscreen tablet with a black frame. On the right corner of the top black frame, the month and year of publication, 'December 2024' are written. Below the top black frame, on the tablet screen, nine symbols are arranged in a grid in three rows. In the first row, from left to right: the accessibility symbol in a pink box, the symbol for Audio Description for TV, Video and Film in an orange box, the symbol for Sign Language Interpretation in a cyan blue box. In the second row, from left to right: the symbol for Access to low vision in a red box, the login tab symbol inside a chrome yellow box, and the Braille symbol in a green box. In the third row, from left to right: the symbol for Access for hearing loss in a light blue box, the closed captioning symbol in a lime green box, and the information symbol in a yellow box. The title of this document, 'Persons with Disabilities vis-à-vis the Digital Personal Data Protection Act, 2023' is written under the grid of nine symbols. The words 'Centre for Communication Governance at National Law University Delhi' are written on the left of the bottom black frame. The institutional logos of National Law University Delhi and the Centre for Communication Governance are written on the right of the bottom black frame.

Persons with Disabilities vis-à-vis the Digital Personal Data Protection Act, 2023

CCG Policy Brief

Centre for Communication Governance
National Law University Delhi

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 and Tithi Neogi

We thank Rahul Bajaj for his feedback on this paper.

Reviewed by Sachin Dhawan, Joanne D'Cunha and Shashank Mohan.

Design by Gopika P.

Acknowledgements: This paper 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. We would also like to thank Jhalak M. Kakkar, Executive Director at CCG, for her unwavering support, encouragement, and mentorship, which have been instrumental in publishing this research. We are particularly grateful to our stakeholders for sharing their insights. Our stakeholders include Shivangi Rai, Deputy Coordinator and Shefali Malhotra, Research Consultant, Centre for Health, Equity, Law and Policy; Maitreya Shah, Tech Policy Fellow at UC Berkeley, and an Affiliate at the Berkman Klein Center for Internet and Society at Harvard University; and Rahul Bajaj, Co-Founder, Mission Accessibility, Senior Associate Fellow, Vidhi Centre for Legal Policy, and Adjunct Faculty, BML Munjal University School of Law. 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 the many ways in which they supported the paper.

Suggested Citation – 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.

ABOUT THE NATIONAL LAW UNIVERSITY DELHI

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 by an Act of the Delhi legislature (Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.

The University offers a five year integrated B.A., LL.B (Hons.), a one-year postgraduate masters in law (LL.M), and a Ph.D. program, along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres, and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

ABOUT THE CENTRE FOR COMMUNICATION GOVERNANCE

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research on information technology law and policy in India. It has in a short span of time, become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy-making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain. CCG works across issues such as privacy and data governance, platform governance, and emerging technologies.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNESCO, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, Tech Policy Design Centre at the Australian National University, and the Technical University of Munich.

The Centre has authored multiple publications over the years, including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, an essay series on Democracy in the Shadow of Big and Emerging Tech, a comprehensive report on Intermediary Liability in India, an edited volume of essays on Emerging Trends in Data Governance, and a guide for Drafting Data Protection Legislation: A Study of Regional Frameworks in collaboration with the United Nations Development Programme, and most recently - a Report on Social Media Regulation and the Rule of

Law in Sri Lanka, India and Bangladesh. It has also published reports from three phases of the Blockchain Project conducted in collaboration with the Tech Policy Design Centre at the Australian National University, which maps the blockchain ecosystem in India and Australia.

Privacy and data protection have been focus areas for CCG since its inception, and the Centre has shaped discourse in this domain through research and analysis, policy inputs, capacity building, and related efforts. In 2020, the Centre launched the Privacy Law Library, a global database that tracks and summarises privacy jurisprudence emerging in courts across the world, in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. The PLL currently covers 250+ cases from 20+ jurisdictions globally and also contains a High Court Privacy Tracker that tracks emerging High Court privacy jurisprudence in India.

CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on information technology law and policy. The Centre has also offered Certificate and Diploma Courses on AI Law and Policy, Technology Law and Policy, and First Principles of Cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and enable a nuanced engagement with the dynamic space of technology and cyberspace, their implications for society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy. Most recently, CCG and UNESCO conducted a Workshop on 'AI and the Rule of Law' for stakeholders of the justice sector from India, Bhutan, Maldives, Nepal, and Sri Lanka.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The policy brief on 'Persons with Disabilities vis-à-vis the Digital Personal Data Protection Act, 2023' ("DPDPA") examines the inclusion of persons with disabilities within India's data protection framework. This has been analysed in terms of consent, autonomy and protection of privacy rights. This is a relevant area of research because there is a close intersection between disability and data protection rights that relates to the unique challenges and vulnerabilities faced by persons with disabilities on the Internet. The DPDPA has acknowledged persons with disabilities as a separate class of data principals. The DPDPA has also attempted to support persons with disabilities in decision-making under Section 9. Through these efforts, the DPDPA has taken a major step towards making the data protection framework more inclusive. However, the inclusion of persons with disabilities within the data protection framework appears to lack nuance. The DPDPA does not define persons with disabilities, which leads to challenges in interpreting how guardianship is envisioned in relation to the DPDPA. The DPDPA, as presently drafted, limits the agency of persons with disabilities particularly in terms of upholding the autonomy already guaranteed under other legal frameworks. For instance, Section 9 of the DPDPA infantilises persons with disabilities by clubbing them with children in the same provision and consequently over-indexes on the role of the lawful guardian in decision-making processes. The DPDPA also does not provide for adequate safeguards to prevent abuse of power by lawful guardians. Further, it fails to carve out exempted digital services for which data fiduciaries may process the data of persons with disabilities without collecting verifiable consent from their lawful guardians. Moreover, in addition to limiting consenting power, the DPDPA does not include sensitive personal data ("SPD") as a distinct category of personal data and additional safeguards, compared to previous iterations of the law. The lack of this distinction has created challenges in ensuring that additionally vulnerable types of personal data such as finance or health related are adequately protected. While SPD is susceptible for all categories of individuals, breaches of data of such sensitive and identifying nature can be particularly vulnerable for persons with disabilities. The law does not appear to consider the additional sensitivity of personal data relating to persons with disabilities.

Part 1 of this policy brief introduces the need to recognise the challenges faced by persons with disabilities in the digital ecosystem. This includes digital exclusion and inaccessible consent mechanisms perpetuated by laws that were agnostic to the needs of persons with disabilities. For example, the extant **Information Technology Act, 2000 ("IT Act")** and the **Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules")** provided no provisions specific to the needs of persons with disabilities. The DPDPA, in attempting to address these concerns, vests excessive consenting power with the lawful guardian of the person with disability.

Part 2 explores the key issues with the DPDPA. It specifically addresses certain concerns with Section 9(1) of the DPDPA, including the curtailing of autonomy of persons with disabilities. Section 9(1) lacks a definition of persons with disabilities. Further, Section 9 of the DPDPA, pertaining to processing of data and verifiable consent, infantilises persons with disabilities by clubbing children and persons with disabilities who have lawful guardians in the same provision. The DPDPA lacks adequate safeguards to ensure that decisions taken by the lawful guardian are mutually taken in consultation with the persons with disabilities. Moreover, the DPDPA does not provide certain data fiduciaries to be exempted from collecting verifiable consent from their lawful guardians. However, this has been carved out for the processing of children's personal data in the absence of verifiable parental consent. In addition to concerns with Section 9(1) of the DPDPA, several other issues arise as well. The DPDPA fails to recognise SPD as a distinct category of data warranting additional safeguards. The DPDPA does not make any provisions for accessible Information and Communication Technologies ("ICT") in relation to data protection, failing to acknowledge that digital accessibility is often the precursor to data privacy.

Part 3 recommends solutions to address these key concerns. Specifically, it contends that a separate provision pertaining to the data and consent of persons with disabilities must be added to the DPDPA. This provision must adequately define the term 'person with disability' itself, for the purposes of the DPDPA. The scope for abuse of power by lawful guardians can be limited by basing decision-making of the lawful guardian on

the principles of limited guardianship and mutual decision-making, informed by the **Rights of Persons With Disabilities Act, 2016 ("RPWDA")**. Certain data fiduciaries should be notified by the government, which may allow their digital services to be accessed by persons with disabilities even in the absence of verifiable consent from their lawful guardians. Additional safeguards for sector-specific sensitive personal data like financial and health data must be reinstated in the DPDPA to cater to the heightened vulnerability of persons with disabilities to breaches of data. Since the DPDPA already carves out a provision for persons with disabilities, it would be useful for the framework to include accessibility considerations as well. Such a provision must obligate data fiduciaries to incorporate accessibility features in their notice and consent mechanisms.

Part 4 concludes the policy brief by reiterating the need for aligning the DPDPA with the principles of limited guardianship and mutual decision-making under the RPWDA, re-emphasising the key problems identified with the DPDPA, and the solutions proposed.

It is hoped that the issues highlighted by the policy brief with regard to the inclusion of persons with disabilities in the DPDPA are rectified, and the recommendations are reflected through legislative amendment and through the subsequent DPDP Rules that will bring the DPDPA into effect.

1. INTRODUCTION

In its landmark *Puttaswamy* ruling,[1] the Indian Supreme Court stressed the need for a comprehensive data protection law. Seven years on and several draft bills later,[2] India finally has a personal data protection law - the **Digital Personal Data Protection Act, 2023 ("DPDPA")**. This is indeed a development of significance that promises to bring about many changes for privacy online.

Some of these changes concern persons with disabilities.[3] An integral aspect of the data protection law is its provisions on consent for persons with disabilities, contained in Section 9(1) of the DPDPA. This provision obligates data fiduciaries to obtain 'verifiable consent' from the lawful guardians of persons with disabilities to process their personal data, in cases where a lawful guardian has been appointed for the person with disability. Section 9(1) of the DPDPA only appears to primarily refer to those persons with disabilities who have been appointed a lawful guardian under guardianship frameworks in India. It is pertinent to clarify that in cases where no guardians exist, the DPDPA does not, through the aforementioned provision, require all persons with disabilities to be appointed lawful guardians for the purposes of providing consent online. Consent is often considered to be an important facet of data processing, because it gives users agency, choice, and autonomy over how their data is

[1] *Justice K.S. Puttaswamy v Union of India* [2017] 10 SCC 1.

[2] Before the DPDPA was tabled in the Parliament, none of the prior draft data protection laws contained distinct provisions for persons with disabilities. In the absence of a dedicated legislation addressing the data protection framework in India, persons with disabilities faced several challenges in navigating the digital ecosystem. As discussed in the policy brief, the DPDPA takes a significant step towards taking into account the special needs of persons with disabilities, but remains limited in its approach.

[3] The language used throughout the policy brief is in alignment with the person-first approach followed by the United Nations ("UN") Disability Inclusive Language Guidelines and the UN Convention on the Rights of Persons with Disabilities, 2006. For the purposes of this policy brief, a "person with disability" means a person with "long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders his full and effective participation in society equally with others," as under Section 2(s) of the Rights of Persons with Disabilities Act, 2016 ("RPWDA").

processed.[4] However, consent alone is very limited,[5] and would be meaningless if safeguards for data protection are inadequate.

The DPDPA takes a step forward from the extant **Information Technology Act, 2000 ("IT Act")** and the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules")**.[6] Prior to the DPDPA, the now replaced SPDI Rules served as the data protection framework in India. The SPDI Rules were delegated legislation made under Section 43A of the IT Act. The SPDI Rules defined personal information and Sensitive Personal Data ("SPD"), and distinguished the two by providing additional safeguards for the latter. Under the SPDI Rules, information pertaining to physical, physiological and mental health conditions[7] and medical records,[8] which is also of relevance to persons with disabilities, was included within the classification of sensitive personal data.[9] However, the SPDI Rules, particularly in terms of its provisions for consent mechanisms and privacy policies, were agnostic to the unique accessibility needs of persons with disabilities. The mechanism of collecting informed consent under the SPDI Rules left persons with disabilities unsupported in an inaccessible data protection framework. This was even after the enactment of the

---

[4] Puttaswamy (n 1).

[5] The authors are cognisant of the fact that consent per se has limited ability to uphold user choice, as indicated in literature including the Srikrishna Committee Report. Consent mechanisms are often boilerplate, which makes it difficult to give informed and meaningful consent. However, this should not be held as a ground to reject the normative value of consent relating to autonomy of the data principal, as suggested in the Srikrishna Committee Report.

[6] The SPDI Rules primarily made up for the data protection framework in India. Some sector specific regulations also dealt with privacy and confidentiality of data, such as the Information Technology (the Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013; directions issued by the Indian Computer Emergency Response Team (CERT-In); Consumer Protection Act, 2019; Consumer Protection (E-Commerce) Rules, 2020; Credit Information Companies (Regulation) Act, 2005 and Rules issued by regulatory authorities such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India, and the Securities Exchange Board of India. The Digital Information Security in Healthcare Act (DISHA) Bill, 2018 was released for public consultation but never enforced.

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

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

[9] As will be explained below, the creation of the SPD category is beneficial to persons with disabilities.

RPWDA, which guaranteed the right to accessible Information and Communication Technologies ("ICT") for persons with disabilities.[10]

In the absence of a dedicated legislation on data protection in India, persons with disabilities faced several unique challenges in navigating the digital ecosystem. This was particularly exacerbated during the pandemic.[11] A notable example of this is the COVID-19 contact tracing app, Aarogya Setu, which was inaccessible to persons with disabilities because it lacked features like closed captioning, audio descriptions, and adequate colour contrast ratio.[12]

The lack of recognition of a lawful guardian as a support mechanism in the SPDI Rules, coupled with barriers to information access, made it difficult for persons with disabilities to give informed consent. For instance, accessibility to banking and financial services became predominantly virtual during the pandemic. However, many digital payment applications were inaccessible for persons with disabilities, particularly blind and low vision users, by being incompatible with assistive technology like screen readers. Women with disabilities in rural areas were particularly affected by inaccessible features on payment applications, and had to rely on others to make or access digital payments.[13]

Against this background, the DPDPA attempts to address this digital exclusion by including persons with disabilities within the data protection framework. It is among

[10] The Rights of Persons with Disabilities Act, 2016, s 42.

[11] Divya Goyal, 'People with disabilities during the COVID-19 pandemic in India' (*ORF Online*, 28 Nov 2020) <https://www.orfonline.org/expert-speak/people-disabilities-covid19-pandemic-india/> accessed 29 November 2024.

[12] Sabah Rahman, 'Aarogya Setu remains inaccessible for disabled despite push from activists' (*The Indian Express*, 27 May 2020) <https://indianexpress.com/article/india/aarogya-setu-app-aarogya-setu-app-disabled-inaccessible-coronavirus-contact-tracing-6416094/> accessed 29 November 2024.

[13] For more on barriers to information access, lack of digital accessibility and support for persons with disabilities, refer to Rising Flame and Sightsavers, 'Neglected and Forgotten: Women with disabilities during Covid crisis in India' (14 July 2020) <https://mhi.org.in/media/insight_files/NeglectedAndForgotten_RFandSS.pdf> accessed 29 November 2024.

the few data protection legislations that carve out distinct protections for persons with disabilities.[14]

1.1. Consent from Persons with Disabilities under the DPDPA

The DPDPA defines data principal as "the individual to whom the personal data relates."[15] In case the data principal is a person with disability, the DPDPA includes within this definition the lawful guardian of such a person.[16]

Section 9 of the DPDPA lays down the manner of processing of personal data belonging to children and persons with disabilities. In order to process personal data of persons with disabilities, data fiduciaries must take verifiable consent from the lawful guardians of persons with disabilities.

At the same time, as this policy brief will show, the DPDPA suffers from an oversight. The DPDPA lacks a definition of persons with disabilities. For data principals who are persons with disabilities, the DPDPA overextends the support of lawful guardians. The DPDPA does not incorporate mutual decision-making [17] and safeguards in the relationship between persons with disabilities and their lawful guardians, as under the **Rights of Persons with Disabilities Act, 2016 ("RPWDA")**. By having verifiable consent be provided for only by lawful guardians, the DPDPA restricts the decisional autonomy that a person with disability may otherwise be capable of

[14] Another example of a data protection law carving out special protections for persons with disabilities, the American Data Privacy and Protection Act ("ADPPA"), is a pending Bill in the United States of America. It explicitly provides protection to persons with disabilities in terms of classifying data relating to disability as "sensitive" under Section 28 (A)(ii), providing heightened safeguards for the same. The ADPPA also includes persons with disabilities within the protected classes designated with respect to civil rights protections. Section 207(a) of the ADPPA prevents service providers from carrying out data practices in a manner that discriminates against persons with disabilities. The General Data Protection Regulation ("GDPR") also classifies health data within its definition of sensitive personal data under Article 9, but it does not explicitly carve out other distinctions for persons with disabilities as data principals. While the GDPR does more broadly recognise "vulnerable natural persons," it does not explicitly mention persons with disabilities there. Such a distinction is only made for children under the GDPR.

[15] The Digital Personal Data Protection Act, 2023, s 2(j).

[16] The Digital Personal Data Protection Act, 2023, s 2(j)(ii).

[17] Mutual decision-making is an integral element in the relationship between a person with disability and their lawful guardian, as envisaged in Section 14 of the RPWDA. This is explained in greater detail in Part 2 of the policy brief.

exercising as a data principal under the DPDPA. Consequently, it creates scope for lawful guardians to overstep their responsibilities in the process of extending support to persons with disabilities under the DPDPA. It is relevant to note that the DPDPA has not explicitly indicated which legislation it refers to or relies upon in terms of guardianship. The authors are cognisant that there are multiple Indian legislations that deal with guardianship in India, including the **National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999**. However, since its enactment in 2016, the RPWDA has been the foremost disability framework in India. The authors recognise certain flaws with this legislation, including challenges with enforceability. Nevertheless, the RPWDA has been relied on for the purpose of this policy brief because of its enactment post India ratifying the **United Nations Convention on the Rights of Persons with Disabilities, 2006 ("UNCRPD")**. The RPWDA best enshrines the principles of the UNCRPD among all the other legislations that deal with guardianship for persons with disabilities in India.

Additionally, the DPDPA completely does away with the categorisation of SPD and additional safeguards which were provided for in previous iterations of the DPDPA.[18] This has led to uncertainty within the Indian policy ecosystem around how to sufficiently safeguard certain sector-specific data like financial and health data, which could directly be more vulnerable. This is particularly relevant because the SPD of persons with disabilities may be exposed to greater vulnerabilities through the effects of data breaches, impacting their employment, healthcare and social welfare.

This policy brief addresses the imbalance in the DPDPA in relation to the rights of persons with disabilities. The policy brief proposes recommendations informed by the principles of limited guardianship and mutual decision-making under the RPWDA, besides recommending additional safeguards for sensitive personal data and digital accessibility.[19]

---

[18] This includes the Personal Data Protection Bill, 2018 and the Personal Data Protection Bill, 2019.

[19] The methodology employed in this policy brief includes secondary data, as well as interviews with stakeholders. Insights from our stakeholders have been anonymously attributed. Our stakeholders include Shivangi Rai, Deputy Coordinator and Shefali Malhotra, Research Consultant, Centre for Health, Equity, Law and Policy; Maitreya Shah, Tech Policy Fellow at UC Berkeley, and an Affiliate at the

To this end, the policy brief seeks to facilitate autonomy for persons with disabilities to be exercised within better safeguarded support mechanisms. The policy brief concludes by proposing certain recommendations which may be incorporated through legislative amendments to the DPDPA and delegated legislation.

Part 2 of this policy brief will detail the problems that will likely arise for persons with disabilities under the DPDPA. Part 3 will propose recommendations to ensure the DPDPA and delegated legislation account for these problems, and Part 4 will conclude the policy brief.

2. KEY PROBLEMS IN THE DPDPA

Certain key problems in the DPDPA, highlighted below, dilute the rights of persons with disabilities:

- Lack of definition of 'persons with disabilities' and challenges in interpreting guardianship in relation to the DPDPA
- Lack of autonomy of persons with disabilities
- Lack of recognition of sensitive personal data
- Lack of provision on digital accessibility in the DPDPA

Berkman Klein Center for Internet and Society at Harvard University; and Rahul Bajaj, Co-Founder, Mission Accessibility, Senior Associate Fellow, Vidhi Centre for Legal Policy, and Adjunct Faculty, BML Munjal University School of Law. The analysis in this policy brief is limited by two factors. Firstly, the lack of primary data, including informed first-person narratives from users with disabilities on data breaches. Hence, the analysis has been backed with insights and lived experiences from disability rights and Internet governance stakeholders, some of whom are persons with disabilities themselves. Secondly, the scope of the policy brief is limited to the challenges faced by persons with disabilities in the context of the DPDPA. It does not explore access to Internet infrastructure/inequitable distribution of resources as a reason for persons with disabilities relying on others to navigate the Internet.

2.1. Lack of definition of 'persons with disabilities' and challenges in interpreting guardianship in relation to the DPDPA

The lack of a definition of persons with disabilities in the DPDPA creates confusion about which category of persons with disabilities from the diverse spectrum of disabilities falls within the ambit of the provisions carved out in the DPDPA. While children have been defined under the DPDPA, persons with disabilities have not been defined under this law.

Presumably, persons with disabilities would have to be defined as per the provisions of the RPWDA. The definition of persons with disabilities in the RPWDA encompasses individuals with all classes of disabilities, ranging from mental and psycho-social disorders, to locomotor disorders.[20] The RPWDA also provides classifications for those with benchmark disability[21] and those with high support needs, who are likely to need some form of intensive support to participate in all areas of life.[22]

The absence of a definition of persons with disabilities in the DPDPA is a missed opportunity to rectify the limitations of the RPWDA in an increasingly digitised world. The DPDPA could have provided greater clarity with regard to the degree of support a person with disability needs from their lawful guardian. The DPDPA could have also established the extent to which the lawful guardian could exercise rights as data principal.

Under the RPWDA, a lawful guardian is appointed based on the inability of the person with disability to make "legally binding decisions."[23] However, as previously described, persons with disabilities are a heterogeneous group. Persons with disabilities who are unable to take larger consequential legally binding decisions, can also show

[20] The Rights of Persons with Disabilities Act, 2016, s 2(s).

[21] Person with benchmark disability means a person with not less than forty percent of a specified disability, as defined under the Rights of Persons with Disabilities Act, 2016, s 2(r).

[22] The Rights of Persons with Disabilities Act, 2016, s 2(t).

[23] The Rights of Persons with Disabilities Act, 2016, s 14(1).

heterogeneity in other decision-making abilities.[24] When this decision-making ability is considered in conjunction with both the offline world as well as cyberspace, a legally binding decision could range from a complex act of transfer of property to a simple act of subscribing to audio-visual storytelling on an online platform. A person with disability who is unable to make a decision about the former but capable of making the second decision would still be classified as "unable to take legally binding decisions" and thus irrespective of the range of decision-making capacities, would be appointed a lawful guardian under the RPWDA.

While the RPWDA provides for a lawful guardian to be appointed for a specific period and a specific decision or situation such as for complex banking and financial purposes, the DPDPA is agnostic to this specific purpose. As a result, such a lawful guardian could also make decisions around persons with disabilities subscribing to content from online platforms. The DPDPA gives the lawful guardian the same rights as the data principal, allowing the lawful guardian to make decisions for which the person with disability may not require a lawful guardian to step in. This is where the DPDPA had the scope to tailor the requirement for a lawful guardian to step in as data principal, by presenting a streamlined definition of persons with disabilities for the digital domain.[25]

Capabilities in the physical world may also operate differently than in the digital domain. Assistive Technologies ("AT") such as screen readers and speech recognition software enable persons with disabilities to perform functions for which they previously relied on human assistance. The RPWDA does not take into account the considerations of the digital domain in classifying disabilities and providing

[24] For nuances and heterogeneity in decision-making capacity, see Vidhi Centre for Legal Policy, 'Decision-making for persons with impaired capacity' (March 2021) <https://vidhilegalpolicy.in/research/decision-making-for-persons-with-impaired-capacity/> accessed 29 November 2024.

[25] According to Stakeholder 2, "Most seemingly inconsequential decisions might have a legally binding character. For example, signing up for a privacy policy would be a legally binding decision - would the consent of the guardian and not of the persons with disabilities be taken in this case? That could not have been the legislative intent because it would then frustrate the RPWDA. This could be an oversight in figuring out the possibility of misuse of power by a lawful guardian, which could be resolved by framing Section 9 in a tightly worded manner."

guardianship. The DPDPA fails to bridge this gap between the limitations of the RPWDA and the digital needs of persons with disabilities.

2.2. Lack of autonomy of persons with disabilities

(i) Processing of data of children and persons with disabilities clubbed together

Section 9 of the DPDPA clubs children and persons with disabilities[26] together. The rationale behind this clubbing is unclear.[27] The provision requires lawful guardians to provide verifiable consent on behalf of the person with disability (in cases where a lawful guardian has been appointed). This is similar to what the provision lays down for parents and children. By clubbing persons with disabilities with children in Section 9 in this manner, and equating the role of lawful guardians with parents, the DPDPA infantilises persons with disabilities. The DPDPA makes an unfair assumption that both children and persons with disabilities with lawful guardians are homogenous groups of individuals, unable to meaningfully navigate the Internet. This assumption may impact how the role of lawful guardians, which is currently equated with parents, is envisioned by the DPDPA. This can vastly undermine the dignity of persons with disabilities, diminishing self-esteem and perpetuating social exclusion.[28]

(ii) Persons with disabilities exercise restricted decision-making as data principals

The DPDPA has taken a step towards inclusivity by including the concept of guardianship for persons with disabilities. However, the DPDPA fails to operationalise

[26] This refers to persons with disabilities with lawful guardians. The DPDPA may not, for example, include persons with disabilities with visual/other physical impairment alone, who can make legally binding decisions.

[27] According to Stakeholder 1, "One reason for this may be that the concept of guardianship may be borrowed from the Guardians and Wards Act, 1890, which was meant for children."

[28] Hari Srinivasan, 'Dignity Remains Elusive for Many Disabled' (*Psychology Today*, 13 July 2023) <https://www.psychologytoday.com/intl/blog/giving-voice/202307/dignity-remains-elusive-for-many-disabled-people> accessed 29 November 2024.

this as a form of support. The intended purpose of the law may have been to support persons with disabilities by onboarding lawful guardians alongside persons with disabilities within the broader consent framework. Instead, Section 9 of the DPDPA allows lawful guardians to give verifiable consent on behalf of persons with disabilities for the processing of data. This provision does not account for a mechanism for mutual decision-making between the person with disability and their lawful guardian. This is contrary to the principles of limited guardianship and mutual decision-making envisaged in the RPWDA.

Guardianship, as envisioned by the RPWDA, is meant to offer support to persons with disabilities in the decision-making process. This is operationalised through Section 14(1) of the RPWDA, which provides the concept of limited guardianship. Limited guardianship is a system of joint decision-making based on mutual trust between the persons with disabilities and their lawful guardian, which is restricted to a specific decision and subject to the prerogative of the persons with disabilities. Section 14(2) deems every guardian appointed for a person with disability under any law a limited guardian from the commencement of the RPWDA.

The DPDPA acknowledging that persons with disabilities may require support with decision-making is well-intentioned. However, the role of the lawful guardian should have been more in terms of assistance and not a complete transfer of decision-making power. The severity of a disability is a spectrum, which should determine the degree of support a person with disability needs from their lawful guardian. Safeguards are necessary to prevent a lawful guardian from overstepping by imposing their will over the person with disability's decision to consent to data processing, or by making unilateral decisions even where a conflict of interest may arise.

The DPDPA has no safeguards for abuse of power by a lawful guardian. The scope of abuse of power by the lawful guardian stems from the broad definition[29] of 'data principal' in the DPDPA. Inclusion of a lawful guardian in the definition of 'data

[29] According to Stakeholder 2, "the term "includes" in 2(j)(ii) carries a lot of weight. As per the rules of interpretation, 'includes' is actually 'means' and whenever "includes" is used, it indicates that you have to include necessarily and not selectively interpret a guardian only when a person with disability is incapable of making decisions on their own. DPDPA does not tell you what are the circumstances in which you can have a lawful guardian."

principal' in the DPDPA erodes the distinction between the person with disability and their lawful guardian as separate entities, which undermines the agency of a person with disability as a data principal. By including lawful guardians of persons with disabilities in the definition of data principal, without adequate safeguards, the DPDPA has created a far more extensive role for lawful guardians than was envisioned in the RPWDA.

(iii) Lack of exemptions to requiring verifiable consent

The DPDPA currently does not provide exemptions - by the government identifying certain exempt data fiduciaries - to the requirement of verifiable consent from lawful guardians. The absence of such exemptions is flawed because this leaves minimal scope for circumstances in which it may not be necessary to require verifiable consent from lawful guardians, in order to process data. This could include, for instance, accessing a digital encyclopaedia.

The absence of exempted data fiduciaries and digital services can also be particularly harmful in cases where a conflict of interest may arise and the lawful guardian may not consent to processing. This is especially significant because the DPDPA currently provides for the government to classify certain websites which will not need parents or lawful guardians to provide verifiable consent for children, but no such option has been provided for persons with disabilities with lawful guardians.[30] This is an example of how, in addition to clubbing persons with disabilities with children, the law also grants greater autonomy to children.

Previous iterations of the DPDPA,[31] while discussing verifiable consent in terms of children, envisioned exempted websites to include those providing services to children like counselling and child protection. This can be correlated to the question of whether persons with disabilities will be able to access certain limited digital services which are exempted from requiring verifiable consent from the lawful guardians. Requiring

[30] The Digital Personal Data Protection Act, 2023, s 9(4).

[31] Namely, the Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2019 and the Data Protection Bill, 2021.

verifiable consent from lawful guardians of persons with disabilities limits digital avenues to independently access information or pathways pertaining to the right to complain against the lawful guardian. This could include access to online communities for persons with disabilities, which can equip them with a better understanding of their rights. Such communities can also provide assistance in directing persons with disabilities to online helplines and provide guidance in submitting a formal complaint against their lawful guardian offline. A lack of digital services exempted from collecting verifiable consent would also hinder persons with disabilities with lawful guardians who also have hearing or speech disabilities. This is a notable concern because it does not allow persons with disabilities to fully exercise rights guaranteed to them. For instance, the **Goa Rights of Persons with Disabilities Rules, 2018** in particular allow persons with disabilities themselves to report their lawful guardian for abuse (physical, emotional or sexual) and/or neglect.[32]

Section 9 can also negatively impact persons with disabilities who have been abused or sexually assaulted by a third party like another family member. In certain cases, including instances where the lawful guardian is also a family member of the person with disability, the lawful guardian might not want the person with disability to submit a sexual abuse complaint.

Essentially, this policy brief contends that certain digital services should be exempted from mandatory verifiable consent in cases where the potential for abuse of power by the lawful guardian is higher. The Recommendations section of the policy brief further explores how this can be envisioned.

2.3. Lack of recognition of sensitive personal data

The DPDPA replaces Section 43A of the IT Act and the SPDI Rules, but does not contain any provisions identifying or defining SPD. As discussed previously, previous iterations of the DPDPA included a separate category and safeguards for SPD, but have been done away with in the current framing of the DPDPA.

[32] The Goa Rights of Persons with Disabilities Rules, 2018, Rule 4(3).

The authors are cognisant that there are criticisms and counter approaches to the categorisation of personal data as sensitive and non-sensitive. For example, Solove argues that the categorisation of personal data as sensitive can often be arbitrary. He contends that all personal data can be sensitive in nature, and instead proposes categorisation on the basis of harm and risk.[33] Similarly, Moerel had contended that it was the manner in which personal data is used, as opposed to its inherent nature, that could be sensitive.[34] She refers to instances where even non-sensitive personal data may become sensitive based on the impact it has on the data principal in the event of data breach.[35]

However, India's data protection framework is still at a nascent stage. Keeping this in mind, the removal of the category of SPD has led to uncertainty in the Indian policy ecosystem regarding how sector-specific data which may be more vulnerable can be adequately safeguarded. For instance, a distinction for SPD as a separate category allows for certain safeguards to be put in place against the overbroad processing of SPD. The lack of a separate provision on SPD could expose sensitive data to misuse and breach, resulting in the significant infringement of rights of individuals, including equality, non-discrimination and privacy.[36]

While SPD is vulnerable for all categories of individuals, breaches of such data can be particularly vulnerable for persons with disabilities.[37] It is pertinent to note here that this includes all persons with disabilities, and not merely those who have been appointed a lawful guardian under Indian guardianship frameworks. Such breaches

---

[33] Daniel Solove, 'Data is what data does: Regulating based on Harm and Risk instead of Sensitive Data' [2024] 118 Northwestern University Law Review 1081.

[34] International Association of Privacy Professionals, 'GDPR conundrums: Processing special categories of data' (*International Association of Privacy Professionals*, 12 September 2016) <https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/> accessed 29 November 2024.

[35] Ibid.

[36] General Data Protection Regulation, Recital 52.

[37] Privacy International, 'Protecting persons with disabilities in a digitised world' (*Privacy International*, 29 November 2023) <https://www.privacyinternational.org/long-read/5170/protecting-persons-disabilities-digitised-world#:~:text=In%20essence%2C%20data%20from%20individuals,respected%20during%20collection%20and%20processing.> accessed 29 November 2024.

will likely dilute confidentiality rights guaranteed to persons with disabilities under the **Mental Healthcare Act, 2017 ("MHA")**.[38] Moreover, personal data breaches could lead to discrimination (in terms of social welfare, healthcare, employment) and harassment of persons with disabilities, affecting their right to equality and non-discrimination[39] and right to protection from cruelty and abuse under the MHA[40] and the RPWDA.[41]

Privacy protections act as a shield for human dignity and personal autonomy.[42] Personal autonomy is intrinsically linked with safeguarding one's identity. The absence of safeguards protecting identifying information results in profiling through intensive processing of personal data. This further de-individualises the data subject (in this case a person with disability), thus reducing their autonomy.[43] Personal autonomy can thus be achieved when the data subject has more control over personal data, for which consent of the data subject is key.[44]

2.4. Lack of provision on digital accessibility in the DPDPA

There are clear examples, in both legislation and case law, of the need to bolster digital accessibility for persons with disabilities. Section 42 of the RPWDA mandates that ICT

---

[38] The Mental Healthcare Act, 2017, s 23; the Mental Healthcare Act, 2017, s 24. Stakeholder 3 highlighted the significance of a lack of safeguards for a separate category of sensitive personal data in regard to persons with disabilities - "Public health professionals are increasingly supporting digitisation in the Healthcare industry. This could mean acquiring and then commercialising huge data sets of health data of persons with disabilities which could then be shared with the private sector. This would expose persons with disabilities to more harm."

[39] The Mental Healthcare Act, 2017, s 21; The Rights of Persons With Disabilities Act, 2016, s 3.

[40] The Mental Healthcare Act, 2017, s 20; The Rights of Persons With Disabilities Act, 2016, s 6-7.

[41] According to Stakeholder 2, "The lack of categorisation of sensitive personal data results in a lack of additional safeguards for health and genetic data of persons with disabilities. Disability itself should have a privacy protection - if the disability is disclosed through an act of data fiduciary without the consent of the persons with disabilities then that needs to be addressed explicitly by a provision in the law."

[42] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 12.

[43] Shraddha Kulhari, *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity* (1st edn, Nomos Verlagsgesellschaft mbH 2018) 23–37.

[44] Ibid.

be made available to persons with disabilities in accessible format and universal design. Additionally, in *Rajive Raturi v Union of India*,[45] the Supreme Court issued directions to make government websites accessible to persons with disabilities. ICT accessibility is defined as a key component of accessibility rights under Article 9 of the UNCRPD.

Digital accessibility is a precursor to persons with disabilities giving meaningful consent.[46] This is because easily navigable features on a digital interface grant autonomy to the persons with disabilities and also prevent any erroneous data entry that could jeopardise the security of their personal data. Digital accessibility would thus enable persons with disabilities to give their consent independently as far as possible. Digital accessibility would benefit persons with disabilities who have lawful guardians under Section 14 of RPWDA. It would also additionally be advantageous for persons with disabilities without lawful guardians who wish to function independently but struggle due to inaccessible interfaces on the Internet.[47]

ICT in accessible format would also mean that data fiduciaries would be compelled to provide simpler consent mechanisms. Instead of simplifying the consent mechanism, Section 9 of the DPDPA currently shifts the onus of giving consent from the persons with disabilities to their lawful guardian. This disincentivises data fiduciaries from making privacy policies that are accessible to persons with disabilities.[48]

---

[45] *Rajive Raturi v Union Of India*, AIRONLINE 2018 SC 544.

[46] 'Accessibility is Privacy and Security' (*Bureau of Internet Accessibility*, 2 July 2019) <https://www.boia.org/blog/accessibility-is-privacy-and-security> accessed 29 November 2024.

[47] According to Stakeholder 3, "It is important to first increase accessibility for PWD, before envisioning a guardian in the decision-making process."

[48] According to Stakeholder 2, "This is a big issue we face in our work (to make apps and websites more accessible). Platforms insist that persons with disabilities take someone else's help to use them when we point out a lack of accessibility features on the platforms. The data protection framework can lead to this happening even more since the consent of the guardian is kept at the same footing as that of the person with disability. Platforms may circumvent the consent of the persons with disabilities to take the guardian's consent for processing data."

3. RECOMMENDATIONS

Addressing the issues listed above, the policy brief proposes certain recommendations to be incorporated through legislative amendments to the DPDPA and through Rules to supplement the DPDPA. While certain recommendations are informed by the provisions of the RPWDA, other suggestions stem from provisions of other domestic legislations in India, as well as best practices from foreign jurisdictions.

3.1. Separate provision pertaining to persons with disabilities

The DPDPA clubs children and persons with disabilities in the same clause, i.e., Section 9, which is titled "processing of personal data of children." As indicated above, clubbing persons with disabilities with children can be restrictive and infantilising for the former, and processing of data of persons with disabilities should, therefore, be dealt with separately. The DPDPA should not apply the same standards of obtaining verifiable consent for both persons with disabilities with lawful guardians and children. Consequently, to protect against infantilisation and safeguard the dignity of persons with disabilities, the DPDPA should incorporate a separate provision for persons with disabilities through legislative amendment.

It is critical that such a decoupling of persons with disabilities and children in the form of a separate provision is also accompanied by a definition of persons with disabilities for the purposes of this law.

Moreover, it is worthwhile to consider expanding the scope of persons with disabilities in the digital domain beyond the purview of the definition of persons with disabilities provided under the RPWDA. The current definition is restricted to include long-term physical, mental, intellectual or sensory impairment.[49] However, cases may arise where digital assistance will also be required by those who have short-term or temporary disability, and have been issued temporary disability certificates for the same.[50] To accommodate these nuances, it's imperative that the DPDPA be amended

[49] The Rights of Persons with Disabilities Act, 2016, s 2(s).

[50] As under the *Guidelines for evaluation of various disabilities and procedure for certification.*

to imbue a consultative framework for providing assistance to such individuals as well, in a manner that retains their autonomy and incorporates their wishes. Further directions on how this framework is to be operationalised must be delineated under the DPDP Rules.

3.2. Include safeguards to prevent abuse of power by lawful guardian

The DPDPA, through delegated legislation, must include safeguards for persons with disabilities before allowing their lawful guardians to step in as data principals. These safeguards should include: provisions for removal of lawful guardians as data principals to prevent undue influence on persons with disabilities and limited guardianship with mutual decision-making.

(i) Removal of lawful guardian as data principals

The DPDPA does not have any specific safeguards to protect persons with disabilities from undue influence by their lawful guardians while consenting to the processing of data. However, the extant framework on persons with disabilities provides for removing lawful guardians on various grounds. The National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999, provides for the removal of the lawful guardian on grounds of abuse and neglect.[51] Some states like Karnataka[52] and Goa[53] have regulations in place to adequately safeguard a person with disability from undue influence by a lawful guardian. For instance, the **Karnataka State Rights of Persons with Disabilities Rules, 2019 ("Karnataka RPWD Rules")** provide for the removal of a lawful guardian in cases of non-fulfilment of obligations, abuse, misappropriation, or any other genuine reason. It could be useful for the DPDPA to operationalise these

[51] The National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999, s 17. The procedure for removal of the lawful guardian is provided under Rule 17 of The National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Rules, 2000.

[52] The Karnataka State Rights of Persons with Disabilities Rules, 2019.

[53] The Goa Rights of Persons with Disabilities Rules, 2018.

safeguards - for example, through mechanisms for removal by the Data Protection Board.

(ii) Limited guardianship and mutual decision-making

The essence of limited guardianship and mutual decision-making between persons with disabilities and their limited guardian, which is inbuilt in the RPWDA, is not reflected in the DPDPA. Firstly, this is because of the overbroad definition of data principal in the DPDPA, which does not distinguish persons with disabilities from their lawful guardians. Secondly, there is a lack of a consultative framework between the person with disability and their lawful guardian for the purpose of consenting to data processing under Section 9.

There is a need for the DPDPA to reimagine the person with disability as the central decision-maker and their lawful guardian as an individual offering support in the decision-making process. To achieve this, the policy brief recommends that the incoming DPDP Rules to the DPDPA be informed specifically by the Karnataka RPWD Rules, the New Drugs and Clinical Trial Rules, 2019, and the UNCRPD.

To illustrate, under the Karnataka RPWD Rules, while appointing a limited guardian, the opinion of a person with disability is taken into consideration, in cases where the person with disability is in a position to give their opinion.[54] The purpose and period of guardianship, not exceeding 5 years,[55] further determine the appointment of a limited guardian. The limited guardian, wherever possible, is mandated to consult the person with disability before taking a legally binding decision on their behalf[56] which is in the best interest of the person with disability.[57] The Karnataka RPWD Rules require limited guardians to report how they are fulfilling their obligations towards the person with disability.[58] These mechanisms illustrate the principles behind

[54] The Karnataka State Rights of Persons With Disabilities Rules, 2019, Rule 6(11)(ii).

[55] The Karnataka State Rights of Persons With Disabilities Rules, 2019, Rule 6(11)(iv).

[56] The Karnataka State Rights of Persons With Disabilities Rules, 2019, Rule 6(7).

[57] The Karnataka State Rights of Persons With Disabilities Rules, 2019, Rule 6(8).

[58] The Karnataka State Rights of Persons With Disabilities Rules, 2019, Rule 6(15).

operationalising mutual decision-making between persons with disabilities and their lawful guardians, and could also provide guidance for shaping mutual decision-making between a person with disability who is a data principal, and their lawful guardian under the DPDPA.

Similarly, consider for example, the New Drugs and Clinical Trial Rules, 2019. These Rules stipulate that written informed consent for any involvement in clinical trials should be obtained from the parent or legal guardian. However, all minors are also required to be additionally informed about the study in accessible and comprehensible language.[59] Moreover, the Rules provide for minors and adolescents to consent to and sign separate assent forms in addition to the consent provided by their parents or legal guardians.[60] Such a provision can be a starting point for envisaging a verifiable consent framework with mutual decision-making for persons with disabilities. One way this can be operationalised by the DPDPA would be through accessible notice and privacy policies being provided to persons with disabilities, irrespective of whether they have a lawful guardian or not.

A consultation mechanism that reflects mutual decision-making under the DPDPA must be aligned with the principles laid down under the UNCRPD.[61] These principles have been enshrined in the RPWDA, which was enacted to give effect to the UNCRPD in the Indian framework.[62] The lawful guardian acting as the data principal on behalf of the person with disability must also consider the best interests of the person with disability, along with previous and ongoing wishes of the person with disability.[63] This

[59] IIIrd Schedule, New Drugs and Clinical Trials Rules, 2019.

[60] Ibid.

[61] As under Article 3, United Nations Convention on the Rights of Persons with Disabilities, these principles include individual autonomy, respect, inclusion, accessibility and the freedom to make independent choices impacting one's life.

[62] According to Stakeholder 1, "No one has an exact picture of what such a consultation mechanism would look like. However, the process, whether through informed consent or supported decision-making, has to be rooted in disability justice. It involves doing away with the initial assumption that persons with disabilities need protection from the government or society. Such a consultation mechanism requires addressing the nuances of different disabilities, especially gradations within the same disability, in cases of degenerative disability."

[63] The Mental Healthcare Act 2017, s 17.

can be operationalised through Section 6 of the DPDPA. Although Section 6 enables lawful guardians who are acting as data principals on behalf of persons with disabilities to give consent which is "free, specific, informed, unconditional and unambiguous," persons with disabilities themselves should be given a similar right to share in the informed consent-giving process by disseminating equal and adequate information to them.

There is no single, straightforward way of operationalising a mutually consultative mechanism to obtain informed consent from a person with disability, within a data protection framework. Since the DPDPA is unique in terms of specifically including persons with disabilities in the data protection framework, precedents from other jurisdictions on operationalising obtaining consent from persons with disabilities are rare. However, as a step toward developing such a mechanism, it is important for the DPDPA to recognise limited guardianship and mutual decision-making as rights in the extant disability justice framework. This will equip persons with disabilities with a recourse to obtain a remedy in cases where their rights as data principals have been infringed upon by their lawful guardians.

3.3. Limited exceptions for mandatory verifiable consent

Under the DPDPA, the government can prescribe certain data fiduciaries which would not require verifiable consent from parents of children before data processing. A similar allowance must be made for persons with disabilities as well.

According to the **Goa Rights of Persons with Disabilities Rules, 2018,** persons with disabilities themselves may submit a complaint of abuse or neglect against the lawful guardian appointed.[64] However, a person with disability would be restricted from doing so if a data fiduciary requires verifiable consent from their lawful guardian, as illustrated previously. For this reason, certain data fiduciaries must be exempted from obligatory verifiable consent collection from the lawful guardian. Such

[64] Under these Rules, abuse constitutes physical or sexual abuse, as well as misappropriation or misutilisation of the property of the person with disability. This provision includes solitary confinement, chaining of the person with disability; beating or treating a person with disability resulting in bruises, skin or tissue damage, sexual abuse; long deprivation of physical needs such as food, water and clothing and misappropriation or misutilisation of the property of the person with disability.

exemption will provide safeguards for persons with disabilities informed by guardrails already guaranteed in India's disability rights framework.

In addition to including persons with disabilities within the DPDPA, India is the only jurisdiction that requires data fiduciaries to obtain verifiable consent from the lawful guardians of persons with disabilities. Therefore, while looking at best practices for exemption of digital services from obtaining verifiable consent, unfortunately only mechanisms that have been envisioned with regard to children's consent, both in India and abroad, can be considered.

Previous iterations of the DPDPA,[65] while borrowing heavily from the General Data Protection Regulation ("GDPR"), had exempted data fiduciaries offering counselling or child protection services to children from the obligation of obtaining consent from the parents or lawful guardian of the child. The GDPR broadly lays down that such consent of a parental authority would not be required in cases where preventive or counselling services are offered directly to a child.[66] Similarly, the framework under the Children's Online Privacy Protection Act, 1998 ("COPPA") in the United States of America also provides some clarity in terms of limited exceptions for verifiable parental consent. The COPPA provides certain categories of "operators" (which may be considered to be the equivalent of "data fiduciary" under the COPPA) and includes certain parameters for these operators to be exempted from collecting verifiable consent from parents, including the protection of children's safety.[67]

In a similar vein, the DPDPA must be amended to provide for exemptions for verifiable consent, allowing persons with disabilities to access certain limited digital services without any mandatory verifiable consent from their lawful guardian. The nature of these digital services and data fiduciaries can be provided under the DPDP Rules. This would include digital services adequately and accurately informing them about sexual

---

[65] This includes the PDP Bill, 2018, the PDP Bill, 2019 and the Data Protection Bill, 2021.

[66] General Data Protection Regulation, Recital 38.

[67] What may be of concern, however, is that the COPPA, in some cases, still requires websites or online services to subsequently give notice to parents of the personal data that has been collected from the children. 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' (*Federal Trade Commission)* <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business> accessed 29 November 2024.

and reproductive health, accessible information about human rights, and about rights especially vested with persons with disabilities. Additionally, digital services that help persons with disabilities exercise their rights by providing persons with disabilities with access to mental health services like counselling services and helplines to report abuse must also be included within this ambit.

These exempted digital services must be presented in a clear and unambiguous format. This could look like a table or schedule enlisting the kind of data fiduciary as well as laying down how long such data may be stored. Additionally, special terms for sharing of such data collected without consent from the lawful guardian, can also be included.

3.4. Reinstating the category of Sensitive Personal Data and associated safeguards

As discussed in previous sections, we acknowledge that criticisms of SPD categorisations may have some merit. However, considering the incipient stage of India's data protection framework, and the unique privacy challenges faced by persons with disabilities, it becomes necessary to prescribe higher standards for certain types of data. This includes sensitive sector-specific personal data like health and finance, that is especially vulnerable for persons with disabilities. Personal data of persons with disabilities is particularly sensitive in nature because it can reveal information pertaining to disability, opening them up to potential discrimination and stigmatisation in healthcare, or employment. Reinstating the category of SPD through legislative amendment would not only define SPD (including the disability status of persons with disabilities), but also provide for additional safeguards for SPD, as previously envisioned. For instance, the Personal Data Protection Bill, 2018 had attempted to safeguard against overbroad processing of SPD. The provisions stated that the processing must be based on explicit consent, for certain functions of the State, and for prompt action, amongst others. Reinstating stringent grounds for the processing SPD will go a long way in ensuring greater security for such SPD of persons with disabilities.

It is also imperative to treat verifiable consent pertaining to this sensitive personal data as sensitive data in its own right.[68] For example, the New Drugs and Clinical Trial Rules, 2019 stipulate that in anti-HIV clinical trials, only audio recordings of the informed consent process would be maintained to prevent discrimination and harassment due to the stigmatised nature of these illnesses.[69] This is relevant because it recognises that consent itself can be sensitive in nature. This could translate to the digital domain in a situation where a person with disability and/or their lawful guardian acting on their behalf, accesses an online portal for information pertaining to HIV treatment. In this situation, the consent they have provided for their data to be processed may be sensitive in its own right. This is because an HIV diagnosis may be potentially inferred when an individual seeks out HIV care and treatment details. Although this may not be a perfect solution, consent collected in relation to SPD for persons with disabilities may also be considered as a subset of SPD.

3.5. The DPDPA should be reconciled with Section 42 of RPWDA

Data privacy for persons with disabilities cannot be achieved without digital accessibility. Hence, the DPDPA, through legislative amendment, must include a provision that is informed by the accessibility mandate under Section 42 of RPWDA,[70] by placing necessary obligations on data fiduciaries to include accessibility features in their consent mechanisms.[71] This could be included by inserting a clause within Section 5 of the DPDPA, similar to Section 5(3) of the DPDPA, which states the languages in which the Data Fiduciary shall give the Data Principal the option to access the contents of the notice. Under this new provision, data fiduciaries will also be

[68] This would mean that SPD would include not only health data, etc. of persons with disabilities, but also verifiable consent obtained from their lawful guardians, where consent has been provided for processing of data that could be sensitive in nature.

[69] IIIrd Schedule, New Drugs and Clinical Trials Rules, 2019.

[70] Section 42, RPWDA, 2016 mandates that the government should ensure that audio, print and electronic media are available to persons with disabilities in accessible formats, and electronic goods and equipment are available in universal design.

[71] According to Stakeholder 2, "Accessibility of data is as important as its privacy. There should be more accessibility in the data processing management. While processing data, organisations must abide by reasonable accommodation norms. Accessibility of notice is one facet, but the portal on which the consent is sought itself should be accessible."

required to ensure that notice and consent mechanisms ensure accessibility standards and are compatible with assistive technology.

Rules may also be framed by referring to the directions issued by the Supreme Court to make government websites accessible to persons with disabilities in *Rajive Raturi v Union of India*.[72] To this extent, the DPDP Rules can provide further guidelines on the kinds of accessibility features data fiduciaries must include to ensure that their consent mechanisms are more inclusive. These features may include supplementing images with text that can be read by screen-reading software, supplementing consent notices with audio-visual formats, making consent notices available in digital or electronic Braille. For instance, the United Kingdom has adopted an Age Appropriate Design Code[73] that mandates information society service providers to abide by certain standards, such as data minimisation, purpose limitation, transparency, default settings to safeguard children's privacy and avoidance of nudge techniques. Similar design codes, if adopted keeping in mind the unique needs of persons with disabilities, would make the Internet more accessible for differing capabilities.

4. Conclusion

Although a step in the right direction, the DPDPA suffers from oversight with regard to safeguarding the rights of persons with disabilities in the data protection framework. This policy brief explores how the DPDPA inadequately attempts course correction from the SPDI Rules, by onboarding lawful guardians into the framework. The policy brief examines some key issues in the DPDPA pertaining to the autonomy, safeguards and digital accessibility for persons with disabilities.

The DPDPA fails to provide a definition of 'persons with disabilities', which makes it challenging to interpret guardianship in relation to the DPDPA. The DPDPA risks

[72] Raturi (n 45).

[73] ICO, 'Executive Summary' (*ICO*) <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/executive-summary/> accessed 29 November 2024.

curbing the autonomy of persons with disabilities on the Internet. Firstly, by clubbing persons with disabilities with children in Section 9, the DPDPA infantilises persons with disabilities and undermines their dignity. Secondly, through an overbroad definition of data principal, the DPDPA denudes the scope of a mutual decision-making process between the persons with disabilities and their lawful guardians. Additionally, the DPDPA does not exempt any data fiduciaries from requiring the verifiable consent of the lawful guardian, in cases where a person with disability has been appointed one. This would make it difficult for persons with disabilities to utilise certain digital services for the purposes of accessing online helplines and counselling services for mental health, amongst many others.

Besides the risk to autonomy, the DPDPA fails to safeguard persons with disabilities from discrimination through the lack of a category of SPD with added protections. Finally, the DPDPA is insufficient in upholding digital accessibility, which becomes a barrier to persons with disabilities exercising their autonomy.

To address these concerns, the policy brief puts forth a series of recommendations. To enhance autonomy, the policy brief recommends de-clubbing persons with disabilities and children in Section 9 of DPDPA. A separate provision for processing personal data of persons with disabilities in the DPDPA must be created. Such a separate provision would include a definition of disability in relation to the digital domain providing clarity on when a lawful guardian would be required to support in the consent framework. The policy brief additionally emphasises the need for safeguards to prevent abuse of power by lawful guardians and recommends the strengthening of the mutual decision-making process based on limited guardianship and consultation mechanisms. Further, it recommends providing limited exceptions to the requirement of verifiable consent from lawful guardians of persons with disabilities. Additionally, the policy brief recommends re-introducing the category of SPD with safeguards to cater to the heightened vulnerability of persons with disabilities to data breaches. Lastly, the policy brief recommends incorporating digital accessibility, especially in regard to the envisioning of consent mechanisms in the DPDPA.

The policy brief presents an analysis of the problems in implementing autonomy, safeguards and accessibility for persons with disabilities within the DPDPA in its

current form. It is hoped that this policy brief offers pathways to solutions to policymakers through legislative amendments to the DPDPA and through the forthcoming Digital Personal Data Protection Rules. Accounting for the concerns raised in this policy brief will enable persons with disabilities to be better represented within the data protection framework.

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