May, 2024

Digital Data Protection & Consent Protocols for Persons with Disabilities: A Legal Primer

A legal primer for legal practitioners, disability rights advocates & policy makers in the context of India's Digital Personal Data Protection Act, 2023 for persons with disabilities

Below are the logos of three collaborating organizations – Chitta Initiative for Research by Pacta, Pacta & Saksham Disability

Global Data Protection Laws: Do they Account for Persons with Disabilities in the Age of Big Data Sharing?

Preface

Early research on digital data privacy, protection and consent for persons with disabilities revealed that globally, not much work has been done to understand consent and data protection for them. While extensive work, including legislative measures, has been undertaken to ensure ethical practices in the sharing of citizens' data (to protect their rights), implementation has remained a challenge.

Data-sharing practices have driven innovation, efficiency, and productivity across sectors including corporations, civil society, and governments to create targeted products, services, and policies for more than a decade.[1] However, these cutting-edge industrialization goals (disruptive technologies) are creating unintended negative consequences such as data abuse, data dominance, and anti-competitive practices leading to abuse of citizens. In this light, persons with disabilities can become more vulnerable in ways that are not yet fully anticipated.

India's new Digital Personal Data Protection (DPDP) Act, 2023, intends to protect persons with disabilities from such abusive data practices and protect their privacy rights by bringing in the consent of a lawful guardian, wherever applicable. However, the law is unclear on how it will (with regard to digital consent and data sharing)

i. protect the rights of persons with disabilities given the variation in disabilities,
ii. not infringe upon and account for the autonomy of persons with disabilities,
iii. assess the role of guardian and their assertions on the person with disabilities, and
iv. ensure the consent of the guardian is given, where applicable.

Therefore, our research aims to

a. **Document the lived experiences of persons with disabilities relative to data sharing;**
b. **Understand practices, if any, on informed consent among persons with disabilities; and**
c. **Create a repository of legislative initiatives to protect the data of persons with disabilities.**

With an end to:

inform robust, implementable practices and habits to obtain informed consent and protect the data of persons with disabilities in India.

The following legal primer fulfils the study objective (c) above and outlines comparative legal practices globally, vis-a-vis India.

[1] 'Whatever happened to the new economy?' (McKinsey Global Institution, 2002)

Table of Contents

Digital Data Protection & Consent Protocols for Persons with Disabilities: A Legal Primer

Summarizing the Context

i. Several day-to-day services such as entertainment, education, banking, healthcare, and mobility have moved online, compelling individuals to access the internet through a computer or smartphone equipped with access to the internet.

ii. We share data our data actively in the form of details such as name, age, and identification documents, and passively such as our browsing history, personal preferences, and behavior in the process of accessing digital services.

iii. Data Protection laws set out to protect a data principal against misuse of the data shared, provide data principals with clear and simple explanations of what the data collector (data fiduciary) would do with the data shared (as the data principal), and mandate that specific steps for securing personal data be implemented by the data fiduciary.

iv. There are two main obligations of a data fiduciary under a data protection law – informed consent to collect data, and reasonable measures to safeguard the data collected.

v. The United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) recognizes that persons with disabilities are entitled to full and equal enjoyment of all human rights and fundamental freedoms including accessible digital environments. Several countries that ratified the UNCRPD went on to have their independent domestic laws echoing the principle of ensuring accessible physical and digital infrastructure for persons with disabilities. India ratified the UNCRPD on October 1, 2007.

vi. While ensuring digital accessibility it is also important to recognize the right to data privacy and data protection of persons with disabilities. However, there appears to be no prior research demonstrating how the right to data privacy/ protection will be achieved. On the other hand, there exist more advanced legislative initiatives for data protection for children.

Key Highlights of Global Data Protection and Consent Laws

vii. Countries across the world have special provisions under their disability law recognizing the rights of persons with disabilities to access the internet and digital services. Additionally, country specific data protection laws accord special status to disability data shared by users digitally. Australia identifies disability data as health data and accord it the status of sensitive personal data. With such recognition, the Australia requires that the data fiduciary comply with higher security standards for such sensitive personal data. The United Kingdom, European Union, and Brazil recognize health data as a special category of data but do not explicitly define disability under health data. However, the data protection laws of India, United States, Singapore and Zimbabwe do not accord special status to disability data.

viii. Country specific data protection laws also mandate consent protocols. One aspect of consent is that, prior to collection of data, consent should be secured from the Data Principal. Such consent may be express or implied. Some countries require consent to be free, specific, informed and unequivocal under respective data protection laws. While consent is considered a significant parameter to determine the collection and use of data, countries have recognised that lengthy and incomprehensible privacy notices have led to 'consent fatigue', thereby, taking away the 'specific' and 'free' nature of consent. With such acknowledgment, data protection laws require consent notice to be simple, easy to understand and available in vernacular languages.

ix. The concept of free and informed consent meets poignant quandaries in the case of persons with disabilities. A person with disability may find it difficult to navigate through inaccessible, and lengthy privacy notices. Some countries require data fiduciaries to provide additional measures

such as interpreters, translations and other measures to enable consent. However, not all countries provide for any such accessible consent provisions for persons with disabilities.

x. Additionally, only Australia, India, and Zimbabwe have, under their respective data protection laws, provided that consent on behalf of a person with disability/incapacity to consent shall be provided by a lawful guardian/representative. Zimbabwe law requires that incapacity to consent must be proven by a physician or other person legally competent to prove incapacity. India requires that the consent of a person with disabilities must be routed through their legal guardian, regardless of the capacity of the person with disability to provide their consent. Australia, however, takes a welfare approach by requiring that a Data Fiduciary shall provide assistive resources to ensure that the capacity is maximally exercised. In Zimbabwe and Australia, the right to consent may be exercised by a parent, guardian, court/ legally appointed person, or person nominated by the data principal.

xi. India's DPDP Act provides for verifiable consent to be obtained through a lawful guardian when there is such a lawful guardian. This arrangement raises the following concerns:

a. there is no clarity if the lawful guardian refers to a guardian appointed under the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation Act (NT Act) or the Rights of Persons with Disabilities Act (RPwD Act). Guardians for persons with disabilities under these two laws play very different roles.
b. a limited guardian appointed under RPwD Act should not provide consent for data sharing, as this will amount to overreach of the guardian's powers.
c. It presupposes that all persons with disabilities who have a lawfully appointed guardian do not have the capacity to consent. It is important to define the circumstances under which the requirement to secure the consent of the lawful guardian would be required, failing which the person with disabilities should directly provide consent with reasonable accommodations.
d. It creates ambiguity on the question of - If the person with disabilities does provide consent without consent of the legal guardian, will this amount to a violation of the law? What would the implications of the override be on the person with disabilities, their data, and their guardian?
e. Disenfranchising persons with disabilities from decision-making capacity, despite the UNCRPD advocating for a paradigm shift from substituted decision-making to supported decision-making, wherein persons with disabilities are provided with the necessary support to make their own decisions.
f. It remains unclear how this provision of the act would be implemented in practice. If it entails asking a data principal whether they are a person with disability- and then proceeding to ask whether they have a lawful guardian, this will mean that additional data would have to be collected. This raises the questions:
    - Whether persons with disabilities will be comfortable with disclosing the status of their disability to private data fiduciaries?
    - Since there are no additional data protection safeguards for sensitive data such as disability data, what would be the extent of data protection afforded?

What to expect in this primer?

India passed a data protection law, the Digital Personal Data Protection (DPDP) Act, in 2023 and is set to release rules to implement the Act in June 2024. The DPDP Act has certain provisions pertaining to persons with disabilities and will impact the way the data of persons with disabilities will be collected and processed in India. Persons with disabilities constitute about 4%-8% (40-80 million) of India's population, and it is important to anticipate how the

DPDP Act will impact this large group of the population. Also, with digitisation increasingly on the rise, it is critical to keep the UNCRPD commitment under Article 9 in sight, which is towards that ensuring no person (with disability) is left behind.

This primer is intended to be used by privacy law and policy practitioners and policy makers, accessibility initiatives of civil society towards informing robust data privacy and data protection protocols for persons with disabilities in the digital sphere.

In this primer, we have compiled the provisions of the data protection initiatives of eight countries (at least one country from each continent) and compared with those of India (the DPDP Act 2023 and the Information Technology Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011 to consolidate laws and frameworks across nine jurisdictions.[2]

We contour:

1. rights of persons with disabilities in the digital medium;
2. special provisions of data privacy laws such as consent mechanisms for persons with disabilities
3. special provisions of data privacy laws such as protection of data applicable to persons with disabilities
4. challenges in the implementation of the current provisions of the DPDP Act with respect to persons with disabilities.

[2] United States, Brazil, Canada, United Kingdom, European Union, Zimbabwe, India, Singapore and Australia – see annexure 3 for selection of countries.

Why does the world need Data Protection Laws?

Do you recall having clicked on an I Agree button, on a website recently? That is because the website asked for your personal data like name, age, date of birth and the data privacy law mandates that a website must ask for your consent before it collects your data.

Several day-to-day services such as entertainment, education, banking, healthcare, mobility have moved online, compelling individuals to access the internet through a computer or smart phone equipped with access to the internet. India has a massive internet user base, ranking second only to China globally. Data from the Internet and Mobile Association of India (IAMAI) estimates around 800 million internet users in India as of 2023.[3] High number of Indian users contribute to India featuring among top three countries for users of platforms such as Facebook (Meta),[4] Google,[5] and YouTube.[6] Internet users in India have consistently increased from 524 million users in 2019 to 821 million in 2023. Video and audio OTT is the top way in which Indians are using the internet, and there are more rural users (442 million) of internet than urban users (378 million), as of 2023 (Figure 1).[7]

With increasing use of internet, there is an increased digital sharing of data, meaning that individuals users share several personal information data points such as name, date of birth, email address, phone number, address, identification details, (Aadhar, PAN, passport information etc) banking information, photograph, biometric data etc upon demand to avail paid services (booking a taxi, ordering food etc) or free digital services (email, social media accounts etc). Additionally, several other types of data such as usage patterns (what websites are browsed, what searches are done via search engine), user preferences (types of products/ content viewed/ purchased etc) and user behaviour are collected.

The data we share is intended to be used to regulate access to the service and customizing the user experience of the service. The data we share allows the service provider to gain an intimate understanding of the user and thus improve the commercial viability of the product. When personal data collected by one service provider online is combined with data collected by another service provider, it creates a very valuable database of high commercial value.

For example, Insurance companies would be willing to buy health data tracked from a running app, cardio vascular data from a health app and food ordering data to arrive at health risks that can be used to determine the insurance premium in a highly individualized manner, without a person even knowing what goes on at the backend.

Large volumes of personal data are collected by the public sector, private sector, and civil society, meaning that all the three sectors value data to make data driven decisions to drive innovation, competitiveness, economic growth, and other development metrics. In this context, a global need was felt to regulate the collection, use and storage of data. More than 130 countries (71% of

[3] 'Internet in India 2023' (Internet and Mobile Association of India, 2023)
[4] 'Leading countries based on Facebook audience size as of April 2024' (*Statista*) accessed 15 May 2024
[5] 'Google Users by Country 2024' (*World Population Review*) accessed 15 May 2024
[6] 'Leading countries based on YouTube audience size as of January 2024' (Statista) accessed 15 May 2024
[7] Annapurna Roy, 'How India is using the Internet' Economic Times (10 March 2024) 15 May 2024

countries) across the world have drafted laws to protect the individual rights over their data (Figure 2).[8]

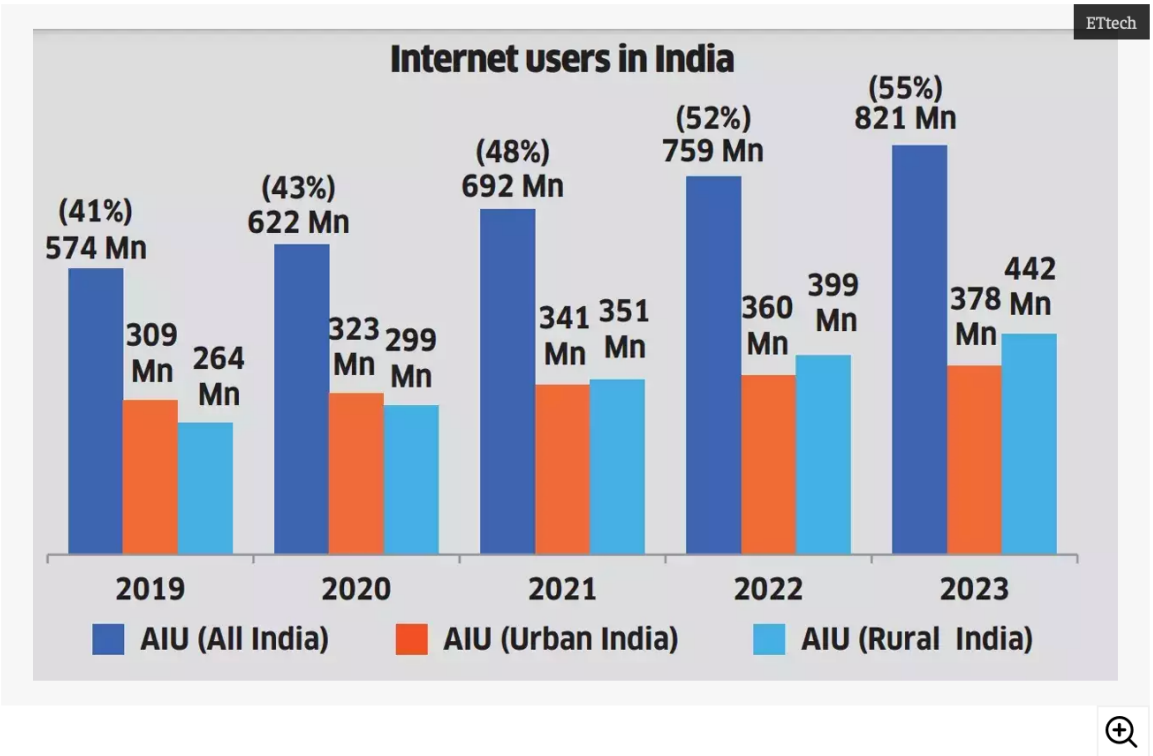

Figure 1. Internet Users in India showing that Internet users in India have consistently increased from 524 million users in 2019 to 821 million in 2023. There are more rural users (442 million) of internet than urban users (378 million), as of 2023.

[8] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) accessed 15 May 2024

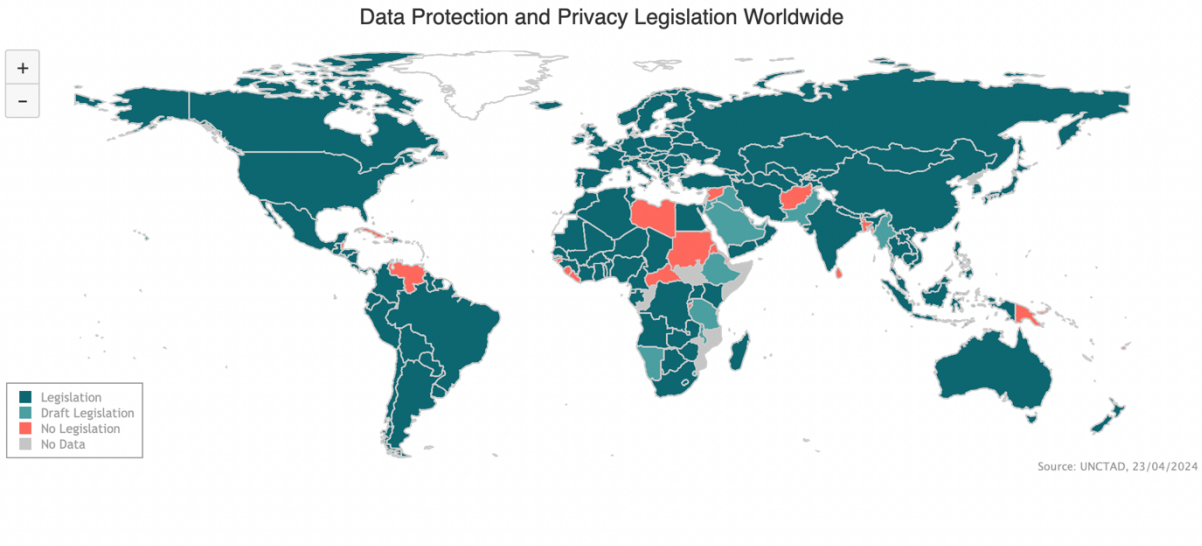

Figure 2. Data Protection and Privacy Legislation Worldwide showing that almost all countries marked in green colour have data protection legislations. This includes all North American countries, South American countries such as Brazil, Argentina and Columbia, European countries, African countries such as South Africa, Congo, and Zimbabwe, Asian Countries including India, China, Japan, and Australia and New Zealand. Countries marked in orange (Cuba, Venezuela, Belize, Haiti, Liberia, Sierra Leone, Guinea Bissau, Central African Republic, Sudan, Libya, Syrian Arab Republic, Eritrea, Bangladesh, Sri Lanka, Afghanistan, Timor Leste, Fiji, and Solomon Islands) do not have a data protection legislation.

General Concepts Under Data Protection Laws

Data Protection laws set out to protect you against misuse of the data you shared, provide you with clear and simple explanations of what the data collector (data fiduciary) would do with the data you share (as the data principal), and mandate that specific steps for securing your data be implemented by the data fiduciary.

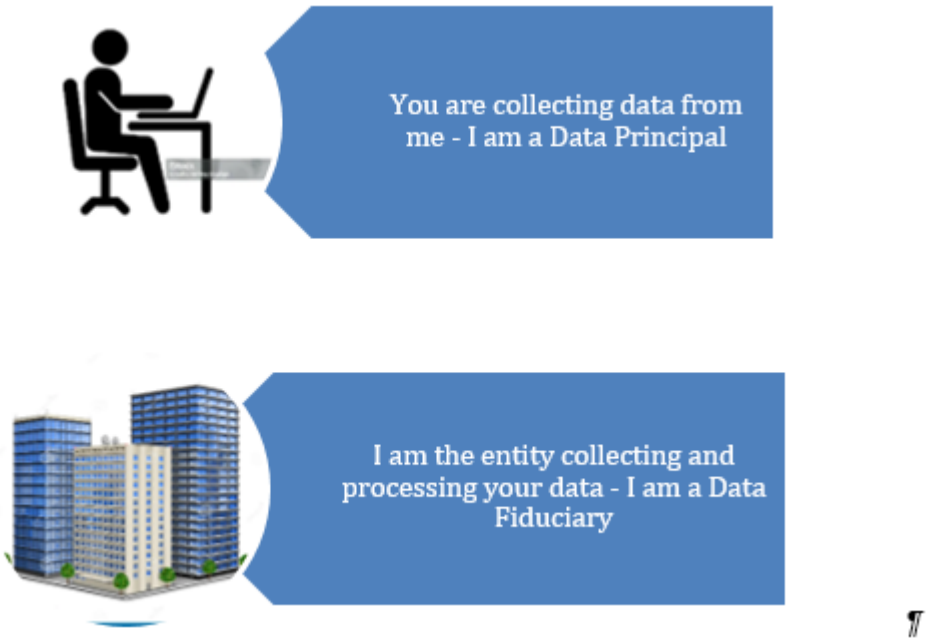

Figure 3. Understanding Who is a Data Principal and Who is a Data Fiduciary

To access digital services, one may be required to provide personal data to the service providers. Figure 4 shows the screen shots of the sign-up pages of Instagram, Swiggy (food delivery app) and The Hindu (newspaper app), each asking for personal data such as the user's name, phone number and email address to sign up for the digital services.

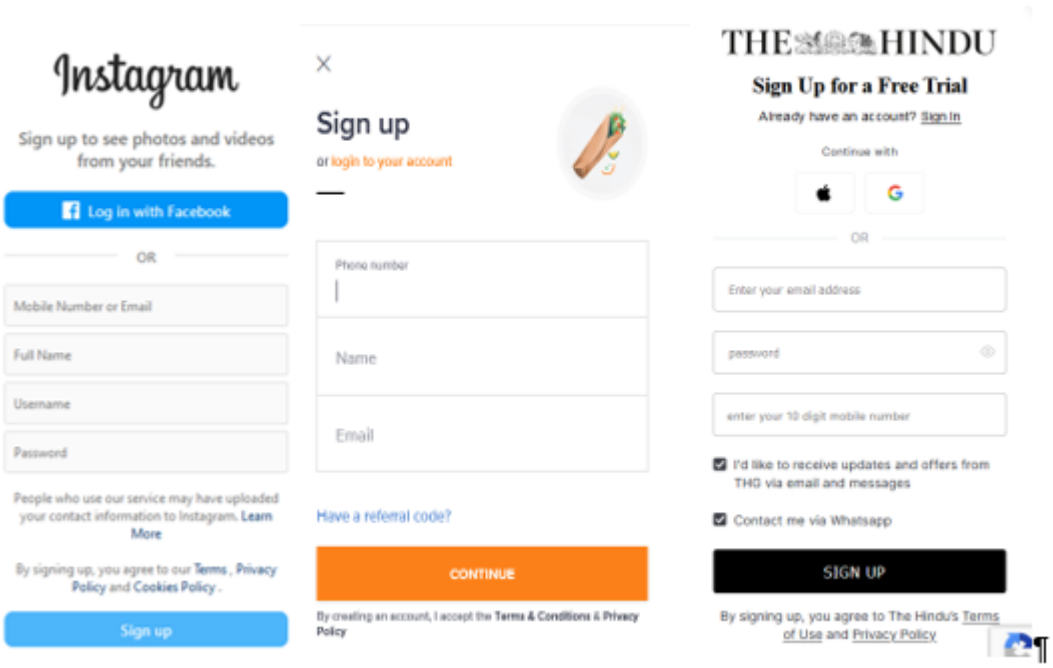

Figure 4. Screen shots of sign-up forms for Instagram, Swiggy and The Hindu.

Data protection legislations across the world provide for:

- **informed-consent-based data collection** meaning that a data principal must be aware of collection of data, the purpose for which such data is collected and how such data shall be used.
- **explicit data-protection rights** to the data principal against abusive use of data especially belonging to vulnerable populations (such as children and persons with disabilities), and special treatment to data of vulnerable populations.

Data collection and processing is expected to be preceded by taking informed consent from the data principal, as seen in figure 5.

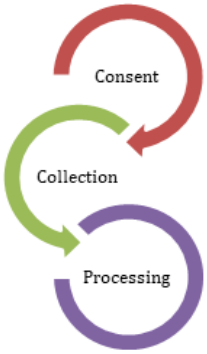

Figure 5. Flow from Data Collection to Data Processing showing that data collection and processing is expected to be preceded by taking informed consent from the data principal

Consent is secured from individuals via a series of documents such as terms of use, privacy policy and cookies policy wherein the Data Fiduciary informs the Data Principal regarding type of data collected, reason of collection of data, purpose of processing, and rights of the Data Principal.

Have you seen platforms asking you to agree to their privacy policy and terms of use while creating an account to avail services? Have you been able to read these documents and understand them? Do you usually click on I agree without reading?

The modus of securing consent can be 'express' wherein the users take a positive action of ticking the box to give consent. It may also be 'implied' wherein by signing up for services, the user is presumed to have given consent (as observed from all three sign-up forms from Figure 4 for Instagram, Swiggy and Hindu). While consent may be express or implied, laws require such consent to be free, specific, informed, and unequivocal. These terms are better explained below:

- ***Consent shall be free***
  Consent provided by the user shall not be caused by coercion, undue influence, fraud, misrepresentation, or mistake.[9] In the event services are conditional upon further processing of data that is not required for performance of services, the consent will not be considered as free.
  For example: A (hypothetical) privacy notice provides that service to buy a book will be provided only if you also consent to receiving marketing material through WhatsApp. Here, the consent to collection and processing of phone number for receiving WhatsApp notifications is not free.
- ***Consent shall be specific and informed***
  The Data Principal shall be aware of the specific purpose of collection and processing of data.
  For example: Privacy notice stating, "data will be used for any purposes" is not specific as the user does not have any information on the purpose.
- ***Consent shall be unequivocal or unambiguous***
  The privacy notice shall be clear and unambiguous.

While consent is required for data collection and processing, data protection laws across jurisdictions provide for purposes (legitimate use) under which data may be processed without the consent of the Data Principal. India's DPDP Act too carries such a provision. However, in India, data may be processed without consent of Data Principal for performance of any function by the State in the interest of security of the State.

Additionally in respect of collecting and processing of data of children or persons with disabilities who have a lawful guardian, the DPDP Act mandates that verifiable consent of the parent (of the child) or the lawful guardian (of the person with disability with such a lawful guardian) must be taken. Verifiable consent means consent that may be verified. Under the GDPR and the DPDP Act, the Data Fiduciary is expected to use available technology to verify that the consent has been given by a parent. A record of such consent provided by the parent is expected to be maintained by Data Fiduciaries.

[9] Section 14, Indian Contract Act 1872.

Box 1: Summary of Key Provisions of GDPR

The Global Data Protection Regulation 2018 (GDPR) which has inspired several other data protection legislations is based on seven key principles for the protection of personal data:[1]

a. Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
b. Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c. Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. Accuracy: Personal data shall be accurate and, where necessary, kept up to date.
e. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
f. Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with the data protection principles.

The GDPR also guides consent protocols as follows:[1]

a. Consent needs to be freely given.
b. Consent needs to be specific, per purpose.
c. Consent needs to be informed.
d. Consent needs to be an unambiguous indication.
e. Consent is an act: it needs to be given by a statement or by a clear act.
f. Consent needs to be distinguishable from other matters.
g. The request for consent needs to be in clear and plain language, intelligible and easily accessible.

Countries across the world have adapted these principles to suit their respective context and applicability.

Are Persons with Disabilities Adequately Protected Under Data Protection Laws?

Though data protection is a globally relevant conversation, there is little literature and dialogue, at the intersection of data protection, consent, and persons with disabilities. That is why this research study is significant and urgent too.

To implement data protections laws in letter and spirit, narratives on informed and meaningful consent protocols have gained momentum internationally. Despite the enactment of regulatory initiatives, meaningful implementation of consent and data protection practices remain unclear. There are currently few guardrails in law and its practise to guide the protection of the data rights of persons with disabilities, though literature has acknowledged this imperative.[10] Compared to protections for persons with disabilities and their data, the narrative pertaining to children[11] and racial minorities[12] are relatively better documented, through legislative provisions, research studies and civil society dialogue. Academic and action research literature on vulnerabilities associated with data of persons with disabilities and shortcomings of data protection frameworks (across jurisdictions) in addressing vulnerabilities of persons with disabilities remains scarce, though some countries including India have acknowledged the need for special provisions of data protection for persons with disabilities.

One explanation for scarcity of literature at the intersection of data, privacy and persons with disabilities could be that access to digital services itself remains elusive for persons with disabilities in India, due to non-compliance with prescribed accessibility standards.[13] Accessibility to ICT (Information and Communication Technology) service is global challenge, not restricted to the Indian sub-continent. Studies based in the United States[14] and United Kingdom[15] too have indicated that persons with disabilities find it difficult to access the internet and digital services.

While narratives of access to internet and ICT for persons with disabilities remain relatively well acknowledged in literature, narratives on meaningful digital/ data collection consent protocols for persons with disabilities have not been explored, even at a global level.

---

[10] Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR when vulnerable people use smart devices' [2022] International Data Privacy Law 1

[11] 'Protecting Children's Data Privacy- International Issues And Compliance Challenges' (Centre for Information Policy Leadership, 2022)

[12] Anita L Allen, 'Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform' [2022] The Yale Law Journal Forum 907

[13] Ameen Jauhar and others, 'Making the Digital Eco-System Disabled Friendly' (Vidhi Centre for Legal Policy, 2023)

[14] Michele Causey and others, 'Enhancing digital government services for persons with disabilities' (*Deloitte*) accessed 15 May 2024

[15] 'Delivering Together for Inclusive Development: Digital Access to Information and Knowledge for Persons with Disabilities' (UNESCO, 2019)

What Do Laws Say About Digital Rights Of Persons With Disabilities?

The United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) is a base framework recognizing that persons with disabilities are entitled to full and equal enjoyment of all human rights and fundamental freedoms including accessible digital environments. Several countries that ratified the UNCRPD went on to have their independent domestic laws echoing the principle of ensuring accessible physical and digital infrastructure for persons with disabilities.[16] India ratified the UNCRPD on October 1, 2007.[17]

Table 1. Countries in Our Study that have ratified the UNCRPD

Country	Ratification Status of UNCRPD
India	Yes
Australia	Yes
Brazil	Yes
Canada	Yes
European Union	Yes
Singapore	Yes
United Kingdom	Yes
United States of America	No
Zimbabwe	Yes

To see a summary of the digital accessibility provisions in the UNCRPD, please see Table 1 of Annexure 1. Additionally, Annexure 1 also carries summaries of the following frameworks which have been crucial to advance digital accessibility:

[16] Convention on the Rights of Persons with Disabilities 2006 (OHCHR)
[17] 'Ratification Status for CRPD - Convention on the Rights of Persons with Disabilities' (OHCHR) accessed 15 May 2024

Web Content Accessibility Guidelines (WCAG) developed by the World Wide Web Consortium (W3C) are a set of internationally recognized technical standards for making web content more accessible to persons with disabilities.[18]

International Telecommunication Union (ITU) Standards developed by the ITU which work to increase access to information and communication technologies (ICTs) for persons with disabilities.

The Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled (the "Marrakesh Treaty").

[18] WCAG 101: Understanding the Web Content Accessibility Guidelines | WCAG

What Do Disability Rights Laws Say In Respect Of Access To Digital Services?

In India, the RPwD Act which replaced the Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995 provides for comprehensive rights and entitlements to persons with disabilities, including provisions related to accessibility in the digital space.[19] The RPWD Act aligns with international frameworks such as the UNCRPD by emphasizing principles of non-discrimination, accessibility and full participation of persons with disabilities in all aspects of life, including digital services. India has seen several initiatives and projects aimed at promoting digital accessibility, including accessible websites, mobile applications and assistive technologies. Organizations such as the National Association for the Blind (NAB) and BarrierBreak are actively involved in promoting digital inclusion through training, advocacy and development of accessible technology solutions.

Laws & Policies in India Pertaining to Digital Accessibility for Persons with Disabilities:

- The RPWD Act mandates that public and private entities ensure accessibility in their digital services and facilities. It requires the adoption of accessibility standards and the provision of reasonable accommodations to ensure equal access for persons with disabilities. In furtherance of Rule 15 of the RPwD Rules which requires all websites to be accessible, and based on the European standard for digital accessibility (EN 301-549), the Bureau of Indian Standards (BIS) has notified standards on ICT accessibility, namely IS 17802.
- The Ministry of Electronics and Information Technology (MeitY) has also issued guidelines for making websites and mobile applications accessible to persons with disabilities, incorporating standards based on WCAG 2.0.[20]
- The Government of India has launched the Accessible India Campaign (Sugamya Bharat Abhiyan) for achieving universal accessibility for persons with disabilities on December 3,2015.[21]

Digital Disability Rights Laws in Countries in Our Study

[19] Nirmita Narasimhan, 'Digital accessibility in the Rights of Persons with Disabilities Act 2016' (The Centre for Internet and Society, 23 January, 2017)
[20] Accessibility Statement (Ministry of Electricity & Information Technology)
[21] Accessible India Campaign (Department of Empowerment of Persons with Disabilities)

Table 2. Summary of Digital Disability Rights Laws in Countries in Our Study

Country	**Disability Law**	**Disability Rights**
India	Rights of Persons with Disabilities Act, 2016	Provides for equal opportunities, non-discrimination, accessibility, and empowerment of persons with disabilities across various aspects of life, including education, employment, healthcare, and social protection. The Act also mandates the creation of mechanisms for the enforcement of these rights and the promotion of inclusivity and accessibility in society.
Australia	Disability Discrimination Act 1992	Prohibits discrimination on the basis of disability in various areas, including access to goods, services, and facilities, including digital services
Brazil	Statute of the Person with Disabilities, 2015	Defines disability, provides for non-discrimination, prescribes priority service in public agencies for persons with disabilities, and emphasizes other public policies favourable to them.

Country	Disability Law	Disability Rights
Canada	Accessibility for Ontarians with Disabilities Act	Sets standards for accessibility in Ontario. AODA requires organizations to comply with the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA for their websites and digital content
	Canadian Human Rights Act	Prohibits discrimination based on disability and applies to digital accessibility. It mandates that organizations provide reasonable accommodations and accessibility measures to ensure equal access for individuals with disabilities
	Canadian Radio-television and Telecommunications Commission (CRTC)	Enforces accessibility regulations for broadcasting and telecommunications services
	Accessibility for Manitobans Act &The Nova Scotia Accessibility Act	Provides accessibility standards to be adopted in Manitoba and Nova Scotia by establishments
European Union	EU Accessibility Act, 2019	States that products and services should be accessible. Provides for privacy of the user.

Country	Disability Law	Disability Rights
	EU directive on accessibility of websites and mobile applications of public sector bodies, 2016	Provides for websites and mobile applications to be made accessible.
	European Electronics Communications Code, 2018	Provides for accessibility for end users with disabilities.
Singapore	Enabling Masterplan 2030 (EMP2030)	Area 8: By 2030, persons with disabilities will have access to information and communications, with reasonable accommodations provided. Recommendation 14: Design digital services with the needs of persons with disabilities in mind. Recommendation 15: Enhance access by persons with disabilities to information and communications across non-digital platforms. The Enabling Masterplan identifies 14 targets – These targets were collectively defined by a coalition of persons with disabilities, caregivers, the Government, corporate partners, social sector agencies.

Country	Disability Law	Disability Rights
United Kingdom	Ofcom Broadcasting Code, 2019	It sets out rules and guidelines for broadcasters to ensure that their content is socially responsible, respects the law, and meets standards of fairness, impartiality, and accuracy. The Code covers various aspects of broadcasting, including programming content, advertising, sponsorship, and the protection of audiences, particularly children and vulnerable groups.
United States	Americans with Disabilities Act, 1990	Prohibits discrimination on the basis of disability in places of public accommodation. Judicial precedents have interpreted "places of public accommodation" to websites and online services
Zimbabwe	National Disability Policy, 2021	a. Privacy of employment data concerning persons with disabilities must be upheld by all sectors. b. Data collected on persons with disabilities for statistical purposes – confidential. c. The transfer and use of disability-related and health-related personal information and data among third parties without the free and informed consent of the person concerned is prohibited. d. Persons with disabilities must have their individual right to free and informed consent respected within healthcare settings – decisions including in the area of sexual and reproductive healthcare, must not be imposed on persons with disabilities, and their individual consent must not be replaced or substituted by a third party.

What are Data Protection Provisions to Persons with Disabilities under Data Protection Laws?

Though data privacy has been a concern for all, and has received attention globally, certain minority groups such as persons with disabilities, racial and ethnic minorities, gender minorities, religious minorities and children are vulnerable need special protections to ensure that their data does not cause further stigmatisation, segregation[22] and prejudicial treatment in the event of breach of data privacy laws.[23]

Laws & Policies in India Pertaining to Privacy/ Data Protection for Persons with Disabilities

- Privacy has been recognised as a fundamental right under Article 21, Constitution of India by the Supreme Court in the case of Justice K.S. Puttaswamy v Union of India[24].
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011[25] (SPDI Rules): Acknowledging that certain categories of data such as biometric, health data, sexual orientation, and others require higher protection, the SPDI Rules divides data into two categories i.e. Personal data and Sensitive Personal data. The SPDI Rules further classifies physical, physiological and mental health condition as Sensitive Personal data and requires the Data Fiduciary to comply with higher standards of security.
- The DPDP Act, has erased the distinction between personal data and sensitive personal data and accords same level of protection to all categories of data (See Annexure 2 for extracts of the DPDP Act, 2023 as it pertains to persons with disabilities).

Similar to the SPDI Rules in India, other countries in our study treat disability or health data with sensitivity and imposes higher safety standards on data fiduciaries.

Treatment of Disability Data under Data Protection Laws in Countries in Our Study

[22] 'Why privacy is particularly crucial for people with disabilities' (*EDRI*, 4 December 2019) accessed 15 May 2024

[23] Jonathan Lazar and others, 'Information Privacy and Security as a Human Right for People with Disabilities' in Jonathan Lazar and Michael Ashley Stein (eds), *Disability, Human Rights, and Information Technology* (University of Pennsylvania Press 2017)

[24] K.S Puttaswamy v. Union of India AIR 2017 SC 4161

[25] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

Table 3. Summary of Provisions on Treatment of Disability Data under Data Protection Laws in Countries in Our Study

S.No.	Country	Special Protection to Disability Data	Classification of Disability Data
01.	India	No[26]	
02	Australia	Yes	Disability is classified under health data that is classified as sensitive personal data
03	Australia, Queensland	Yes	Disability is classified under health data that is classified as sensitive personal data
04	Australia, Tasmania	Yes	Disability is classified under health data that is classified as sensitive personal data
05	Brazil	No	Health data is construed as sensitive personal data, however, disability has not been explicitly mentioned.
06	Canada	No	
07	European Union	No	Health data has been construed as a special category of data, however, disability has not been explicitly mentioned.
08	United Kingdom	No	Health Data is a special category, however, does not explicitly provide for disability data
09	United States	No	
10	Singapore	No	
11	Zimbabwe	No	

With classification of disability data as sensitive personal data, data protection laws accord such data higher level of protection as compared to non-sensitive personal data. For instance, under the Privacy Act, 1988 in Australia, non-sensitive personal information may be collected without the

[26] The DPDP Act does not make any distinction between sensitive personal data and personal data. Under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, physical, physiological and mental health condition is classified under sensitive personal data.

consent of Data Principal, however, consent is required for collection of sensitive personal information.

What are Provisions on Consent for Persons with Disabilities under Data Protection Laws?

Jurisdictional Provisions on Consent

*Table 4. Elements Within the Definition of Consent Under Respective Data Protection Laws[27]**

Country	Applicable Law	Specific /Express	Informed	Free/Voluntary	Unequivocal	Implied
India	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[28]	Yes	No	No	No	No
	Digital Personal Data Protection Act, 2023	Yes	Yes	Yes	Yes	No
Australia	Privacy Act, 1988	Yes	No	No	No	Yes
	Australian Privacy Principles[29]	Yes	Yes	Yes	No	Yes
Australia, New South Wales	Privacy and Personal Information Protection Act 1998[30]	Yes	No	No	No	No

[27] The Personal Information Protection and Electronic Documents Act in Canada does not define consent. Personal Information Protection and Electronic Documents Act
[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011
[29] Australian Privacy Principles Guidelines
[30] Privacy and Personal Information Protection Act 1998 No 133 (New South Wales)

Country	Applicable Law	Specific /Express	Informed	Free/Voluntary	Unequivocal	Implied
Australia, Victoria	Privacy and Data Protection Act, 2014[31]	Yes	No	No	No	Yes
Australia, Queensland	Information Privacy Act, 2009	Yes	No	No	No	Yes
Australian Capital Territory	Information Privacy Act, 2014[32]	Yes	No	No	No	Yes
Brazil	Brazilian General Data Protection Law (LGPD), 2020	Yes	Yes	Yes	Yes	No
European Union	General Data Protection Regulation	Yes	Yes	Yes	Yes	No
Singapore	Advisory Guidelines[33]	Yes	Yes	Yes	Yes	No
United Kingdom	Data Protection Act, 2018[34]	Yes	Yes	Yes	Yes	No
United States, California	The California Consumer Privacy Act[35]	Yes	Yes	Yes	Yes	No
Zimbabwe	Data Protection Act, 2021	Yes	Yes	Yes	Yes	No

[31] Privacy and Data Protection Act 2014 (Victoria)
[32] Information Privacy Act 2014 (Australian Capital Territory)
[33] Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Personal Data Protection Commission Singapore, 23 September 2013)
[34] Data Protection Act 2018 (United Kingdom)
[35] California Code, Civil Code - CIV § 1798.140

The Table 4 indicates that countries are increasingly moving away from implied consent to positive or express action by the Data Principal to give consent. While consent is considered as a significant parameter to determine collection and use of data, countries have recognised that lengthy and incomprehensible privacy notices have led to 'consent fatigue', thereby, taking away the 'specific' and 'free' nature of consent.[36] The concept of free and informed consent meets poignant quandaries in the case of persons with disabilities. A person with disability would find it difficult to navigate through inaccessible, and lengthy privacy notices. Some countries also take account of the ability of persons with disabilities to read consent notices and comprehend the implications of consent. With such acknowledgement, countries have suggested measures to ensure that free and informed consent is secured from persons with disabilities. However, not all countries provide for any such accessible consent provisions for persons with disabilities.

**Data protection laws primarily define consent as express or implied consent. A few jurisdictions define consent to include additional features such as informed, free, and unequivocal. The table provides details on how countries define consent under applicable data protection laws.*

[36] Bart Schermer and others, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' [2014] Ethics and Information Technology

Jurisdictional Provisions on Consent Protocols for Collection of Digital Data

Data protection laws require the Data Principal to give consent, however, in case of children such consent is obtained from the parent or lawful guardian of the child. Under the DPDP Act, a requirement to secure consent from a lawful guardian has been imposed for persons with disabilities (who has a lawful guardian) as well. The Figure 6 lists countries that provide for the assignment of a person with disabilities' right to give consent under respective data protection laws. Countries that have a provision for assignment of rights under respective data protection laws are India, Zimbabwe, and Australia. Countries that don't carry a provision to assign are Canada, European Union, United Kingdom, United States and Singapore.

Figure 6. Assignment of Right to Consent for Persons with Disabilities under respective Data Protection Laws

Australia, India, and Zimbabwe have, under their respective data protection laws, provided that consent on behalf of a person with disability shall be provided by a lawful guardian/representative. Each country however takes a distinctive approach towards assignment of right to consent under data protection laws. Australia, takes a welfare approach by requiring that a Data Fiduciary shall provide assistive resources to facilitate that the capacity is maximally exercised as described in the Figure 7 below.

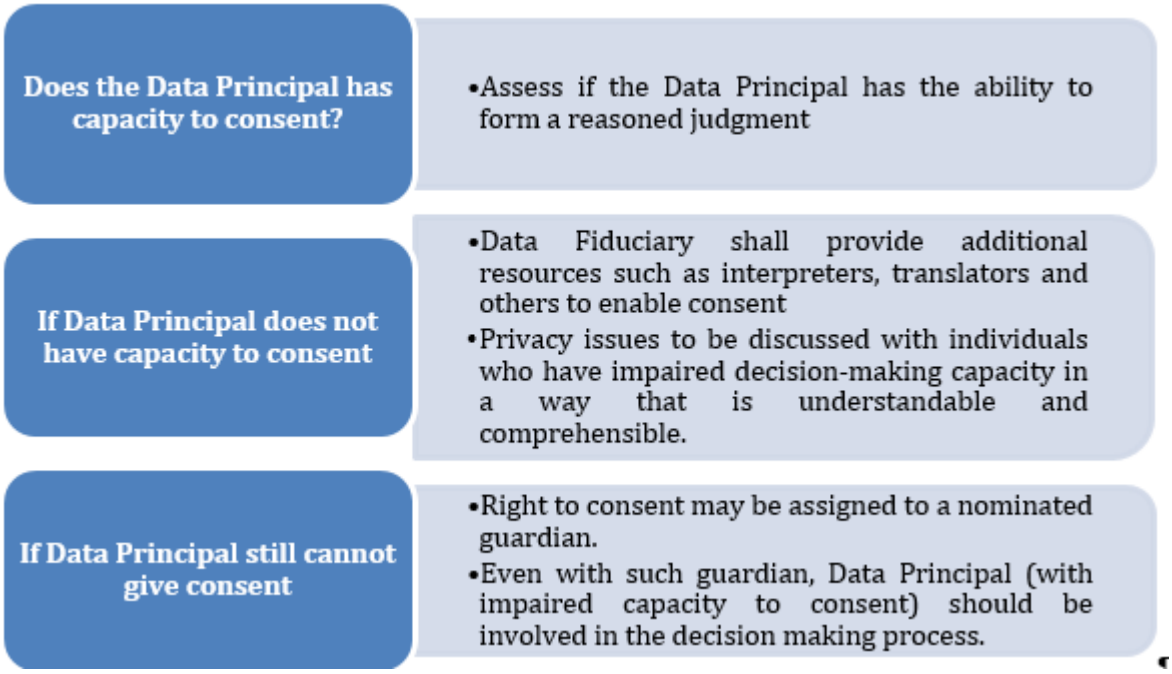

Figure 7. Assignment of Right to Consent in Australia under the Data Protection Law

The law in Australia does not presume lack of capacity, but requires the Data Fiduciary to address the root of such incapacity. For example: If consent from a person with visual impairment must be secured, the Data Fiduciary is expected to make efforts to convert text to audio and allow for obtaining audio consent.

The Data Protection Act in Zimbabwe requires that incapacity to consent must be proven by a physician or other person legally competent to prove incapacity whereas the DPDP Act in India requires that consent of a person with disability must be routed through their legal guardian, regardless of the capacity of the person with disability to provide their own consent. Figure 8 explains the approach of Zimbabwe and India in detail.

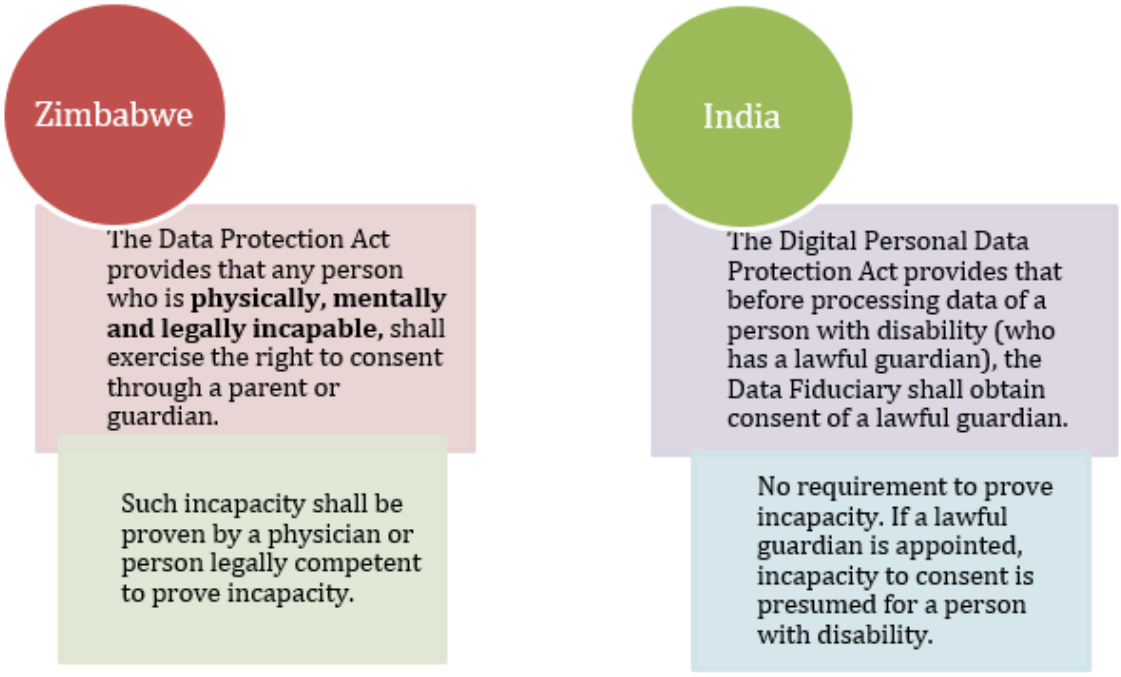

Figure 8. Summary of Provisions Pertaining to Assignment of Consent (of a person with disability) under Data Protection Laws in Zimbabwe and India

Zimbabwe has taken a positive step by placing a requirement that the incapacity of a person to give consent shall be proven to assign the right to consent. However, even though disability may be physical, intellectual, mental or sensory, India under the DPDP Act imposes a blanket presumption to imply that a person with disability does/does not have decision making abilities so long as there is/is not a lawful guardian.

Right to consent may be assigned in India, Zimbabwe and Australia, but who has the authority to give consent on behalf of a person with disability under data protection laws?

1. In Zimbabwe:
    a. Parent
    b. Guardian
    c. Person designated by court
    d. Person as provided under law
2. In Australia:
    a. Guardian
    b. Person with Power of Attorney

c. Person Responsible under the Guardianship Act

d. Person nominated

3. In India: Lawful guardian. However, the DPDP Act provides no clarity if such guardians should be appointed under the National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (NT Act) or the Rights of Persons with Disabilities Act (RPwD Act). The co-existence of two laws for appointment of a guardian, each with very similar scope of decision making by the guardian, leaves a wide scope for interpretation.

Limitations Of India's Data Protection Act for Persons with Disabilities

a. On the Complexities of Guardianship as It Exists in The Law: Language in DPDP does not differentiate between guardianship under NT Act and RPwD Act. What complications does this result in?

For a person with disability, a guardian may be appointed under the NT Act and the RPwD Act. The process and purpose of appointment of a guardian vary under the two laws. Under the NT Act, the guardian is appointed by the local committee on an application from the parent or relative of a person with disability whereas the court determines the need to appoint a guardian under RPwD Act.

A lawful guardian may be appointed for the care, and maintenance of persons with disability and their property under the NT Act. Under the RPwD Act, a limited guardian may be appointed for limited purposes to take legally abiding decisions and support the person with disability in taking decisions. RPwD Act upholds the autonomy of a person with disability to make independent decisions and provides for limited guardianship. Further, the NT Act covers only four disabilities i.e. autism, cerebral palsy, intellectual disabilities and combination of these whereas RPwD Act covers 21 kinds of disabilities.

i. **There is no clarity if the lawful guardian should have been appointed under the NT Act or RPwD Act.**
ii. **A limited guardian appointed under RPwD Act should not provide consent for data sharing, as this will amount to overreach of the guardian's powers.**

b. On Legal Capacity for People with Disabilities:

B.1 Are there circumstances where despite having a guardian under NT Act/RPwD Act, a person with disability still has capacity to provide consent for data sharing?

A disability may be physical, intellectual, mental or sensory. Accounting for the spectrum of disabilities, there cannot be a blanket presumption to imply that a person with disability does/does not have decision making abilities.

The principle of individual autonomy, freedom to make one's choices and independence of persons have been furthered in the Convention on Persons with Disabilities and RPwD Act.

The question arises - has the individual autonomy of a person with disability been undermined by the DPDP Act placing a blanket requirement of securing consent of the lawful guardian? Moreover, even if a guardian has been appointed, the person with disability may have the ability to make decisions regarding data sharing.

It is important to define the circumstances under which the requirement to secure consent of the lawful guardian would be required, failing which the person with disability should directly provide consent with reasonable accommodations.

B.2 Does appointment of a lawful guardian necessarily mean that the person with disability cannot give consent for data sharing?

If a lawful guardian is appointed under the NT Act or RPwD Act but the person with disability has the capacity to make decisions related to data sharing, can the person with disability override the requirement of consent from the lawful guardian? **If the person with disability provides consent without consent of the legal guardian, will this amount to violation of the law? What would the implications of the override be on the person with disability, their data, and their guardian?**

c. On Adequacy of DPDP in Protecting Data of Persons with disability: What are the ways and/or practices to strengthen the DPDP Act to secure data of Person with disability?

C.1 Consent Mechanism

To comply with the requirement of obtaining the consent of the lawful guardian, additional information such as the kind of disability, degree of disability, proof of disability, proof of lawful guardian, etc. are expected to be collected. This will result in collection of additional data pertaining to persons with disabilities to avail the internet services. However, the law does not provide any additional measures to safeguard data of vulnerable groups, and there is no provision for compensation/ damages.

C.2 Accessibility of Grievance Redressal Mechanism

Grievance redressal mechanisms to enable a data principal to exercise rights under the DPDP Act would need to be made accessible to persons with disabilities so that such mechanisms are effective and inclusive.

In the next steps of the research, we will engage with experts and lived experiences of persons with disabilities to find potential solutions from a legal, policy and practice lens, towards data protection and consent frameworks that are meaningful for persons with disabilities.

Annexure 1: Digital Accessibility Provisions and Standards

Table 1: Digital Accessibility Provisions in UNCRPD

SI. No.	Article	Provisions
1.	Article 9	Upholds the importance of accessibility for persons with disabilities in all areas of life, including the physical environment, transportation, information and communication and technology. It calls for the removal of barriers and the adoption of measures to ensure equal access to facilities, services and opportunities
2.	Article 21	Imposes states to take appropriate measures to provide information intended for the general public to persons with disabilities in accessible formats and technologies appropriate to different kinds of disabilities; facilitate the use of sign languages, Braille, augmentative and alternative communication and all other accessible means, modes and formats of communication of their choice by persons with disabilities in official interactions; urging private entities that provide services to the general public, including through the Internet, to provide information and services in accessible and usable formats for persons with disabilities; encouraging mass media, including providers of information through the Internet, to make their services accessible to persons with disabilities and recognizing and promoting the use of sign languages
3.	Article 24	State Parties are required to take appropriate measures to provide learning alternative communication methods such as Braille, sign language and other augmentative and alternate modes of communication. promote the linguistic identity of the deaf community by facilitating the learning of sign language and ensuring that education for persons who are blind, deaf, or deafblind is delivered in appropriate languages and communication modes. States Parties are obligated to employ qualified teachers, including those with disabilities, who are proficient in sign language and/or Braille and must ensure that persons with disabilities have equal access to general tertiary education, vocational training, adult education, and lifelong learning opportunities without discrimination.

Web Content Accessibility Guidelines (WCAG)

The WCAG developed by the World Wide Web Consortium (W3C) are a set of internationally recognized technical standards for making web content more accessible to persons with disabilities. The guidelines aim to make websites, apps, electronic documents, and other digital assets accessible

to people with a broad range of disabilities, including sensory, intellectual, learning and physical disabilities.[37] The WCAG are categorized based on four main principles that are as follows:

1. **Perceivable**: Web content should be presented in a way that can be perceived by all users, regardless of their sensory abilities. This includes providing text alternatives for non-text content, such as images and multimedia, and ensuring that content can be presented in different ways without losing meaning.
2. **Operable**: Users should be able to navigate and interact with web content using various input methods, such as keyboard, mouse, or assistive technologies. This involves making all functionality available from a keyboard, providing sufficient time for users to read and use content, and avoiding content that can cause seizures or physical reactions.
3. **Understandable**: Web content should be easy to understand and operate for all users, including those with cognitive or learning disabilities. This includes using clear and simple language, providing predictable and consistent navigation, and ensuring that users can avoid and correct mistakes.
4. **Robust**: The content must be robust enough that it can be interpreted by a wide variety of possible user agents, including assistive technologies. The website should have maximum compatibility with current users as well as technologies that may evolve.

International Telecommunication Union (ITU) Standards

ITU works to increase access to information and communication technologies (ICTs) for persons with disabilities.[38] These guidelines cover a wide range of technologies, including telecommunications, broadcasting, and internet services. ITU develops technical specifications for ICT products and services to ensure interoperability and compatibility which will help manufacturers and developers to create products that meet accessibility requirements and can be used by persons with disabilities. ITU standards include recommendations for the development and deployment of assistive technologies, such as screen readers, magnification software and alternative input devices.

Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled

The Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled (the "Marrakesh Treaty") is an international treaty adopted in 2013 under the auspices of the World Intellectual Property Organization (WIPO). The primary

[37] WCAG 101: Understanding the Web Content Accessibility Guidelines | WCAG

[38] Accessibility (itu.int).

objective of the Marrakesh Treaty is to facilitate access to published works in accessible formats such as Braille, audio and digital text. The Marrakesh Treaty promotes cross-border exchange of accessible format copies by allowing authorized entities to share these copies with other authorized entities across national borders. This facilitates access to a wider range of accessible materials for persons with print disabilities.[39]

[39] Summary of the Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired, or Otherwise Print Disabled (MVT) (2013) (wipo.int).

Annexure 2: Provisions pertaining to Persons with Disabilities in the DPDP Act

Section 2(j) – Definition of Data Principal	"Data Principal" means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf
Section 9 – Processing of Personal Data of Children	(1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian, obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed. Explanation—For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.

Annexure 3: Methodology for Selection of Countries

137 out of 194 countries had put in place legislation to secure the protection of data and privacy.[40] We wanted to obtain a representative sense of legislative approaches across the world to consent protocols related to persons with disabilities. Our preliminary research indicated that several states in Africa and Australia have provisions related to persons with disabilities in their data protection laws. We also found that some countries with advanced data protection jurisprudence do not make any reference to persons with disabilities. ***We wanted to consider both: laws that provide and laws that do not provide sections relating to persons with disabilities. So, we chose at least one country with advanced data protection jurisprudence from each continent and arrived at the following list of eight countries: India, Australia, Brazil, United States, Canada, European Union, United Kingdom, Zimbabwe, and Singapore.***

[40] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) accessed 15 May 2024