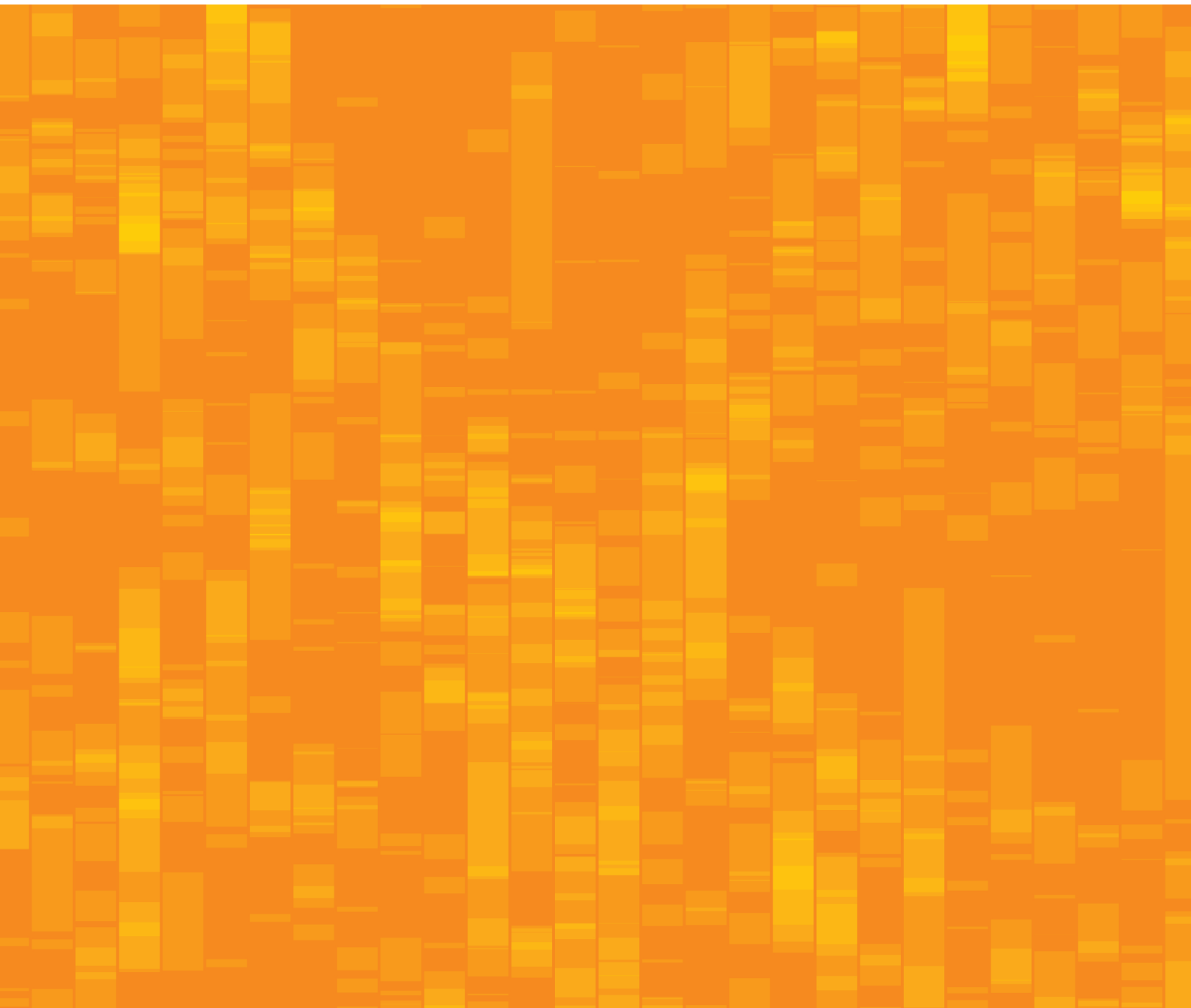
ESYA centre

An Empirical Evaluation of the Implementation Challenges of the Digital Personal Data Protection Act 2023

Insights and Recommendations for the Way Forward | January 2024



ATTRIBUTION
Meghna Bal. An Empirical Evaluation of the Implementation Challenges of the Digital Personal Data Protection Act, 2023: Insights and Recommendations for the Way Forward. January 2024, Esya Centre.

ESYA CENTRE
B-40 First Floor, Soami Nagar South, New Delhi - 110017, India

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org.

AUTHOR
Meghna Bal is the Head of Research at the Esya Centre.

ACKNOWLEDGEMENT
The author thanks Mohit Chawdhry, Tamanna Sharma, and Dr. Vikash Gautam for their inputs on this paper.

ESYA centre

Table of Contents

Table of Figures

Executive Summary

a. This report examines the challenges to implementing India's Digital Personal Data Protection Act, 2023 (DPDPA). Seeking to understand the operational and technical hurdles faced by organisations to the Act's enforcement, the report delves into aspects related to the implementation of consent mechanisms, provisions for children and persons with disabilities, and the intricacies of appointing data protection officers. Specifically, it explores the internal processes required for compliance and establishes the timelines necessary for meeting the DPDPA's obligations.

b. This report adopts a mixed-method approach, combining semi-structured interviews with 16 respondents (13 data fiduciaries and three experts) with secondary research. The questionnaire provided to the respondents – a mix of close- and open-ended questions – was designed to capture diverse perspectives, experience, and organisational structures. Respondents provided insights into their business size, data handling practices, and prior experience of abiding by data protection laws. They also discussed their understanding and compliance plans for the DPDPA's key provisions, such as consent mechanisms and the appointment of a data protection officer. Neutrality and clarity in questioning have been ensured to accurately capture the complexities of DPDPA implementation.

c. Analysis of enactment of data protection laws in various jurisdictions, including the European Union (EU), Brazil, Japan, and California in the United States (US), reveals a common trend of granting a two-year grace period and ensuring leniency in enforcement post implementation. The EU's General Data Protection Regulation (GDPR) was enacted in May 2016, but it was only enforced from May 2018, with authorities showing relaxed enforcement initially. Brazil's Lei Geral de Proteção de Dados Pessoais (LGPDP) was passed in August 2018, but penalties were not enforced until 2021, demonstrating a similar leniency. In Japan, significant amendments to the Act on the Protection of Personal Information in June 2020 became applicable only in April 2022, despite some stricter penalties coming into effect from December 2020. Similarly, the enforcement of California's Consumer Privacy Act (CCPA), passed in June 2018, was delayed till July 2020, in line with the GDPR's approach. These cases illustrate a global pattern of allowing organisations a substantial period of time to adapt to new data protection regulations.

d. The report analyses seven key aspects of implementing India's DPDPA:

i. **Experience and Preparation**
Among the 13 data fiduciaries interviewed, 54% lacked experience in implementing data protection laws in other jurisdictions – mostly firms with large user bases. Despite this, 85% have begun preliminary deliberations on DPDPA compliance. However, their preparation is hindered by the absence of rules which make up the substance of implementation for many provisions in the DPDPA. However, some data fiduciaries said that the absence of a data protection law in India until recently meant that a complete overhaul of business structures was required to implement the DPDPA.

ii. **Notice and Consent**
Implementing Section 6 of the DPDPA, which demands explicit consent for data processing, presents operational challenges. Take, for instance, the requirement to provide consent notices in 22 languages. Translating legal terms into the languages listed in the Eighth Schedule of the Constitution of India poses difficulties, with some terms lacking equivalents. Concerns were raised about the effectiveness and inclusivity of this requirement, as some languages, such as Sanskrit, are spoken by a very small section of the population; preferred languages of some groups may also not be included. In addition, most fiduciaries' consent documentations are currently in English only, indicating a significant need for technical changes and interface adaptations.

iii. **Verifiable Consent for Parents/Guardians of Children and Persons with a Disability**
Section 9 of the DPDPA requires verifiable parental or guardian's consent for children and disabled persons – another considerable operational burden. The lack of a clear definition of "person with disability" under the DPDPA creates ambiguity and potential prejudice against such persons as it leaves the scope of the term broad, potentially including all persons with disability, even those who are competent to contract. This, in turn, could bring about a potential conflict with the Rights of Persons with Disabilities Act, 2016.

iv. **Appointment of a Data Protection Officer**
Most respondents, including experts, indicated that hiring data protection officers would be challenging due to the need for experience and expertise for this role, compounded by high market competition for such professionals.

v. **Lack of Clarity on Implementation**
The absence of a clarifying authority under the DPDPA and varying interpretations of data protection terms can create uncertainty around implementation.

vi. **Timelines for Implementation**
Respondents indicated that it would take upto two years, from the time the rules are finalised, to implement the provisions of the DPDPA. This seems to be in line with the timeline provided by jurisdictions such as Japan, Brazil, the US (California), and the EU for compliance with their data protection laws when they were introduced/substantially amended.

e. Given the challenges identified, the report makes the following recommendations:

i. **Provide a two-year timeline for the implementation of the DPDPA (from the time the rules are notified)**
This will follow the international best practices in Japan, Brazil, the US (California), and the European Union. It will also give firms of varying sizes and experience in India ample time to coordinate their internal processes and resources, and comply with different provisions effectively. To reiterate, while the firms with experience of implementing a data protection law and the ones with no experience differed on the timelines for consent notices, most of these converged on a 24-month timeline for the verifiable consent provision. Given that many firms may have to implement provisions sequentially due to resource constraints, it makes sense to allow a 24-month period for compliance. This timeline should begin from the time the rules are notified and finalised, as the crux of the implementation lies within them.

ii. **Observe a leniency period for 12 months after the initial 24-month timeline for implementation is over**
Leniency periods are common in other jurisdictions. Most countries did not start seriously enforcing penalties and other sanctions under their data protection laws immediately after these came into force. In the European Union, there was an unofficial leniency period for nine months, whereas in Brazil, it extended up to two years. Given that some of the provisions of the DPDPA are particularly challenging to comply with, such as the obligation related to obtaining the verifiable consent of a guardian of a disabled person, it may be prudent to accord to companies some amount of leniency so that they are not unnecessarily harassed by enforcement actions.

iii. **Refrain from making the notice and consent requirement overly prescriptive to reduce the technical burden on entities**
Ideally, entities should have the freedom to present notices in a manner that does not add friction to their consumer journey. If consent requirements are overly burdensome, respondents indicated that this might diminish the customer experience. It also adds to complication and cost of implementing the provision, which can be particularly burdensome for smaller organisations.

iv. **Allow data fiduciaries to decide which languages to display consent notices in, based on an evaluation of customer needs**
This will ensure that no groups of data principals feel excluded due to the limited list of languages in the Eighth Schedule. It will also reduce some of the burden on smaller data fiduciaries, which may face a hard time complying with this requirement.

v. **Clarify the scope of the term, "person with disability", under Section 9 to mean only those persons who are severely mentally disabled or of unsound mind**

At present, the term, "persons with disability", is not defined, indicating that the provision extends to both mentally and physically disabled persons. This provision is challenging because it may be difficult for firms to create a means to identify all kinds of disabled persons. In addition, it is also prejudicial to the rights of disabled persons that are competent to contract, and therefore, required by law to be treated equally with those who are not disabled.

vi. **Establish a mechanism for clarification of terms and provisions under the DPDPA, such as regular open-house discussions**

There is currently no authority that can provide clarity regarding the scope of terms and obligations under the DPDPA. This can be a considerable challenge, particularly for smaller entities. Studies on other countries show that even when there are authorities in place and even when the rules are promulgated, entities may face a hard time understanding the scope of their obligations. The experience of other countries reveals that a clarificatory authority is indispensable for the successful implementation of a data protection law. As such, the government must consider ways to introduce a similar mechanism or at the very least, provide some channel of communication through which clarifications may be sought.

vii. **Ensure a consultation period of at least 60 days for the rules made under the DPDPA**

To enhance clarity and facilitate effective implementation of the DPDPA and its associated rules, it is crucial to allocate ample time for consultation. For example, in Japan, the consultation period for the amendments to the Act on the Protection of Personal Information (APPI) started 11 months before they were formally implemented. As highlighted in this document, the introduction of a data protection law necessitates coordination across various segments within an organisation, including business, technical, and legal departments. For multinational corporations, this coordination also involves their global teams. Adequate time is needed for these stakeholders to understand the impact of new provisions and offer constructive feedback on their implementation. Additionally, longer consultation periods tend to be more inclusive. Smaller companies and entrepreneurs, who may lack awareness or resources, often find it challenging to engage in shorter consultation periods. Extending the timeline for consultation can provide an opportunity for such groups to share their perspectives.

Introduction

Data protection laws are integral for granting consumers of digital products a sense of agency over their data. These laws are also important from a cybersecurity perspective – as they nudge organisations, through a framework of remedies and penalties, to safeguard personal data under their care.[1] Despite their significance, data protection laws are challenging to implement. These challenges have been mapped in the context of other jurisdictions, such as the European Union, and typically arise from operational and technical aspects of implementation as well as issues related to interpreting data protection obligations.[2]

Based on the interviews with 16 respondents (13 data fiduciaries and three experts), this report maps the challenges related to implementing India's recently enacted Digital Personal Data Protection Act, 2023 (DPDPA). The objectives of the report are to:

i. identify the challenges faced by organisations to meeting different key obligations under the DPDPA, such as obtaining verifiable consent of parents/guardians of children and persons with disabilities, hiring a data protection officer, and carrying out data audits;

ii. uncover the internal processes and coordination that go into complying with these requirements; and

iii. establish the timelines necessary for meeting these obligations once subordinate legislations/rules are notified.

The main findings of this report indicate that organisations will face considerable operational and technical burden when implementing the notice and consent provisions due to the requirement of making this facility available in 22 languages. Organisations will also face considerable difficulties in implementing the verifiable consent provision for children and persons with disabilities, particularly if the scope of the term, "disabled persons", is not clearly delineated. The requirement for verifiable consent of a parent/guardian of a disabled person can also be prejudicial to the rights of such persons, if the scope of this term is not limited to mentally challenged individuals, who by law are not competent to enter into contracts on their own.

Consequently, the report recommends that these implementation challenges be addressed, in part, by providing stakeholders with at least a two-year time period to execute complex provisions, a leniency regime for penalties, along with some other measures that allow for greater clarity and flexibility. The provision of opportunities for constructive dialogue is also a necessary prerequisite for effective implementation of the new data protection framework in India.

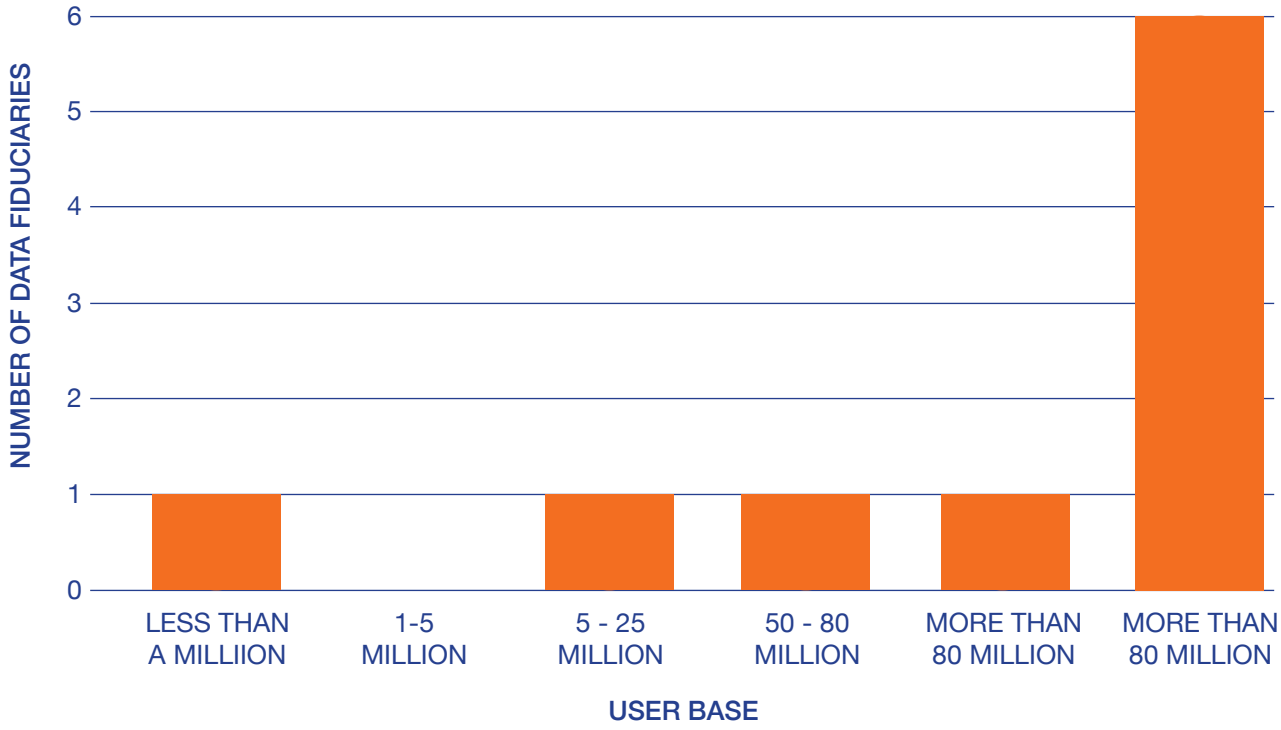
Details of the Participants

The 13 data fiduciaries interviewed included organisations operating in different sectors with varied user bases (see Figure 1 below);

70% of the data fiduciaries reported a user base of five million or more.
Some respondents could not indicate the number of users due to internal policies. The three experts interviewed were from a public policy firm, a think tank, and an industry association.

FIGURE 1

Number of registered Indian users and customers, across data fiduciaries



Note: The sample consists of 10 data fiduciaries. Three data fiduciary respondents did not answer the question regarding their user bases because of their company policies.

Source: Author's own

Methodology

A mixed-method approach was adopted for preparing the report. It involved semi-structured interviews with 13 data fiduciaries and three experts as well as secondary research on the implementation of data protection laws in other jurisdictions. The survey questionnaire provided included both close-ended and open-ended questions. Such a format allowed for flexibility to accommodate diverse expertise, organisational structures and experiences, and viewpoints while also creating modalities for data on timelines that are necessary for implementation.

Respondents were first asked to provide background information regarding the size of their business, scope of personal data collection, and prior experience of implementing a data protection law. They were also asked if they had enough clarity regarding the extent of their obligations under the DPDPA. They were then requested to share their overall plans for compliance with various provisions of the DPDPA, such as those related to the notice and consent mechanism, verifiable consent of parents and guardians of children and disabled persons, tracking and monitoring of children, and the appointment of a data protection officer.

Questions were framed as neutrally as possible. Biases that led respondents to any particular answer were avoided. If a respondent did not understand a question, examples were provided to ensure greater clarity. Broadly, the framing of the survey followed Kvale (1994),[3] and Wang and Yan (2012).[4]

Previous Work

a. Challenges to Implementation

There is a considerable body of literature delving into the challenges to implementing data protection laws in other jurisdictions. Difficulties mapped by scholars include technical challenges, lack of awareness, high costs and resource requirements, and a lack of clarity around certain terms within the legislations. [5] Similar barriers regarding GDPR compliance were outlined in Tikkinen-Piri, Rohunen, and Markkula (2017). [6] In a study that looked at the awareness and readiness of organisations with regard to the implementation of the GDPR, Addis and Kutar (2018) found that entites expected the new law to have a significant impact on projects, budget allocation (for GDPR training and projects), and resource onboarding.[7] The disruption extended to an organisation's internal processes, which needed to be adapted to new GDPR requirements.[8]

Overall, the concerns highlighted in the literature about complying with data protection laws in other jurisdictions were echoed by our respondents' feedback on compliance with the DPDPA in India.

b. Timelines for Implementation of Data Protection Laws and Leniency Regimes

An analysis of the process of enactment of data protection laws across different jurisdictions revealed that many countries, including the European Union, Japan, Brazil, and the state of California, either officially or unofficially, observed a two-year grace period before implementing and enforcing these laws. In addition, authorities in these jurisdictions observed a period of leniency before imposing penalties and non-monetary sanctions on firms. These experiences are described below.

i. European Union: General Data Protection Regulation

The European Union enacted the General Data Protection Regulation (GDPR) in May 2016 but started enforcing it only in May 2018. During the time between the GDPR's enactment and enforcement, the Article 29 Working Party (precursor to the European Data Protection Board, the EU's data protection authority) issued action plans and guidance on the different facets of the law.[9] Moreover, scholars found that in the months following the implementation of the GDPR, enforcement of its norms was somewhat relaxed, indicating that the authorities adopted an unofficial leniency policy. Illustratively, Hilliard (2020) undertook a study of GDPR fines and non-monetary sanctions, both imposed and pending, from May 2018 to March 2020. [10] Hilliard (2020) found that data protection authorities in EU member states hardly imposed fines or administrative measures in the first three quarters after the GDPR came into effect. [11] The number of fines imposed across EU member nations crossed 20 after the third quarter of 2019, indicating that the authorities observed a leniency period till this time.[12]

ii. Brazil: Lei Geral de Proteção de Dados Pessoais

Brazil enacted its data protection law, Lei Geral de Proteção de Dados Pessoais (LGPDP), in August 2018, and its substantive provisions were supposed to take effect in August 2020.[13] After the COVID-19 crisis erupted, there was a proposal to postpone the LGPDP's enforcement till August 2021; however, this was not followed through due to a legislative impasse.[14] While the LGPDP came into effect in 2020, enforcement of penalties was put off till 2021. The Brazilian Data Protection Authority (ANPD) issued its first sanction under the LGPDP in July 2023, indicating additional two years of leniency that were observed once the LGPDP came into force.

iii. Japan: Amendments to the Act on the Protection of Personal Information

In June 2020, Japan significantly amended its privacy law, the Act on the Protection of Personal Information (APPI).[15] The amendments included obligations for data breach reporting and notification of affected persons where there was a risk of harm, obtaining additional specific consent for personal data transfers outside Japan, and enhanced obligations for data processors to obtain consent when transferring personally referrable information[16] to a recipient. Importantly, the majority of the new provisions became applicable only in April 2022, close to two years after they were promulgated.[17]

iv. The US: California Consumer Privacy Act

The California State Legislature passed the California Consumer Privacy Act (CCPA) on 28 June 2018. Section 1798.185 of the Act required the Attorney General (AG), the designated enforcement authority, to promulgate regulations on different aspects of the CCPA after broad public consultation on or before 1 January 2020.[18] Section 1798.185(c) also stipulated that the AG might not initiate enforcement actions under the CCPA for a period of six months after the date of regulation or 1 January 2020, whichever was earlier.[19] The CCPA thus allowed a leniency period of 18 months following the Act's entry into force during which the AG had to finalise the regulations and businesses had to comply with.

In August 2018, the California State Legislature passed Senate Bill-1121, which delayed enforcement of the law. It extended the deadline for the AG to consult on and issue regulations by six months – 1 July 2020 instead of 1 January 2020.[20] The deadline for taking enforcement action under the CCPA was also extended to 1 July 2020.[21] Essentially, the period between the passage of the CCPA and its enforcement was two years, the same as the GDPR.

Results and Analysis

This report analysed seven aspects of implementing the DPDPA. The results of these evaluations are described in detail below:

i. Experience and Preliminary Preparation

Out of the 13 data fiduciaries interviewed, **seven (54% lacked experience in implementing data protection laws in other jurisdictions.** All seven of these inexperienced firms are significant in size, having user bases ranging from 50 to 80+million.

FIGURE 2

Data fiduciaries with experience in implementation of data protection laws

Note:13 data fiduciaries participated in the survey on this question. *Source: Author's Own*

It was found that **85 percent of the respondents had begun considering how to implement the compliance requirements of the DPDPA**. Most respondents indicated that these were preliminary considerations as the rules required for implementation are not yet in place. The substantive provisions of the DPDPA were to be set out through rules. Until these were in place, companies could not realistically prepare for implementation and compliance.

FIGURE 3

Data fiduciaries that have started deliberating on implementing the law within their organisations

Note:13 data fiduciaries participated in the survey on this question. *Source: Author's Own*

ii. Notice and Consent

Section 6 of the DPDPA requires data fiduciaries to obtain "free, specific, informed, unconditional and unambiguous" consent from data principals to process the latter's personal data for a specified purpose. Such consent must be provided through "a clear affirmative action", i.e., users must indicate their consent by opting in.

As per Section 5(1) of the DPDPA, request for consent must be accompanied or preceded by a notice that informs the data principal concerned of the personal data collected and the purpose of such collection, how to exercise rights under the Act, and how to lodge a complaint with the Data Protection Board.

FIGURE 4

Data fiduciaries that have (non DPDPA) consent mechanisms on their websites and applications

Note:13 data iduciaries participated in the survey on this question. *Source: Author's Own*

According to Section 5(3), data fiduciaries must provide data principals with the option to read a notice in English or any of the 22 languages listed under the Eighth Schedule of the Constitution of India. The majority of the respondents indicated that the extensive language requirement under Section 5(3) presented a significant operational burden as their service was offered only in two languages and the scheme of compliance was unclear. Illustratively, **84 percent of the data fiduciaries interviewed already had a consent mechanism in place prior to the enactment of the DPDPA**. However, the majority of the entities pointed out that their consent documentation was available only in English.

FIGURE 5

Percentage of data fiduciaries that require technical/architectural/interface changes to their products or services to display notices in 22 languages

Note: 13 data iduciaries participated in the survey on this question. *Source: Author's own*

Furthermore, **94 percent of the respondents indicated that implementing the language option requirement for notices would yield technical/interface changes to their products or services.** Some pointed out that the process would, at a minimum, involve building backend architecture, figuring out the code that was compatible with the 22 languages and testing the changes made to understand the impact on customer journeys to ensure that the consumer experience was not disrupted.

Data mapping was another necessary measure highlighted by the survey respondents. It is an exercise whereby an organisation tracks what kind of data is collected, how it is transmitted, stored and processed, and with whom it is shared. The necessity of data mapping is also emphasised in existing literature. For instance, Sirur, Nurse, and Webb (2018) highlighted that data mapping was integral to any attempt by an organisation to comply with the GDPR.[22] Data mapping helps organisations uncover risky data practices that they may not be aware of and gain a better sense of being able to control data.[23] However, mapping data in the right manner is also a challenge, particularly for small and medium enterprises, as it is both time-consuming and expensive.[24] Illustratively, a study on GDPR readiness found that most of the data mapping process was manual.[25]

The majority of data fiduciaries surveyed indicated that they would rely on translations to meet the notice language requirement under the DPDPA. However, they also highlighted some issues with such an approach. Certain words in English, particularly legal terms conveying information about rights and legal processes, do not have equivalents in many of the languages included under the Eighth Schedule. Similarly, many words in other languages under the Eighth Schedule are not translatable. The respondents pointed out that in such cases, only a "best-effort" transliteration could be the solution. However, they stressed that this may amount to compliance tokenism. [26]

The respondents also said that the policy objective of providing notices in all languages listed in the Eighth Schedule was unclear. If the goal of relying on the

Eighth Schedule was to ensure inclusivity, this objective could be defeated for two reasons. Firstly, some of the languages listed are spoken by a very small fraction of the population. Illustratively, one respondent noted that Sanskrit is one of the Eighth Schedule languages; according to the last available census data, it is considered mother tongue by less than .002% of the population.

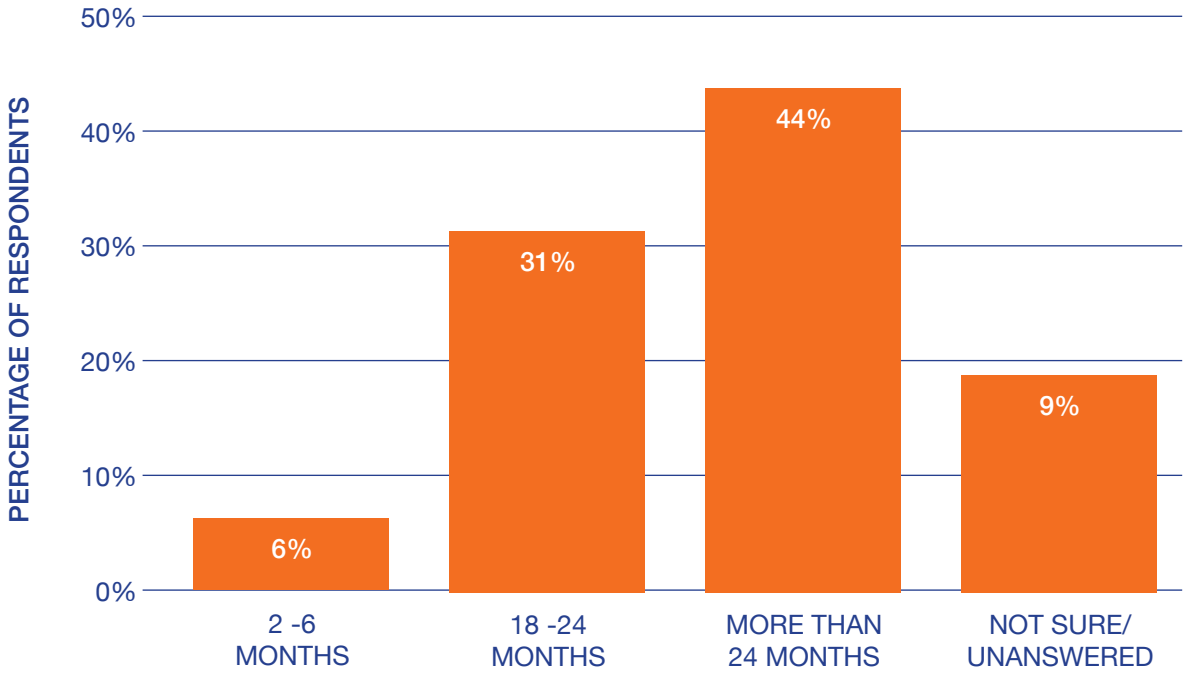
Secondly, preferences for languages that are not included in the Eighth Schedule may also lead to exclusion of some data principals whose primary language is not listed in it. Of the 13 data fiduciaries surveyed, only three provided their privacy policies in more than two languages. One of them stated that its terms of service and privacy policies were available in 22 languages. However, when the author looked at the company's website, only 11 of the language options were Eighth Schedule languages. It is reasonable to assume that a business selects language options for its service on the basis of customer preferences. The Eighth Schedule requirement may, thus, exclude the preferences of different groups of data principals as some popularly spoken languages are not listed in it. We draw this conclusion as the data fiduciary in question made its service available in a number of languages that were not in the Eighth Schedule. The language requirement can also be misused by motivated entities. Say, an entity does not offer the Sanskrit option, thinking that it is very unlikely that one will come across a person who does not speak any other language. A motivated entity could use such an omission to create problems for the entity which has not made Sanskrit available, by filing a complaint with the Data Protection Board. The expert respondents agreed with the feedback provided by the data fiduciaries, acknowledging the fact that complying with the notice and consent mechanism would require changes to a service's interface/technical architecture.

iii. Verifiable Consent of the Parent or the Guardian of a Child or Persons with Disabilities

Section 9 of the DPDPA requires data fiduciaries to obtain verifiable consent of the parent or the guardian of a child or a person with a disability in the manner prescribed. **Only 46 percent of the data fiduciaries surveyed process children's personal data.** They noted that the verifiable consent requirement once again presented a considerable operational burden as multiple build options (means for parents to provide their consent) would have to be devised and deployed.

FIGURE 6

Time required by data fiduciaries to comply with the verifiable consent requirements for guardians of persons with disabilities



Note:13 data iduciaries participated in the survey on this question. *Source: Author's Own*

Some data fiduciaries expressed concerns about the consent requirement for persons with disabilities. They indicated that the Indian Contract Act, 1872 does not recognise contracts entered into by persons of unsound mind. As per Section 12 of the Contract Act, a person is of sound mind if they are capable of understanding a contract when making it and forming a rational judgment regarding its effects on their interests.[27] In terms of persons with disabilities, this will be restricted to an individual with a severe mental incapacity.

The DPDPA does not define the term, "disability". It is, therefore, unclear whether it extends to all persons with disabilities. This, respondents noted, is problematic and prejudicial to the rights of disabled persons who are competent to contract. Indeed, the provision in its current form may conflict with the Rights of Persons with Disabilities Act, 2016, which requires the Government to ensure that persons with disabilities enjoy the same legal capacity as persons with no disabilities.[28] For instance, what happens if a person is physically disabled, and competent to contract, but does not have a parent or a guardian? Will they be unable to access digital services? Moreover, will this provision also extend to persons with age-related disabilities?

A more fundamental challenge involves identifying disabled persons, for which there is currently no clarity in the Act. This, in turn, raises questions about the objective of this provision and how it will be enforced.

iv. Tracking and Behavioural Monitoring of Children and Targeting Advertising at Them

Some respondents stressed that tracking and behavioural monitoring of children were necessary to ensure their safety and also help parents keep track of their children's online activities. The respondents noted that blanket restrictions on such activities would hamper online safety for minors. For instance, instead of receiving age appropriate ads, minors would receive ads meant for adults, which could be highly problematic. Moreover, available literature indicates that blanket restrictions on targeting advertising at minors are not effective. A number of studies have found that in the absence of rules expressly guiding companies on what is appropriate for children, websites can be riddled with advertisements that are not age-appropriate. In a study that looked at 2,000 child-directed websites in the European Union and the United States, Moti et al. (2023) found that 90 percent of these sites embedded trackers and 27 percent contained targeted advertising – practices that require parental or verifiable parental consent under the EU GDPR and the US Children's Online Privacy Protection Rule respectively.[29]

v. Appointment of a Data Protection Officer

Around eight data fiduciaries had more than 25 million (2.5 crore) users each, indicating that they may be notified as significant data fiduciaries (SDFs). The DPDPA requires each SDF to appoint a data protection officer, who must be based in India to represent the SDF under the provisions of the Act, serve as the point of contact for data protection-related grievances, and be answerable to the governing body of the organisation.

Overall, most of the respondents, including the experts, pointed out that hiring a data protection officer would be moderately to extremely difficult. Respondents noted that the challenge to onboarding such a person lay in the fact that he or she had to be relatively senior and have significant experience and expertise – a difficult combination to find in the market. In addition, some respondents highlighted the fact that there would be significant competition between organisations for such resources.

vi. Lack of Clarity for Implementation

The majority of the respondents (61 percent) lacked clarity regarding their obligations under the DPDPA in India, largely because a substantive portion of the Act is going to be outlined by rules.

Some respondents noted that prior experience in data protection does not give a company an advantage for implementation of the Act. This is because the DPDPA is not interoperable with data protection requirements in other jurisdictions; in other words, the compliance modalities are not the same. Moreover, firms with prior experience have local teams with localised experience of managing compliance with the DPDPA; they do not have the knowhow with regard to the implementation of data protection laws in other countries.

FIGURE 7

A majority of data fiduciaries are unclear about the DPDPA obligations and compliance mechanisms

Note:13 data iduciaries participated in the survey on this question. *Source: Author's Own*

Existing literature shows there can also be lack of clarity regarding the terms within the data protection law and this can pose a challenge to compliance (Sirur, Nurse, and Webb, 2018). In other jurisdictions, such as the European Union, clarity is ensured by the presence of the national Data Protection Authorities and the European Data Protection Supervisor, who provide guidance on interpretation of the GDPR. However, there is no such clarifying authority under the DPDPA. The Data Protection Board is primarily meant to act on instances of non-compliance that are brought to its notice and has been provided with no clarificatory/ interpretive powers or jurisdiction. The absence of such an entity may create a guidance vacuum for firms in India, particularly for smaller enterprises that have little to no understanding of the data protection law.

vii. Timelines for Implementation

Overall, most data fiduciaries and experts indicated that, in aggregate, it would take entities around two years (24 months) or more to satisfactorily comply with the provisions of the DPDPA. A few organisations noted that they would be able to carry out the operations necessary for compliance with different provisions in parallel. This means the teams could be working simultaneously on figuring out how to deal with the notice and consent requirement as well as with verifiable consent at the same time. Others, however, indicated that they might not be able to undertake compliance with different provisions in parallel as they would have to assign or onboard resources based on the requirements of different provisions. Many organisations do not have large teams, particularly technical staff, at their disposal. They would, thus, have to prioritise accordingly and undertake compliance with different provisions sequentially (one after the other). Around 44 percent of the respondents said that it would take them up to 24 months to comply with the consent requirement, given the language considerations and their impact on technical architecture. Most firms that indicated shorter timelines, i.e. 6-12 months and 12-18 months, were the ones with no prior experience of data protection implementation. It is likely that the lack of experience has led to the suggestion of a more ambitious timeline for implementation.

The median timeline, suggested by inexperienced firms, for the implementation of the provisions related to the verifiable parental consent for children and persons with disabilities, was 18-24 months whereas experienced firms suggested it would take more than 24 months.

Both inexperienced and experienced firms indicated that it would take them 6-12 months to hire data protection officers.

FIGURE 8

Median implementation timelines for the DPDPA – firms with experience vs inexperienced firms

	Inexperienced firms	Experienced firms
Consent notices	12-18 MONTHS	18-24 MONTHS
Requirement for parental consent and persons with disabilities	18-24 MONTHS	MORE THAN 24 MONTHS
Appointing a data protection officer	6-12 MONTHS	6-12 MONTHS

Note:13 data iduciaries participated in the survey on this question. *Source: Author's Own*

Recommendations

i. **Provide a two-year timeline for the implementation of the DPDPA (from the time the rules are notified)**
This will follow the international best practices in Japan, Brazil, the US (California), and the European Union. It will also give firms of varying sizes and experience in India ample time to coordinate their internal processes and resources, and comply with different provisions effectively. To reiterate, while the firms with experience of implementing a data protection law and the ones with no experience differed on the timelines for consent notices, most of these converged on a 24-month timeline for the verifiable consent provision. Given that many firms may have to implement provisions sequentially due to resource constraints, it makes sense to allow a 24-month period for compliance. This timeline should begin from the time the rules are notified and finalised, as the crux of the implementation lies within them.

ii. **Observe a leniency period for 12 months after the initial 24-month timeline for implementation is over**
Leniency periods are common in other jurisdictions. To reiterate, most countries did not start seriously enforcing penalties and other sanctions under their data protection laws immediately after these came into force. In the European Union, there was an unofficial leniency period for nine months, whereas in Brazil, it extended up to two years. Given that some of the provisions of the DPDPA are particularly challenging to comply with, such as the obligation related to obtaining verifiable consent of a guardian of a disabled person, it may be prudent to accord to companies some amount of leniency so that they are not unnecessarily harassed by enforcement actions.

iii. **Refrain from making the notice and consent requirement overly prescriptive to reduce the technical and commercial burden on entities**
Ideally, entities should have the freedom to present notices in a manner that does not add friction to their consumer journey. If consent requirements are overly burdensome, respondents indicated that this might diminish the customer experience. It also adds to complication and cost of implementing the provision, which can be particularly burdensome for smaller organisations.

iv. **Allow data fiduciaries to decide on which languages to display consent notices in, based on an evaluation of customer needs**
This will ensure that no groups of data principals feel excluded due to the limited list of languages in the Eighth Schedule. It will also reduce some of the burden on smaller data fiduciaries, which may face a hard time complying with this requirement.

v. **Clarify the scope of the term, "person with disability", under Section 9 to mean only those persons who are severely mentally disabled or of unsound mind**

At present, the term, "person with disability", is not defined, indicating that the provision extends to both mentally and physically disabled persons. This provision is challenging because it may be difficult for firms to create a means to identify all kinds of disabled persons. In addition, it is also prejudicial to the rights of disabled persons that are competent to contract, and therefore, required by law to be treated equally with those who are not disabled.

vi. **Establish a mechanism for clarification of terms and provisions under the DPDPA, such as regular open-house discussions**

There is currently no authority that can provide clarity regarding the scope of terms and obligations under the DPDPA. This can be a considerable challenge, particularly for smaller entities. Surveys on other countries show that even when there are authorities in place and rules are promulgated, entities may face a hard time understanding the scope of their obligations. The experience of other countries reveals that a clarificatory authority is indispensable for the successful implementation of a data protection law. As such, the Indian Government must consider ways to introduce a similar mechanism or, at the very least, provide some channel of communication through which clarifications may be sought.

vii. **Ensure a consultation period of at least 60 days for the rules made under the DPDPA**

To enhance clarity and facilitate effective implementation of the DPDPA and its associated rules, it is crucial to allocate ample time for consultation. For example, in Japan, the consultation period for the amendments to the APPI started 11 months before they were formally implemented. As highlighted in this document, the introduction of a data protection law necessitates coordination across various segments within an organisation, including business, technical, and legal departments. For multinational corporations, this coordination also involves their global teams. Adequate time is needed for these stakeholders to understand the impact of the new provisions and offer constructive feedback on their implementation. Additionally, longer consultation periods tend to be more inclusive. Smaller companies and entrepreneurs, who may lack awareness or resources, often find it challenging to engage in consultations with shorter response periods. Extending the timeline for consultation can provide an opportunity to such groups to share their perspectives.

Endnotes

1. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'. arXiv, 22 August 2018. http://arxiv.org/abs/1808.07338.
2. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
3. Kvale, Steinar. 'Ten Standard Objections to Qualitative Research Interviews'. Journal of Phenomenological Psychology25, no. 2 (1994): 147–73. https://doi.org/10.1163/156916294X00016.
4. Gubrium, Jaber, James Holstein, Amir Marvasti, and Karyn McKinney. The SAGE Handbook of Interview Research: The Complexity of the Craft. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2012. https://doi.org/10.4135/9781452218403.
5. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
6. Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies'. Computer Law & Security Review 34, no. 1 (February 2018): 134–53. https://doi.org/10.1016/j.clsr.2017.05.015.
7. Addis, Maria Chiara and Kutar, Maria, "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness" (2018). UK Academy for Information Systems Conference Proceedings 2018. 29. https://aisel.aisnet.org/ukais2018/29
8. Addis, Maria Chiara and Kutar, Maria, "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness"
9. Article 29 Data Protection Working Party. Statement on the 2016 Action Plan for the Implementation of the General Data Protection Regulation (GDPR), 2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf.
10. Erin Hillard, The GDPR: A Retrospective Look at the First Two Years, Berkley Technology Law Journal, 2020, https://btlj.org/wp-content/uploads/2022/01/0012-35-4-Hilliard.pdf
11. Erin Hillard, The GDPR: A Retrospective Look at the First Two Years.
12. Erin Hillard, The GDPR: A Retrospective Look at the First Two Years.
13. 'Brazil's Data Protection Law Will Be Effective After All, But Enforcement Provisions Delayed Until August 2021 | Insights | Greenberg Traurig LLP'. Accessed 9 January 2024. https://www.gtlaw.com/en/insights/2020/8/brazils-data-protection-law-effective-enforcement-provisions-delayed-august-2021.
14. International Network of Privacy Law Professionals. 'Brazil's Data Protection Law: A Brief Overview', 3 February 2021. https://inplp.com/latest-news/article/brazils-data-protection-law-a-brief-overview/.
15. 'Promulgation of the Amendment Act of the Act on the Protection of Personal Information, Etc. (12th June, 2020) |PPC Personal Information Protection Commission,Japan'. Personal Information Protection Commission Japan, 18 June 2020. https://www.ppc.go.jp/en/news/archives/2020/20200618/
16. "Personally referable information" is information which relates to a living individual but does not constitute personal information, pseudonymously processed information, or anonymously processed information. For example, website viewing history or information on operating system usage.
17. 'Amended Japan Privacy Law Will Come into Effect in April 2022 - O'Melveny', 16 November 2021. https://www.omm.com/insights/alerts-publications/amended-japan-privacy-law-will-come-into-effect-in-april-2022/.

18. Casetest.com (n.d.) California Civil Code § 1798.185. Available at: https://casetext.com/statute/california-codes/california-civil-code/division-3-obligations/part-4-obligations-arising-from-particular-transactions/title-1815-california-consumer-privacy-act-of-2018/section-1798185-effective-112024-regulations
19. Casetest.com (n.d.) California Civil Code § 1798.185.
20. California Legislative Information (n.d.) SB-1121 California Consumer Privacy Act of 2018. Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
21. Casetest.com (n.d.) California Civil Code § 1798.185.
22. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
23. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
24. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
25. Sirur, Sean, Jason R. C. Nurse, and Helena Webb. 'Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)'.
26. CNBCTV18. 'Only 24,821 People in India Have Sanskrit as Mother Tongue', 28 September 2022. https://www.cnbctv18.com/india/only-24821-people-in-india-have-sanskrit-as-mother-tongue-govt-data-14819891.htm.
27. Padmanabhan, Aishwarya. 'Unsoundness of Mind in Contract'. Manupatra, n.d. https://www.manupatra.com/roundup/325/Articles/Unsoundness%20of%20Mind%20in%20Contract.pdf.
28. Mishra, Siddhant, and Abhijit Mishra. "E-Contract in India: The Legal Framework, Issues, and Challenges." Issue 5 Indian JL & Legal Rsch. 4 (2022): 1.
29. Moti, Zahra, Asuman Senol, Hamid Bostani, Frederik Zuiderveen Borgesius, Veelasha Moonsamy, Arunesh Mathur, and Gunes Acar. 'Targeted and Troublesome: Tracking and Advertising on Children's Websites'. arXiv, 10 December 2023. http://arxiv.org/abs/2308.04887.