# Essential Factors for an Efficient Consent Management Framework

## Wadhwani Centre for Government Digital Transformation (WGDT)

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

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

## Table of Contents

# List of Tables

# Executive Summary

This paper delves into the realm of consent in the context of digital personal data protection in India, specifically examining the Digital Personal Data Protection (DPDP) Act of 2023. This landmark legislation aims to oversee the collection, storage, and processing of personal data, with a focus on transparency, consent, and robust data protection protocols. The paper is structured into three distinct sections, each dedicated to enhancing the framework of consent mechanisms.

### Section A: Operational Definition of Consent and Related Challenges

Initially, the paper sets out to define consent operationally, aligning this definition with global data protection standards. It highlights the essential characteristics of consent as outlined in Article 6(1) of the DPDP Act: freely given, specific, informed, unconditional, and unambiguous. The section further delves into three predominant challenges plaguing current consent mechanisms: unwitting, coerced, and incapacitated consent. Unwitting consent is often a result of convoluted terms and conditions, coerced consent emerges from manipulative practices or undue pressure, and incapacitated consent pertains to individuals, such as minors, who are legally unable to give consent.

### Section B: Exploring Various Consent Mechanisms

In this segment, the paper introduces and evaluates two primary consent mechanisms: broad consent and precise consent. While broad consent offers wide-ranging coverage, it runs the risk of insufficient communication with data principals, potentially leading to unwitting consent. Precise consent, on the other hand, allows for detailed user control but may encounter practical difficulties and might not fully address the issue of coerced consent. The section also discusses the role of Consent Management Platforms (CMPs) in maintaining adherence to data privacy regulations.

### Section C: Framework for Consent Mechanism

The concluding section proposes a detailed framework for consent management, addressing the issues raised in the previous sections. This framework incorporates elements crucial for effective consent, including strategies for obtaining and verifying consent, considerations for consent storage, methods for consent modification, and mechanisms for grievance resolution. It strives to be in harmony with the DPDP Act and incorporates international best practices. The focus is on user-centric consent notices,

combating coerced consent through clear transparency, and establishing solid channels for grievance redressal.

Overall, the paper offers insightful perspectives on the intricacies of consent mechanisms within the framework of India's DPDP Act and presents actionable recommendations for policymakers to consider.

# 1. Introduction

India's Digital Personal Data Protection (DPDP) Act was passed by the parliament on 11 August 2023. It is a noteworthy progress in the area of digital legislations, and it aims to regulate the collection, storage, processing, and transfer of personal data by entities, emphasizing consent, transparency, and data protection measures. DPDP Act mandates all the data processors to process the personal data only after obtaining a due consent from the user (here after, Data Principal). The Act asserts that any consent request to process the personal data should be accompanied by a notice explaining the purpose of collection the data, rights of the data principal and mechanisms for grievance redressal. However, guidelines for enforcing the DPDP Act have not been established, and consequently, a comprehensive consent management framework is still pending formulation.

Wadhwani Centre for Government Digital Transformation (WGDT), with its research on the consent mechanism proposes necessary factors in drafting a consent management framework aiming to keep the consent mechanism contextual and protect the democratic principles of the nation. This paper is divided into three sections. Section A provides an operational definition of the consent and a detailed explanation of the problems with the consent mechanism. Section B provides factors that had to be avoided while drafting a consent mechanism. Section C recommends necessary factors in making a consent management framework.

# 2. Section A: Consent - Operational Definition and Issues

## 2.1 Operational Definition of Consent

Table 1 presents the definition of 'consent' as explicitly outlined by various countries. In cases where the respective legislations do not provide a direct definition, the table instead details the key characteristics of consent as inferred from these laws." The common factors in the definitions and the key features are identified and have been adopted to put forward an operational definition.

***Table 1*** *Definitions and Key Factors of Consent across Select Countries*

| Legislation | Definition and operation of Consent |
|---|---|
| Article 4(11) of GDPR[1] | 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her |
| Article 6 (1) of Canada's Personal Information Protection and Electronic Documents Act[2] | The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. |
| Article 14 of China's The Personal Information Protection Law[3] | Consent shall be given by the individual concerned in a voluntary and explicit manner in the condition of full knowledge. If laws and administrative regulations provide that the processing of personal information shall be subject to the individual's separate consent or written consent, such provisions shall prevail. |
| Commissioner's Australian Privacy Protection Guidelines[4] | **Key elements of consent:**<br>• The individual is adequately informed before giving consent.<br>• The individual gives consent voluntarily.<br>• The consent is current (that is, the consent may be withdrawn and has not been withdrawn) and specific to the privacy affecting activity.<br>• The individual has the capacity to understand and communicate their consent. |

[1] General Data Protection Regulation (GDPR). "Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR)," March 29, 2018. https://gdpr-info.eu/art-4-gdpr/.
[2] "Personal Information Protection and Electronic Documents Act." Government of Canda. Accessed November 26, 2023. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416889.
[3] Briefing, China. "The PRC Personal Information Protection Law (Final): A Full Translation." China Briefing News, December 29, 2021. https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.
[4] Leonard, Peter. "Australian Data Protection and Privacy Laws A Primer." Data Synergies, 2019. https://iabaustralia.com.au/wp-content/uploads/2019/08/Australian-Privacy-and-Data-Protection-Law_A-Primer_2019_Peter-Leonard_Data-Synergies.pdf.

| Legislation | Definition and operation of Consent |
|---|---|
| Brazil's General Data Protection Law[5] | Consent is free, informed, and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data. |

The Data legislation of European Union, China, Canada, Brazil, and Australia emphasize on the factors – free, knowledge, specific, and unambiguous in defining the way the consent is provided. These factors have already been considered by the DPDP Act in its Section 6 (1), making the consent provision in line with the factors adopted by the other existing legislations worldwide.

Section 6 (1) of DPDP - *The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purposes.*

However, the consent itself is not defined in all the data protection legislations except the EU's GDPR and Brazil's General Data Protection Law, as mentioned in the Table 1. To enact the DPDP Act, a proper operational definition is required. Considering the factors that are adopted in making and executing a consent by various data legislations, the following operational definition is proposed.

***An Operational Definition of Consent*** – A conscious, and voluntary agreement by a written statement or by a clear affirmative action between the data principal and data fiduciary/data processor for the processing of personal data of data principal, where both the parties are equally aware of the purpose/use of the collected data, the envisaged outcomes, and the possible risks.

## 2.2 Identified Problems in Consent Mechanism

Even if we have the operational definition of the consent, it is crucial to identify the issues of consent mechanism within the context of enacting DPDP Act, primarily due to the lack of model consent mechanisms. The practices adopted by companies to gather consent from the Data Principals, in general are alleged

[5] "Brazilian General Data Protection Law." National Congress, 2019. https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf.

to be illusionary with limited alternatives.[6] Some scholars argue that the current consent mechanism is weaker in protecting the data principal data and privacy.[7] Numerous situations exist where individuals face an onslaught of consent requests, leaving them with little option but to accept terms and conditions to access services. These reasons further reiterate the necessity to look into the current problems arising due to the consent mechanisms. This section explores three major challenges arising from lax consent mechanisms.[8]

### 2.2.1 Unwitting Consent

Unwitting consent occurs when the Data Principal consents to use his/her personal data without any knowledge about the data processing, associated risks, and further disclosure of the data by the service providers. For example, Data Principals grants consent to online services including social media platforms without a comprehensive understanding of the intricacies of data collection or the potential outcomes of such data usage on their decision making and behavioral development. Many people are often unaware of the data practices and unsure of what they are agreeing to while availing the services digitally.[9] Thus, a data principal is forced to give her consent before experiencing.

Unwitting consent typically arises when consumers or data principals are faced with several challenges, including:

a. **Lengthy and legally complex terms and conditions:** The documents containing the terms are often extensive and filled with legal terminology, making it difficult for individuals to comprehend the details.
b. **Lack of understanding of technology:** Data principals may not fully grasp the technology that facilitates the interaction between themselves and the service provider, resulting in consent given before fully understanding the application.

*Illustration:*

[6] World Economic Forum. "Redesigning Data Privacy: Reimagining Notice & Consent for Human technology Interaction." World Economic Forum, 2020. https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.
[7] Kemp, Katharine, and Ross P. Buckley. "Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model." Georgetown Journal of International Affairs 18, no. 3 (2017): 35. http://www.jstor.org/stable/26395922.
[8] Richards, N., & Hartzog, W. (2019). The pathologies of digital consent. Washington University Law Review, 96(6), 1461-1504.
[9] Kemp, Katharine, and Ross P. Buckley. "Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model." Georgetown Journal of International Affairs 18, no. 3 (2017): 38. http://www.jstor.org/stable/26395922.

The scandal of Cambridge Analytica: Facebook users unknowingly consented to the collection of their personal data and their friends' data through a third-party app called "This Is Your Digital Life." The users were not fully aware of how their data would be used for political profiling and targeting during the 2016 U.S. Presidential election.[10]

a. **Challenges in assessing future risks:** It can be challenging to foresee and evaluate the potential risks associated with granting consent, leading to a lack of awareness regarding the implications of their consent.
b. **Timing of the consent:** The consent notices are shown prior making any registration for the application or service.[11] Only after using the applications or services, data principals are more likely to understand the data processing and associated risks.[12] This makes the data principal to give consent before understanding the risks.

### 2.2.2 Coerced Consent

Coerced consent is a situation where individuals are pressured into providing consent due to high opportunity costs or the use of manipulative techniques by the data fiduciary, such as dark patterns, to obtain their consent. For instance, if a person does not want to agree to the terms of an application, the available alternatives may offer similar terms, leaving him/her with limited choices. Leaving aside the similar consent forms of the alternatives service providers, the platforms offer consent notices which are unilateral, where there is no negotiation in the consent agreements but an imposition of agreements from the service provider.[13] In this scenario, the person is compelled to consent because if the data principal makes a choice of not consenting, s/he might be denied access to the service.

Another way of forcing consent is the usage of dark patterns which are same as defined by the Guidelines for Preventions and Regulation of Dark Patterns released by the Ministry of Consumer Affairs. Dark patterns are -

[10] Curzi, Corallina Lopez. "Facebook Users Now Know If They Were Affected by the Cambridge Analyticia Scandal. What Next?" EachOther, March 17, 2020. https://eachother.org.uk/cambridge-analytica-scandal-matter/
[11] World Economic Forum. "Redesigning Data Privacy: Reimagining Notice & Consent for Humantechnology Interaction." World Economic Forum, 2020. https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.
[12] Ibid. P 7
[13] Stasi, Maria Luisa. "Social Media Platforms and Content Exposure: How to Restore Users' Control." Competition and Regulation in Network Industries 20, no. 1 (March 2019): 86–110. https://doi.org/10.1177/1783591719847545.

"*any practices or deceptive design patterns using UI/UX (user interface/user experience) interactions on any platform; designed to mislead or trick users to do something they originally did not intend or want to do; by subverting or impairing the consumer autonomy, decision making or choice; amounting to misleading advertisement or unfair trade practice or violation of consumer rights*"[14]

*Illustration:*

One of the common dark patterns used in consent mechanism is while deploying website cookies.[15] Cookie consent forms generally display the button "Accept All" in an easy manner and while the data principal decides to manage cookies, the process becomes confusing.[16] It is reported that most of the data principals click on 'Accept All,' to avoid the consent banner and also when the other options are not displayed in the first instance of the notice.[17] This shows that cookie consent management mechanism should adopt practices that provide the three options 'Accept none of the cookies,' 'Accept select cookies,' and 'Accept all cookies' equal design importance.

### 2.2.3 Incapacitated Consent

Incapacitated consent occurs when individuals are not legally eligible to provide consent, but under certain laws, only a select age group is restricted.[18] For example, the Children's Online Privacy Protection Act of 1998 (COPPA) of the USA, only regulates the data collection of children under the age 13. Though the legal age for consent in the US is 18, individuals aged 13–18 are able to provide contractual consent for the purpose of data collection.[19] In India, this is not the case as to the Care and Protection of Children Act, 2015, categorises individuals under the age of 18 as children. Further, the legal age where an individual could provide valid consent is also 18 years.

[14] Department of Consumer Affairs. "Guidelines for Prevention and Regulation of Dark Patterns." Department of Consumer Affairs, 2023. https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf.

[15] Habib, Hana, Megan Li, Ellie Young, and Lorrie Cranor. "'Okay, Whatever': An Evaluation of Cookie Consent Interfaces." CHI Conference on Human Factors in Computing Systems, April 29, 2022. https://doi.org/10.1145/3491102.3501985.

[16] Ibid

[17] Ibid

[18] Richards, N. The pathologies of digital consent.

[19] Ibid

As per Article 9 of the DPDP Act, data fiduciaries must seek consent from the guardian or parents to process personal data of children. This asserts that everyone under the age of 18 shall have a dual consent mechanism to share their personal information, which would in turn means they would require in most of the cases the consent of parents for the online registrations.

Issue arises when the children circumvent the consent mechanism. Instances of children making the in-app purchases through the parent's credit cards have been well reported.[20] The problems are identified even in the usage of dating apps, and social media. Adolescents, who bypass the age verification to use dating apps are reported to be closer to the dangers of sexually transmitted diseases, dating violence, and mental health issues.[21] School going children using social media often could not control their usage leading to disturbances in their growth and lifestyle.[22] These instances show that the consent mechanism even for the incapacitated population should be redesigned to get a proper consent verification.

***Table 2*** *Consent problems and Factors of consent*

| Problem Identified | Factor |
|---|---|
| Data principals will have difficulty in understanding the consent notice because of the legal jargon, technical terms used in the explanation of data processing and because of the habitual action of clicking 'Yes' to the consent notices. | Unwitted consent |
| • Data principal has no alternatives while providing a consent for a particular service, making it a necessary consent. | Coerced consent |

[20] Arthur, Charles. "Apple Faces Multimillion US Settlement over 'in-App Purchases' by Children." the Guardian, December 29, 2017. https://www.theguardian.com/technology/2013/feb/26/apple-settlement-children-in-app-purchases.

[21] Chakravarty, Rahul, Gopika Jagota, and Swapnajeet Sahoo. "Impact of Online Dating on the Adolescent Population: A Brief Review of the Literature with Special Reference to the Indian Scenario." Consortium Psychiatricum 4, no. 3 (September 29, 2023): 65–70. https://doi.org/10.17816/cp222.

[22] Vadher, Sneha B, Bharat N Panchal, Ashok U Vala, Imran J Ratnani, Kinjal J Vasava, Rishi S Desai, and Aayushi H Shah. "Predictors of Problematic Internet Use in School Going Adolescents of Bhavnagar, India." International Journal of Social Psychiatry 65, no. 2 (February 11, 2019): 151–57. https://doi.org/10.1177/0020764019827985.

| Problem Identified | Factor |
|---|---|
| • Dark patterns such as nagging are employed to get consent[23] | |
| Validity of consent among students and children | Incapacitated consent |

# 3. Section B: Consent Mechanism –Available Forms

## 3.1 Different forms of Consent Mechanism

The identified challenges of consent are partly solved by the two mechanisms – **broad consent** and **precise consent**. They have emerged as pivotal frameworks, shaping the ethical and legal dimensions of data utilization. Broad consent, a comprehensive approach, seeks to encompass a wide spectrum of potential uses for collected data, providing flexibility for unforeseen research endeavours. On the other hand, precise consent emphasizes granular control, allowing individuals to specifically tailor their permissions, thus safeguarding privacy with surgical precision.

In both the broad and precise consent mechanisms, incapacitated consent can be avoided by using government digital ids of the citizens like Digilocker to ascertain the age and use other established methods such as Email verification or through One Time Password (OTP) verification to get consent form the parents. Further, the difficulties with both the approaches are provided below.

### 3.1.1 Broad Consent

One of the many ways to protect data principal privacy and liberty is to allow broad consent to be the first step in processing or collecting personal data.

*Factors difficult to Incorporate:*

1. Broad consent allows companies to bombard the data principal with pages of information regarding the data usage, which in most of the cases are ignored because of lack of time, tough language, requirement of service, and other circumstances. This makes data principal consent an unwitted one.

[23] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November 6). (Un)informed Consent. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3319535.3354212

2. Broad consent will allow companies offering similar digital services to have a similar consent notice. In such a situation, Data Principal will be left with no alternative to choose from leading to a coerced consent.

### 3.1.2 Precise Consent

This approach asks data principals to consent to each distinct purpose or type of data usage separately. It provides more transparency and control to Data Principals over how their data is utilized but can be more time-consuming and complex.

*Factors difficult to incorporate*

1. In case of algorithmic services, it will be difficult to ascertain the exact use case of the personal data processing.[24] This will make the precise notices difficult. However, precise consent mechanism still allows data principals to have information/notice fatigue.
2. Coercive consent cannot be solved by precise consent, as the repeated notices would force the data principals to provide consent without reading the terms of data usages.

It is well documented that people have been habituated to click "I agree" without reading the consent notices, leave alone understanding it.[25] We must accept the reality that consent notices are not read by the data principals before consenting.[26] In case of precise consent, constant notices will give rise to consent fatigue. Perhaps, an alternative way is to have consent managers to take the onus of understanding the consent and help data principals to take more informed decisions.

## 3.2 Alternative Consent Route - Consent Managers

Consent management platforms (CMPs) as mentioned in the GDPR or consent managers, as mentioned in the DPDP Act are third parties who use tools to manage individual consents for various entities while ensuring compliance with data privacy regulation. The consent managers would act as mediators

[24] Giannopoulou, Alexandra. "Algorithmic Systems: The Consent Is in the Detail?" Internet Policy Review 9, no. 1 (March 23, 2020). https://doi.org/10.14763/2020.1.1452.
[25] Machuletz, Dominique, and Rainer Böhme. "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR." Proceedings on Privacy Enhancing Technologies 2020, no. 2 (April 1, 2020): 481–98. https://doi.org/10.2478/popets-2020-0037.
[26] This assertion is an outcome of the consultative workshop that has been conducted with practitioners, industry and academia.

facilitating the communication between the data principal and the data fiduciary.

The Combined Annual Growth Rate (CAGR) growth rate of the consent managers is estimated to be 19.3% and the market value would grow from USD 317 million in 2020 to USD 765 million in 2025.[27] According to another market research report, consent management market would grow at CAGR 20.4% from 2022 – 2030.[28] This shows that the consent manager platforms are operational and are set to capture the open market as in when the data legislations are enacted. These platforms can adopt any of the consent practices mentioned above as per the mandate provided by the data principal. However, skepticism has been noted where consent managers use the data for their own benefit.[29]

***Table 3*** *Analysis of the Factors to be incorporated by Consent Managers*

| Factors difficult to incorporate | Factors easy to incorporate |
|---|---|
| Coerced consent problem cannot be addressed as the consent management platforms only ensures that the companies are complying with the data regulations. | As the consent managers' sole purpose is to provide compliance with the data legislations, they would do a fair job in avoiding dark patterns (a part of coerced consent) and ensuring a level playing field for drafting the consent between the two parties. |

[27] MarketsandMarkets. "Consent Management Market Growth Drivers & Opportunities | MarketsandMarkets," 2020. https://www.marketsandmarkets.com/Market-Reports/consent-management-market-68100621.html.

[28] The Insight Partners. "Consent Management Market Growth Report - Opportunities & Forecast 2030," August 29, 2023. https://www.theinsightpartners.com/reports/consent-management-market.

[29] Toth, Michael, Nataliia Bielova, and Vincent Roca. "On Dark Patterns and Manipulation of Website Publishers by CMPs." *Proceedings on Privacy Enhancing Technologies* 2022, no. 3 (July 2022): 478–97. https://doi.org/10.56553/popets-2022-0082.

# 4. Section C: Consent Mechanism


***Figure 1:*** *Proposed Skeleton Framework of Consent Mechanism*

The framework delineates the consent process through a structured sequence comprising five distinct stages. In the initial stage, the approach of data fiduciaries is detailed, encompassing their method of engaging with data principals. This stage involves an examination of the current understanding of consent and the associated challenges. The second stage delves into the challenges inherent in consent notices and scrutinizes the way these notices are presented. The third stage, pertaining to storage, outlines the constraints imposed on data fiduciaries concerning the duration and geographical location of data storage. The fourth stage focuses on the modifications to consent made by the data principal, while the final stage addresses the mechanism for grievance redressal.

Each category is further expanded with necessary factors to be incorporated to make the consent mechanism an efficient one. Finally, a comprehensive recommendation involving the factors that are to be incorporated while making a consent mechanism framework is provided.

## A. Approach

**Table 4** Approach Stage - DPDP Act Challenges and Global practices

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| Section 4 (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,<br>(a) for which the Data Principal has given her consent; or<br>(b) for certain legitimate uses. | **Quasi Electronic Consent:**<br>The consent mechanism has been evolved from Browse Wrap to Click Wrap.[30] Browse wrap espouses that a data principal automatically provides his/her consent on the usage of application of any digital service. While the 'click wrap' mandates a click function to ensure that the data principal has explicitly given the consent. However, this approach towards consent becomes a problem as research points out that the consent notices are usually not read by the data principals.[31][32] This brings the problem that | No practices identified |

[30] Kamantauskas, Povilas. "Formation of click-wrap and browse-wrap contracts." Teises Apzvalga L. Rev. 12 (2015): 51.

[31] Lomas, Natasha . "Most EU Cookie 'Consent' Notices Are Meaningless or Manipulative, Study Finds," 2019. https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/.

[32] Statista. "Consumers Worldwide Who Read Online Consent Notices Entirely 2019," July 7, 2022. https://www.statista.com/statistics/1107860/global-consumers-read-consent-notices-entirely-online/.

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| | the traditional thought of 'click wrap' is no longer suitable in achieving meaning consent while availing digital services. | |
| | **Lack of Model consent:** There are no consent standards or model frameworks which the data fiduciaries could adopt. Every sector has differential understanding of the personal data and the model frameworks also will differ accordingly. | No practices identified |

**Recommendations**

1. To facilitate user control over their consent preferences, data fiduciaries/consent managers should be mandated to provide a clear and easily accessible mechanism where users can view and manage their consents. This mechanism should include options for users to easily revoke or modify their consent settings.
2. The mandate should also include maintenance of a comprehensive log of user consents and revocations. These logs should serve as critical evidence for grievance redressals, ensuring transparency and accountability in the data processing ecosystem.
3. Model sectoral consent notices should be provided, which can be issued by the data protection board in consultation with relevant authorities.

## B. Format of Consent

***Table 5*** *Consent Stage* - DPDP Act Challenges and Global practices

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| Section 5 (1) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her, (i) the personal data and the purpose for which the same is proposed to be processed; (ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and (iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed | **Unwitted consent:** Data principals do not understand the risks, and technical process even if it is mentioned in the consent notice. This is because of long notices, technical and legal jargon used in the consent notices. | No practices identified |
| | **Unwitted Consent:** Under section 5(1), consent notices are not mandated to provide sufficient and relevant details regarding the transfer of personal data to other parties. | a. Section 20 (1) of **Singapore's Personal Data Protection Act**[33] mandates an organisation to inform - (a) the purposes for the collection, use or disclosure of the personal data (as the case may be) on or before collecting the personal data (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or |

[33] "Personal Data Protection Act 2012 - Singapore Statutes Online," October 1, 2022. https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P14-#pr18-.

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| | | disclosure of the personal data for that purpose<br><br>**b. Canada's Office of Privacy Commissioner** in its guidelines for obtaining meaningful consent advices companies to provide details with whom the personal data will be shared with specifics.[34] |
| Section 6 (4) (4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given. | **Coercive consent:**<br>The persistent use of pre-selected boxes poses a significant challenge to the data principles, potentially leading to a lack of data principal awareness and control over their personal data. | **EU's GDPR** in its recital 25**,** clarifies that the usage of pre-selected boxes while asking for a data principal consent should be avoided.[35] |
| | **Coercive Consent: Dark Patterns**<br>Dark patterns can also be used to obtain consent from the data principal. One such practice observed is on | Central Consumer Protection Authority, on 30th November 2023, issued the guidelines for Prevention and Regulation of Dark Patterns, under the |

[34] Office of the Privacy Commissioner of Canada. "Guidelines for Obtaining Meaningful Consent," August 13, 2021. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

[35] ICO. "How Should We Obtain, Record and Manage Consent?," n.d. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/.

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| | the cookie consent notices, where the design of a cookie notice influences the decisions of data principals on whether to consent to data collection, as well as whether they recall seeing the notice at all.[36] | Consumer Protection Act, 2019.[37] |
| Section 9 (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. | **Consent Verification:** Consent mechanism to verify age and parent consent in case of minors using the digital services is generally a self-declared one, which provides low level of assurance and validity.[38] | **Children's Online Privacy Protection Rule of the US[39]:** Acceptable methods include having the parent: a. sign a consent form and send it back to you via fax, mail, or electronic scan; b. use a credit card, debit card, or other online payment system that provides notification of each |

[36] Borberg, Ida, Rene Hougaard, Willard Rafnsson, and Oksana Kulyk. "So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions." In Workshop on Usable Security and Privacy (USEC), vol. 3. 2022.

[37] Department of Consumer Affairs. "Guidelines for Prevention and Regulation of Dark Patterns." Department of Consumer Affairs, 2023. https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf.

[38] Hof, S. van der, and S. Ouburg. "'We Take Your Word For It' — A Review of Methods of Age Verification and Parental Consent in Digital Services." European Data Protection Law Review 8, no. 1 (2022): 61–72. https://doi.org/10.21552/edpl/2022/1/10.

[39] Federal Trade Commission. "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," July 17, 2020. https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4.

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| | | separate transaction to the account holder; c. call a toll-free number staffed by trained personnel; connect to trained personnel via a video conference;<br>d. provide a copy of a form of government issued ID that you check against a database, as long as you delete the identification from your records when you finish the verification process;<br>e. answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer;<br>f. Verify a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology. |

## Recommendations

### Clear and Plain Language of the Consent Notice

1. To enhance data principal comprehension and ensure informed consent, data fiduciaries should be encouraged to utilise visual or pictographic notices, especially where necessary, to effectively communicate risks to

data principals. Consent notices should also be accessible to persons with disabilities.

2. Consent notices should comprehensively disclose the entities with whom the data will be shared.

**Consent Practices**

3. The consent mechanism should strictly avoid coercive consent practices, drawing on global best practices. For example, the rules should explicitly prohibit the use of pre-ticked boxes in consent dialogues or notices.
4. Central Consumer Protection Authority, on 30 November 2023, issued the guidelines for Prevention and Regulation of Dark Patterns, under the Consumer Protection Act, 2019. These guidelines aim to regulate dark patterns and their impact on consumers within e-commerce. The rules or guidelines should recognize and address these dark patterns within the framework of consent management to protect individuals' rights and interests.
5. Cookies consent notice should display all the options including 'rejecting all the cookies,' 'accepting all the cookies,' and to select data principal interested cookies in a single page and they should be given equal importance in the design of user interface.

## C. Storage

***Table 6*** *Storage Stage* - DPDP Act Challenges and Global practices

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| Section 12 (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in | **Erasure of Data**<br>When the account is deleted or consent to process personal data is withdrawn, the data fiduciary is not advised or mandated to delete all the personal data and request all the parties with which the data has been shared or | **Section 17 (2) of GDPR** - Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost |

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| accordance with any requirement or procedure under any law for the time being in force | duplicated to be deleted. | of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. |
| | **Erasure of Data**<br>IP address, both the static and dynamic, identifiers provided by devices, cookie identifiers should not be stored as they can be used to directly identify the data principal. They should be stored or processed only after a due consent and as per the section 6 (1) of DPDP Act | **Recital 30 of GDPR** identifies online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags, as personal data.[40] |

## Recommendations

1. The rules expanding the consent mechanism should explicitly state that identifiers such as IP addresses, both static and dynamic, and cookie identifiers should not be stored without due consent, in accordance with Section 6(1) of the Data Protection and Privacy Laws. There should be clear

[40] General Data Protection Regulation (GDPR). "Recital 30 - Online Identifiers for Profiling and Identification - General Data Protection Regulation (GDPR)," September 2, 2019. https://gdpr-info.eu/recitals/no-30/.

guidelines on the conditions under which these identifiers can be stored or processed, ensuring that data principal consent is obtained and adhering to the principles of data protection.

## D. Modify

***Table 7*** *Modify Stage* - DPDP Act Challenges and Global practices

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| Section 12 (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force. | **Modification of Consent**<br>Many data fiduciaries currently lack a comprehensive and transparent mechanism that allows data principals to easily access and manage their consents. The challenge lies in addressing the existing deficiency where data principals may not have clear visibility into the consents they have provided, hindering their ability to make informed decisions about data processing activities. | No practices identified |

### Recommendations

1. The guidelines should promote to offer a data principal an option of deleting the personal data and account while deleting the application from an operating system. One way of doing it is to force developers to put an option of deleting the account from within the application. For example, App store

of Apple asserted that all the developers have to provide an option for the data principals to delete their account within the app.[41] This includes deletion of data principal generated data while the account was active.

2. The consent mechanism should incorporate comprehensive provisions for the erasure of personal data, aligning with global best practices. When an account is deleted or consent for data processing is withdrawn, data fiduciaries/consent managers should provide an option to delete all personal data and notify all parties with whom the data has been shared or duplicated to do the same.

## E. Grievance Redressal

***Table 8*** *Grievance Redressal Stage* - DPDP Act Challenges and Global practices

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| Section 13 (1) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act | **Grievance Redressal Mechanism**<br>One notable limitation within the current provision of the DPDP Act of India is the absence of explicit directives regarding the establishment of an online complaint filing platform or a physical complaint office accessible to the Data Principal in their residing location. While the Act emphasizes the right of a Data Principal to have readily available means of grievance | **Section 77 of GDPR** – Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes |

[41] "Offering Account Deletion in Your App - Support - Apple Developer," n.d. https://developer.apple.com/support/offering-account-deletion-in-your-app/.

| Bare Act | Challenges | Global Practices - Data Protection Legislations |
|---|---|---|
| and the rules made thereunder. (2) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section (1) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries. (3) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board. | redressal, it falls short in specifying the necessity for easily accessible and data principal-friendly online platforms or local complaint offices. | this Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78. |

## Recommendations

1. The consent mechanism should address grievances related to consent violations by incorporating violations such as coercive consent, especially those involving impractically long notices, adopt dark patterns like nagging by sending repeated consent notices even after the data principal provides their choice, as grounds for lodging complaints.
2. The Data Protection Board should be designated as the responsible authority at district, state, and central level for receiving and adjudicating complaints related to these violations, having an administrative structure similar to Right to Information Act. Further, the Data Protection Board should have an online platform to register complaints, which will also help in analysing the frequent issues pertaining to the consent.

## 5. Conclusion

This paper is aimed to provide recommendations to implement an efficient consent management framework. The initial sections provided an operational definition and identified the challenges faced by the current practices. The final section provided a streamlined and categorized consent mechanism process. It consists of a detailed assessment of the DPDP Act, the challenges it faces, and the possible solutions adopted by legislation worldwide.

To establish an efficient consent management system, Data Fiduciaries/Consent managers should ensure both parties have an equal understanding of the consent notice. Innovations in consent notice presentation are crucial, along with providing a consent management mechanism for data fiduciaries to manage consents at any time.

Within the consent notices, Data Fiduciaries should avoid the usage of pre ticked boxes, dark patterns in nudging the Data Principal into giving a consent. They should also disclose to whom the collected data is shared with. Guidelines or rules under DPDP Act should explicitly state that identifiers such as IP addresses, both static and dynamic, and cookie identifiers should not be stored without due consent. Additionally, the cookie consent notices should be displayed in a user-friendly manner where all the options are given equal weightage in the user interface design.

The efforts in making the consent notice more efficient should follow the effective consent verification process for age sensitive digital service delivery platforms. Government-controlled digital platforms like Digilocker can be considered for verification of age while ensuring the data minimization principle and avoidance of storage of data during the verification process. Only, the success and failure logs should be stored.

Finally, establish a grievance redressal system providing online and offline access for Data Principals to register complaints. An administrative structure similar to RTI Act can be considered for an efficient grievance redressal mechanism.

## About Authors:

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

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

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

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

WADHWANI FOUNDATION

www.wfglobal.org

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

ASIA | AFRICA | LATIN AMERICA