

# IMPORTANCE OF CONSENT: FUNDAMENTAL PRINCIPLE OF PRIVACY



Wednesday Wisdom  
27-08-2025

---

## 1. INTRODUCTION [1]:

Privacy is a fundamental human right that protects an individual's autonomy, dignity, and freedom[2]. A landmark moment in the global recognition of privacy came with the adoption of the Convention for the Protection of Individuals with regard to automatic processing of personal data on 28 January 1981 by the Council of Europe[3]. This was the first legally binding international treaty aimed specifically at safeguarding personal data. In recognition of this milestone, Data Privacy Day is celebrated annually on 28th January to raise awareness and promote best practices in data protection[4].

Today, the principle of consent lies at the heart of privacy discussions and one of the important conditions for collecting, processing and storing of personal data under data protection law. It empowers individuals to make informed choices about how their personal data is collected, used, and shared. This article explores the significance of choice and consent as a foundational principle of privacy, particularly in the digital age where data flows freely and often invisibly.

[1] The article reflects the general work of the authors and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.

[2] Justice K.S.Puttaswamy(Retd) vs Union of India 2019 (1) SCC 1

[3] [chrome-extension://efaidnbnmnibpcajpcglclefindmkaj/https://rm.coe.int/1680078b37](https://rm.coe.int/1680078b37)

[4] [https://en.wikipedia.org/wiki/Data\\_Privacy\\_Day](https://en.wikipedia.org/wiki/Data_Privacy_Day)

---

## 2. CHOICE AND CONSENT :

The principle of choice is fundamental to the concept of privacy. It refers to an individual's ability to make informed and voluntary decisions about how their personal data is collected, used, and shared. Choice empowers individuals to exercise control over their personal information, thereby safeguarding their autonomy and dignity in both physical and digital spaces.

Generally, individuals are offered choices in the form of opt-in or opt-out mechanisms, which are intended to allow active participation in the consent process. However, these options are often overly broad or vague, and in many cases, the individual may not have a meaningful ability to opt out. This is particularly true in the case of bundled consent, which obliges users to agree to multiple purposes simultaneously rather than allowing them to provide consent separately for specific uses of their data.

Consent and choice are frequently treated as interchangeable, yet they serve distinct but interconnected roles in privacy protection. Consent is a legal and ethical expression of the choice principle and it requires that individuals voluntarily agree to the collection, use, and disclosure of their personal information, based on clear and specific information. For consent to be valid, it must be informed, specific, and freely given, which in turn requires that real and unbundled choices be available[5].

[5] Article 7 and recital 32 of General Data Protection Regulation (GDPR)

---

### 3. TYPES OF CONSENT:

Consent is a key mechanism that enables individuals to exercise control over their personal data. However, not all consent is equal. The nature and quality of consent can vary depending on how it is obtained and the context in which it is given.

- **Explicit Consent:** It is clearly and unambiguously stated, either verbally or in writing. For example, checking a box that says "**I agree to the terms and conditions**" or signing a form authorizing the use of personal data. Data Protection law across nations requires[6], such explicit consent must be obtained on the basis of clear, understandable, and sufficient information regarding the purpose, scope, and consequences of the data processing ("**Informed Consent**").
- **Implied Consent:** It is inferred from a person's actions, behavior, or the circumstances. For example, when an individual includes their contact number or address in a résumé and submits it to a potential employer, it is implied that they have consented to the use of those details by the employer for the purpose of contacting them regarding employment opportunities.

[6] Refer Article on Consent Management across Nations- [https://www.linkedin.com/posts/ynz-legal\\_consent-management-provisions-across-nations-activity-7252305594232016896-rWDz?utm\\_source=social\\_share\\_send&utm\\_medium=member\\_desktop\\_web&rcm=ACoAAAO\\_91wBeFdGHqoGB6wsdptBaBJtfoi8lpg](https://www.linkedin.com/posts/ynz-legal_consent-management-provisions-across-nations-activity-7252305594232016896-rWDz?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAAAO_91wBeFdGHqoGB6wsdptBaBJtfoi8lpg)

---

## 4. ISSUES OF CONSENT IN CURRENT PRACTICE IN INDIA

- **Lack of informed consent:** Consent is frequently obtained in a bundled manner, where users must accept all terms and conditions collectively, without the ability to provide selective or purpose-specific consent for different types of data processing. In practice consent are sought through privacy policies which are often lengthy, complex, and filled with legal or technical jargon, making it challenging for the average user to fully comprehend the nature and implications of what they are consenting to.
- **No Choice Mechanism in the garb of Consent:** In numerous digital services, users are required to provide consent as a mandatory requirement to access essential services such as mobile apps, banking platforms, or government portals. This practice leads to forced consent, contradicting the internationally recognized principle that consent should be freely given and voluntary.
- **Lack of Accountability:** Until recently, India lacked a dedicated data protection authority to oversee whether organizations obtained and used consent lawfully. Many digital platforms collect data by requiring individuals to click an “I Agree” button, often relying on bundled consent that offers no meaningful choices and shifts the entire responsibility onto the individual providing consent. As a result, accountability for the misuse of personal data after consent is given has been minimal.

---

## 5. RECENT DEVELOPMENT OF DATA PROTECTION LAW IN INDIA:

The enactment of Digital Personal Data Protection Act, 2023 (DPDP Act)[7] in August 2023, represents a major advancement in India's data privacy framework, placing consent at the heart of personal data protection. Following are the key features of Consent under DPDP Act:

- 1. Nature of Consent:** The Act mandates that consent must be free, specific, informed, unconditional, and unambiguous. It should be given through clear affirmative action, ensuring that individuals are fully aware of what they are consenting to[8].
- 2. Consent Manager:** A significant innovation under the Act is the introduction of the Consent Manager, a registered entity with Data Protection Board that enables individuals to manage, monitor, and withdraw their consent across various platforms and service providers, promoting user control and transparency[9].
- 3. Right to withdraw Consent:** Individuals retain the right to withdraw their consent at any time. Upon withdrawal, data fiduciaries[10] are legally obligated to immediately stop processing the individual's personal data, reinforcing the principle of user autonomy[11].

[7]Refer Article on DPDP Act: [https://www.linkedin.com/posts/ynz-legal\\_the-dpdp-act-and-gdpr-provisions-distinction-ugcPost-7102624091517444096-t4tE?utm\\_source=social\\_share\\_send&utm\\_medium=member\\_desktop\\_web&rcm=ACoAAAO\\_91wBeFdGHqoGB6wsdptBaBJtfoi8lpg](https://www.linkedin.com/posts/ynz-legal_the-dpdp-act-and-gdpr-provisions-distinction-ugcPost-7102624091517444096-t4tE?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAAAO_91wBeFdGHqoGB6wsdptBaBJtfoi8lpg)

[8] Section 6(1) of DPDP Act.

[9] Section 2 (g) of DPDP Act.

[10] 2 (i) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

[11] Section 6(4) of DPDP Act.

---

**4. Purpose Limitation:** Consent must be obtained only for specific, clearly stated purposes. Processing data beyond these purposes is prohibited unless permitted under other lawful grounds provided by the Act, aligning with the principles of purpose limitation[12].

**5. Special provisions for children:** To protect the privacy of minors, the Act requires that consent for processing the personal data of individuals under the age of 18 must be obtained from a parent or legal guardian. This adds an extra layer of protection for children in the digital ecosystem[13].

## **6. KEY STEPS TOWARD EFFECTIVE CONSENT COMPLIANCE:**

**a. Notice to be accompanied with request for consent[14]:** For the purposes of complying with DPDP Act provisions related to consent it will require Data Fiduciary to provide written notice specifying:

- a.the type of personal data and the purpose for which the same is proposed to be processed;
- b.the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and
- c.the manner in which the Data Principal[15] may make a complaint to the Board,

[12] Section 5(1) (i) of DPDP Act.

[13] Section 9(1) of DPDP Act.

[14] Section 5(1) of DPDP Act

[15] Section 2(j) “Data Principal” means the individual to whom the personal data relates and where such individual is—

- (i) a child, includes the parents or lawful guardian of such a child;
- (ii) a person with disability, includes her lawful guardian, acting on her behalf;

---

**b. Implement purpose specific consent:** Instead of bundled consent, it is important that individuals are given choice to selectively agree to specific data processing activities, aligned with clearly defined purposes.

**c. Promote transparency and accountability:** Organizations collecting digital data shall maintain clear records of consent, provide easy options for users to withdraw consent, and communicate changes in data practices proactively.

## CONCLUSION:

While the introduction of the Digital Personal Data Protection Act, 2023 is a landmark development in India's privacy landscape, the actual practice of consent remains a work in progress. To ensure that consent goes beyond a mere formality and truly reflects user autonomy, it is essential to combine strong legal enforcement, increased public awareness, and responsible industry practices.

In May 2023, a groundbreaking GDPR fine exceeding €1.2 billion was imposed on Meta (formerly Facebook) by the Irish Data Protection Commission (DPC)[16] on U.S. tech giant Meta for unlawfully transferring personal data of EU users to the United States, marking one of the most significant milestones in the history of data protection enforcement. The DPDP Act, signals a similar regulatory approach in India. It empowers the Data Protection Board to impose monetary penalties of up to Rs. 250 crores[17] for each instance of non-compliance, including failure to take reasonable security safeguards, non-fulfilment of obligations relating to children's data, or breach of consent requirements.

DPDP Act is likely to be notified soon and therefore it is important that organizations approach consent compliance with seriousness rather than treating it as a mere box-ticking exercise. Consent must be embedded as a substantive, user-centric safeguard at the core of data processing practices.

[16] <https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/>

[17] Section 33(1) of India's Digital Personal Data Protection (DPDP) Act, 2023

For any feedback or response on this article, the authors can be reached on [priya.shahdeo@ynzgroup.co.in](mailto:priya.shahdeo@ynzgroup.co.in) and [atharva.amdekar@ynzgroup.co.in](mailto:atharva.amdekar@ynzgroup.co.in)

**Author: Priya Shahdeo**

Priya is a Senior Manager-Corporate Legal at YNZ Legal.

By qualification she has completed her Bachelor of Arts and Bachelor of Law from Bharati Vidyapeeth Deemed University, Pune.



**Co-author: Atharva Amdekar**

Atharva is an Associate at YNZ Legal. By qualification he is Bachelor of Commerce and Bachelor of Law from Mumbai University

