The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CONSENT UNDER THE DPDP ACT: A RIGHT IN NAME, A CHECKBOX IN PRACTICE

Sesha Pangam

INTRODUCTION

We live in an era in which our lives are intertwined with the digital world[1], where connectivity and convenience have come with new vulnerabilities. Cyberspace that simplifies an individual's life can also be used against it. While India holds the second-largest rapidly growing online population in the world, and prior to 2023, it did not have a framework or legislation to govern data protection for decades. India passed its first data protection law in August 2023.

Legal experts called it 'overdue' because it is India's first comprehensive data protection legislation. The Information Technology Act, 2000[2], and the Information Technology (Reasonable Security Practices Procedures and Sensitive Personal Data of Information) Rules, 2011[3], governed the rules of data protection before the DPDP Act 2023.

The Digital Personal Data Protection Act, 2023[4], was enacted to bring about change and replace scattered regulations across various acts and laws. It is a framework that governs data protection and classifies individuals as Data Principals, the persons to whom the personal data pertains. In simple terms they are the owner of the data. Another key term introduced by the Act is Data Fiduciaries, the entities that collect and process the data.

---

[1] https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights

[2] *The Information Technology Act, No. 21 of 2000, India Code (2000).*

[3] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, Apr. 11, 2011.*

[4] *The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).*

The term Data Processor simply means any individual, organization, or authority that processes private information on behalf of a data fiduciary. It creates obligations around how data can be collected, used, and stored. Moreover, it gives individuals the right to access[5], correct, and erase their personal data, and it is based on a foundational concept called CONSENT.

It is intended that no company can use your personal data without your knowledge and a signed formal contract, which simply means: You decide, You control, and You consent to your personal data.

Section 6 of the Act[6] lays down that the consent must be free, specific, informed, unconditional, and unambiguous. In simple terms, the Data Principals, who are individuals like you and me must be given a clear notice before any data is collected, explaining why it is being collected and how the consent can be withdrawn.

The Act also states that if a company asks for permission to collect, store, and then use your personal data, then the Data Fiduciary cannot penalize an individual for withdrawing their consent. Moreover, it cannot make access to the information go beyond what is strictly necessary for that service. For Instance, it cannot demand access to your contacts or photos. The Act is meant to ensure that the Data Principals are not pressured into sharing information that is not required.

OVERVIEW OF GDPR STATUTE

GDPR stands for General Data Protection Regulation. It is a law on data privacy which was passed by the European Union (EU) in 2018. It is regarded as the most thorough privacy legislation and is regarded as the worldwide standard for data protection laws. It gave European citizens rights over their personal data and imposed heavy penalties on companies that violated those rights.

This framework, outlined in the European General Data Protection Regulation, puts India in the company of countries that have data privacy and consent as rights. India's first comprehensive data protection act by the Ministry of Electronics and Information Technology.

[5] *Data Protection Laws in India, DLA Piper, https://www.dlapiperdataprotection.com*
[6] *Digital Personal Data Protection Act, No. 22 of 2023, § 6, INDIA CODE (2023).*

CONSENT is central to both laws, which state that companies cannot collect or use personal data without clear and informed consent. The burden lies mainly on two places that are the reasons and methods of processing the data.

LAWS AND PRINCIPLES OF CONSENT

Data privacy, consent, and internet autonomy of information have been issues before the Indian courts that are grappling with. Some statements provide the basic legal context to which the Act is to be read. Of all these, the Supreme Court's nine-judge bench privacy judgment in Justice K.S. Puttaswamy v. Union of India[7] is the most important.

The court unanimously ruled that the right to privacy is a fundamental right under Article 21 of the Constitution of India[8]. The Court recognized the concept of informational privacy. Moreover, the Puttaswamy judgment also introduced the Proportionality test for any state interference with privacy.

The Supreme Court in Shreya Singhal v Union of India (2015)[9] had ruled Section 66A of the Information Technology Act[10] as being vague and overbroad. In the case of Justice K.S. Puttaswamy v. Union of India (Aadhar) (2019)[11], the Supreme Court reaffirmed the parts of the Aadhaar framework that it had approved previously, but it ruled that private entities should not have access to the Aadhaar database and that consent to share sensitive personal data with the state should not automatically be extended to private companies.

A relevant judgment issued by the Delhi High Court was in Karmanya Singh Sareen v. Union of India (2017)[12] which came in the wake of WhatsApp's 2016 privacy policy that enabled access to WhatsApp data by Facebook. The Court held that the users who registered via one set of frames are experiencing different data practices without their consent.

THE CHECKBOX PROBLEM

[7] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).*
[8] *India Const. art. 21.*
[9] *Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).*
[10] *The Information Technology Act, No. 21 of 2000, India Code § 66A (2000).*
[11] *Justice K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (India).*
[12] *Karmanya Singh Sareen v. Union of India, (2017) 239 DLT 780 (India).*

Before the DPDP Act, 2023, India had no comprehensive rules on how companies were required to obtain your consent. Earlier, there were lengthy complicated privacy policies to sign with an 'I Agree' box. Button on it.

The Companies resorted to the use of very small and difficult-to-understand reject options pre-ticked. The checkbox problem was this. This is now directly addressed by the DPDP Act, 2023, and the DPDP Rules, 2025 dark patterns are now banned and pre-ticked boxes are not allowed. Companies will need to give consent notices in plain terms. To sum up, the success of the DPDP Act depends on several aspects, including statute participation in interactions with overseas data protection systems.

Finally, and most importantly, the DPDP Act is not only a technical regulation but a declaration of values regarding the problem of personal autonomy and privacy, as well as the value of personal data in society.