Page: 517-572 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 2

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.61

CONSENT MECHANISMS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A COMPARATIVE LEGAL ANALYSIS WITH GDPR AND CCPA/CPRA

Vedant Raj Chaurasiya[1]

I. ABSTRACT

Consent remains a foundational pillar in contemporary data protection frameworks, yet its normative basis, scope, and enforceability vary significantly across jurisdictions. India's enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) signals a shift towards a consent-centric model, but this framework departs in meaningful ways from the paradigms established under the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), as enhanced by the California Privacy Rights Act (CPRA). This paper conducts a structured comparative and doctrinal analysis to examine how each of these regimes conceptualizes consent, the role of enforcement mechanisms, and the degree of autonomy afforded to individuals.

The GDPR situates consent within a rights-based approach, requiring it to be freely given, informed, specific, and revocable—supported by institutional safeguards like independent data protection authorities and mandatory risk assessments. Conversely, the CCPA/CPRA reflects a consumer-choice model where transparency and opt-out functionality dominate, with consent obligations emerging only in limited scenarios. The DPDP Act, though framed around consent, weakens its efficacy by introducing expansive "deemed consent" provisions and lacking critical oversight tools such as mandatory Data Protection Impact Assessments (DPIAs) or a fully independent regulatory authority.

The analysis further explores the consequences of this design on India's cross-border data transfer capability, especially its divergence from GDPR adequacy standards.

[1] BBA LLB (Final Year – X Sem.), Amity Law School, Amity University Madhya Pradesh

Arguing for the evolution of a consent-plus architecture, this paper recommends enhancements such as fiduciary accountability, dynamic and context-sensitive consent models, and user interfaces tailored to India's socio-linguistic diversity. These interventions are imperative for strengthening user autonomy, enhancing legal coherence, and enabling India's data regime to stand alongside global best practices in digital rights governance.

II. KEYWORDS

Consent, Digital Personal Data Protection Act, DPDP Act, GDPR, CCPA/CPRA, Deemed Consent, Data Fiduciary, Cross-Border Data Transfers, Dynamic Consent, Data Protection Impact Assessment, Privacy Rights

III. INTRODUCTION

In an era increasingly defined by ubiquitous digital interaction and algorithmic governance, the legal significance of consent has been substantially reimagined. Once limited to contractual doctrines and informed decision-making in medicine, the idea of consent now occupies a central role in global data protection law. Its transformation is especially visible in regimes that attempt to balance individual autonomy with the demands of data-driven economies. Consent, when adequately safeguarded and operationalized, serves not merely as a procedural formality, but as a legal expression of personal sovereignty over informational identity[2].

India's response to the global demand for robust data protection came in the form of the Digital Personal Data Protection Act, 2023 (DPDP Act), which replaces a patchwork of prior regulations like the IT Rules, 2011. The DPDP Act represents a substantial leap forward, introducing statutory definitions of personal data, specifying rights of data principals, and mandating consent as the default basis for processing personal data[3]. It builds upon the constitutional foundation laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, wherein the Supreme Court declared privacy to be a fundamental right under Article 21 of the Constitution[4]. This

[2]DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 97 (Harvard University Press 2008).
[3] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 6 (India).
[4]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

jurisprudential shift compels a higher threshold for what counts as valid, meaningful consent in Indian data law.

The DPDP Act outlines consent as "free, specific, informed, unconditional and unambiguous"[5]—a definition that bears resemblance to international benchmarks such as the General Data Protection Regulation (GDPR) of the European Union. The GDPR defines consent as a "freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action"[6]. On the other hand, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), adopts an opt-out model, where the user must take affirmative steps to restrict the sale or sharing of personal data[7]. Unlike the GDPR's stringent opt-in regime, the CCPA emphasizes transparency and retrospective user control.

India's DPDP Act introduces a hybrid approach. While it mandates explicit consent for most forms of data processing, it also allows "*legitimate use without consent*" under specified circumstances, such as for state functions, legal compliance, or employment-related purposes[8]. This bifurcated model is conceptually similar to the "lawful bases" doctrine under Article 6 of the GDPR, where consent is only one of multiple grounds for lawful data processing[9]. However, questions remain about how informed and voluntary consent can be in a socio-digital context characterized by low data literacy, consent fatigue, and linguistic diversity.

Furthermore, the Act introduces the novel institutional mechanism of Consent Managers, aimed at enabling users to manage, review, and withdraw consent through interoperable platforms[10]. While the idea is progressive, its implementation details are currently sparse and have led to concerns about interoperability, standardization, and

[5] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 6(1) (India).
[6] Regulation (EU) 2016/679, art. 4(11), 2016 O.J. (L 119) 1, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj
[7] Cal. Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (West 2018); see also Cal. Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq. (West 2020).
[8] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 7 (India).
[9] Regulation 2016/679 of the European Parliament and of the Council, art. 6, 2016 O.J. (L 119) 1 (EU).
[10] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 6(5) (India).

potential misuse. Whether this will improve informed user control or devolve into another bureaucratic layer remains to be seen.

This paper aims to critically examine the consent architecture under the DPDP Act, by comparing it with the more established and operationalized models under the GDPR and the CCPA, as amended. The objective is not only to identify similarities and doctrinal differences, but to assess whether the Indian framework is normatively sound, procedurally robust, and pragmatically enforceable. Through this comparative lens, the study explores whether India's legal regime meets international standards or merely adopts the appearance of compliance without substantive empowerment of data principals.

Thus, this inquiry is not merely descriptive but evaluative. In asking whether India's consent mechanisms under the DPDP Act can withstand the pressures of digital asymmetry, corporate opacity, and weak enforcement, this paper situates the Indian law in its comparative and constitutional contexts. The following chapters will examine the conceptual, operational, and doctrinal dimensions of consent across jurisdictions and evaluate the efficacy of India's evolving data protection framework.

IV. LEGAL FOUNDATIONS AND EVOLUTION OF CONSENT IN DATA PROTECTION LAW

A. Conceptual Roots of Consent in Legal Philosophy

Consent, in its purest legal and philosophical sense, embodies the principle of personal autonomy—the right of individuals to exercise dominion over their bodies, actions, and, in the modern context, personal data. Traditionally rooted in the fields of contract law and medical ethics, consent has functioned as a gatekeeping device—signifying voluntary agreement to a proposed action or condition. Within the realm of data protection, this function has evolved to represent the individual's capacity to control the collection, use, and dissemination of their personal information[11].

This transformation of consent into a privacy-enabling mechanism is best understood through the lens of informational self-determination, a conceptual evolution that was

[11]Alan F. Westin, *Privacy and Freedom* 7 (Atheneum 1967).

first robustly articulated in German constitutional law, particularly through the landmark *Volkszählungsurteil* (Census Act Case) of 1983. In this case, the Bundesverfassungsgericht (Federal Constitutional Court of Germany) held that "a person who is unsure whether unusual behaviour is being recorded and permanently stored will try to avoid such behaviours" and that such uncertainty undermines the free development of personality protected under Article 2(1) in conjunction with Article 1(1) of the Basic Law.[12] The Court formally established the right to informational self-determination, asserting that individuals must be able to decide "when and within what limits information about their personal life should be communicated to others."[13] This doctrine not only shaped German national law but also deeply influenced European data protection standards.

The European Court of Human Rights (ECtHR) has similarly developed a robust jurisprudence under Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for "private and family life, home and correspondence." In *Klass v. Germany*,[14] the ECtHR recognized that surveillance measures—even when conducted for national security purposes—must be "necessary in a democratic society", and that individuals must be offered effective legal remedies to challenge such intrusion. Importantly, the Court stressed that the mere existence of secret surveillance powers could interfere with the enjoyment of the right to privacy, even if such powers are not actively used against a particular individual.[15]

This foundational reasoning was extended in *S. and Marper v. United Kingdom*,[16] where the Court held that the indefinite retention of DNA profiles and fingerprints of individuals acquitted of criminal charges violated Article 8. The ECtHR emphasized that consent cannot be presumed by silence or state discretion, and that data collection practices must be proportionate to the aims pursued. The judgment reaffirmed the

[12] *Volkszählungsurteil*, BVerfGE 65, 1, para. 155 (1983).
[13] *Id.*
[14] *Klass v. Germany*, App. No. 5029/71, Eur. Ct. H.R. (1978).
[15] *Id.* ¶¶ 49–50.
[16] *S. and Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. (2008).

principle that any interference with informational privacy must be justified by a pressing social need and subject to adequate safeguards.[17]

Further jurisprudential development occurred in *Bărbulescu v. Romania*,[18] where the Court ruled that an employer's monitoring of an employee's electronic communications without prior notification was a disproportionate infringement of the employee's right to privacy. The judgment clarified that individuals do not surrender their privacy rights merely by entering into private or professional relationships, and that clear, informed, and context-specific consent is indispensable for legitimate data processing.

These ECtHR decisions together crystallize the normative foundation of consent in European privacy law. They recognize that autonomy in the digital age demands not just the freedom to consent, but also the freedom from coercion, opacity, or procedural imbalance in how that consent is obtained. The ECtHR's standards of necessity, proportionality, and procedural fairness laid the groundwork for the General Data Protection Regulation (GDPR), particularly its emphasis on *freely given, specific, informed and unambiguous* consent under Article 4(11), and its robust accountability regime under Articles 5–7.

India's constitutional jurisprudence has gradually aligned with these global standards. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[19] the Indian Supreme Court recognized privacy as a fundamental right under Article 21 of the Constitution, situating informational self-determination within the broader rights to dignity and autonomy. Drawing inspiration from both *Volkszählungsurteil* and ECtHR decisions, the Court stated that "informational privacy is a facet of the right to privacy," and that the State bears a fiduciary duty in safeguarding personal data.

Thus, the evolution of consent from a contractually operative concept to a substantive constitutional safeguard is neither accidental nor jurisdiction-specific. It reflects a global legal consensus—that true consent in data protection must not merely be

[17] *S. and Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. (2008), ¶¶ 103–107.
[18] *Bărbulescu v. Romania*, App. No. 61496/08, Eur. Ct. H.R. (2017).
[19] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

obtained, but ethically constructed, voluntarily exercised, and institutionally protected.

B. Evolution of Consent in Global Data Protection Frameworks

Consent began to gain legal prominence in data protection statutes with the adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which emphasized individual participation and control[20]. These soft-law instruments laid the groundwork for binding frameworks such as the EU Data Protection Directive (Directive 95/46/EC), and later, the General Data Protection Regulation (GDPR), which codified stricter requirements for valid consent.

The GDPR, in particular, institutionalized consent as a lawful basis for processing under Article 6(1)(a), defining it narrowly under Article 4(11) and subjecting it to a host of conditions under Article 7. Consent under the GDPR must be**:**

- Freely given,
- Specific,
- Informed, and
- Unambiguous, expressed through affirmative action[21].

Moreover, the GDPR introduced the principle of granular consent, where data subjects must provide separate consents for distinct processing purposes. A pre-ticked box, silence, or inactivity no longer suffices[22]. Withdrawal of consent must be as easy as giving it, per Article 7(3).

In contrast, the California Consumer Privacy Act (CCPA) initially avoided placing strong emphasis on consent. Instead, it relied on a notice-and-opt-out regime. The California Privacy Rights Act (CPRA), effective in 2023, marked a conceptual shift in

[20]Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf (last visited May 24, 2025).

[21] Regulation 2016/679 of the European Parliament and of the Council, art. 4(11), 2016 O.J. (L 119) 1 (EU).

[22] Regulation 2016/679 of the European Parliament and of the Council, recital 32, 2016 O.J. (L 119) 1 (EU).

data privacy by expanding consumer rights and requiring businesses to offer opt-out mechanisms for the use of sensitive personal information and cross-context behavioural advertising[23]. However, it still does not demand affirmative consent for general data processing, thereby limiting its ability to fully empower consumers.

This divergence illustrates the two dominant models of consent globally:

- **The GDPR Model:** Emphasizing user agency and affirmative opt-in.
- **The CCPA/CPRA Model:** Leaning towards business flexibility with user transparency.

C. India's Consent Framework Prior to DPDP, 2023

Before the enactment of the DPDP Act, India's legal stance on consent was governed by a modest regulatory framework embedded in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under Section 43A of the IT Act, 2000[24]. These rules required companies to obtain consent in writing, via letter, fax or email, before collecting sensitive personal data. However, this model lacked granularity and enforceability. There was minimal guidance on withdrawal, layered consent, or purpose limitation.

Judicial recognition of the right to privacy in *Puttaswamy* further exposed the inadequacies of this regime[25]. Consent, in this pre-DPDP context, often operated more as a legal fiction than a substantive protection. The digital asymmetries in India—stemming from low literacy, language barriers, and the lack of meaningful alternatives—rendered consent neither truly informed nor voluntary.

This lacuna created the impetus for a more robust and codified framework, culminating in the passage of the DPDP Act in 2023. The Act attempts to bridge this historical gap, albeit with certain structural ambiguities.

[23] Cal. Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq. (West 2020).
[24] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, May 11, 2011 (India).
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

V. CONSENT UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A. Statutory Foundations and Core Definitions

The Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a structured, consent-centric framework for personal data governance in India, marking a decisive shift from the fragmented norms that existed under the Information Technology Act, 2000.

Section 6(1) of the DPDP Act defines consent as "*free, specific, informed, unconditional, and unambiguous*," to be provided through a "*clear affirmative action.*"[26] This definition rejects implicit consent and aligns India with global data protection benchmarks such as the GDPR, which also emphasizes affirmative, express consent.[27]

However, unlike the GDPR, which embeds consent within a broader web of purpose limitation, accountability, and supervisory oversight, the Indian Act vests operational responsibility in private actors and a new category of intermediaries called Consent Managers.

As per Section 6(5), Consent Managers are expected to provide data principals with the ability to manage, review, and withdraw consent across platforms.[28] This innovation was further clarified in the Draft Rules on the DPDP Act released by the Ministry of Electronics and Information Technology (MeitY) in January 2025, which outline eligibility conditions, grievance redressal procedures, and technological standards for Consent Managers under Rule 6(2) and Rule 10(1).[29]

While this model is progressive, the Act lacks detailed provisions regarding their interoperability standards, data architecture, or accountability mechanisms. This raises concerns about fragmentation, inconsistent user experiences, and limited

[26]Digital Personal Data Protection Act, No. 22 of 2023, § 6(1) (India).
[27]Regulation 2016/679 of the European Parliament and of the Council, art. 4(11), 2016 O.J. (L 119) 1 (EU), https://gdpr-info.eu/art-4-gdpr/ (last visited May 25, 2025).
[28]Digital Personal Data Protection Act, No. 22 of 2023, § 6(5) (India).
[29] Ministry of Electronics and Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act, 2023*, Rules 6(2), 10(1) (Jan. 2025), available at: https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf.

enforceability—issues also identified by the Justice B.N. Srikrishna Committee in 2018.[30]

One may argue that the statutory definition reflects the legislator's intent to integrate individual autonomy into data governance. However, its effectiveness hinges on procedural infrastructure that has yet to be clearly defined by subordinate rules or technical standards. Without uniform protocols for how Consent Managers must operate, the risk of inconsistent implementation and weakened user trust remains high.

Further, Section 9(2) of the Act introduces an additional safeguard in the context of children's personal data, prohibiting processing that is likely to cause any "detrimental effect on the well-being of a child", while also disallowing behavioural tracking or targeted advertising directed at children.[31] This provision reflects growing international recognition of the vulnerability of minors in digital environments and mandates stricter fiduciary obligations when handling their data.

B. Procedural Requirements and Challenges

Section 6(3) of the Act mandates that every request for consent must be preceded by a notice informing the data principal of the nature of personal data to be collected, its intended purpose, and available grievance redress mechanisms.[32]

Section 6(4) allows this notice to be communicated in any of the 22 languages listed in the Eighth Schedule of the Constitution.[33]

While the provision is inclusive on its face, its implementation relies heavily on private compliance. The statute does not obligate the data fiduciary to provide notice in a language the user actually understands; it merely allows such an option.

In India's context—characterized by linguistic plurality, low digital literacy, and urban–rural access divides—this can result in formal but ineffective consent. For

[30]. Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Gov't of India 2018), https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited May 25, 2025).
[31] Digital Personal Data Protection Act, No. 22 of 2023, § 9(2) (India).
[32]Digital Personal Data Protection Act, No. 22 of 2023, § 6(3) (India).
[33]Digital Personal Data Protection Act, No. 22 of 2023, § 6(4) (India).

instance, during the COVID-19 vaccination drive, the CoWIN portal was available only in English and Hindi at launch, creating a barrier to access for many rural and non-Hindi speaking users, particularly in the hinterland.[34] The Indian Express reported this language limitation as a significant factor contributing to vaccine inequity and consent comprehension failures. This undermines the statutory goal of informed decision-making under Section 6(3).

Section 6(5) of the Act also introduces Consent Managers, whose role is to enable individuals to manage, review, and withdraw consent in a user-friendly and interoperable manner.[35]

However, operational clarity on this mechanism is limited in the principal legislation. The MeitY Draft Rules of January 2025 provide additional detail, particularly Rule 10(1), which outlines the functional obligations of Consent Managers, including secure verification of user identity, secure data exchange protocols, audit mechanisms, and redressal frameworks.[36] Despite this elaboration, the rules do not yet specify interoperability standards or interface uniformity, thereby raising concerns about fragmented user experiences and inconsistent enforcement.

Section 6(6) recognizes the right to withdraw consent at any time and states that the procedure for withdrawal must be as easy as giving consent.[37]

However, the Act neither prescribes specific timelines for such withdrawal nor mandates audit trails or regulator-notified standards to document whether withdrawal requests were honoured in time.

---

[34]Indian Express, *Vaccine Inequity Gets Worse: Rural India, Smaller Hospitals Hit*, INDIAN EXPRESS (May 11, 2021), https://indianexpress.com/article/india/vaccine-inequity-gets-worse-rural-india-smaller-hospitals-hit-7310043/#:~:text=The%20unavailability%20of%20the%20CoWin%20portal%20in%20languages%20other%20than%20English%20is%20an%20inherent%20entry%20barrier (last visited June 5, 2025).

[35] Digital Personal Data Protection Act, No. 22 of 2023, § 6(5) (India).

[36] Ministry of Electronics & Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act, 2023*, Rule 10(1) (Jan. 2025), available at: https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf.

[37]Digital Personal Data Protection Act, No. 22 of 2023, § 6(6) (India).

In contrast, the GDPR under Article 7(3) not only mandates easy withdrawal but also requires prompt cessation of processing post-withdrawal.[38] In the absence of such procedural mandates, Indian data fiduciaries may technically enable withdrawal while introducing hidden friction—e.g., through multi-step processes, opaque dashboards, or delayed compliance.

Section 9 of the DPDP Act, significantly addresses the protection of children's data, in which it stipulates that processing personal data of children (defined as persons under the age of 18) or of persons with disabilities who require guardianship shall require verifiable consent from a parent or lawful guardian.[39]

Yet, the Act does not define what constitutes a "verifiable" mechanism, nor does it mandate a uniform procedure for obtaining or authenticating such consent. This opens the door to inconsistencies, especially when processing involves high-risk data sets like biometrics, geolocation, or behavioural profiling.

The MeitY Draft Rules of January 2025 attempt to plug this gap, especially regarding the functioning of Consent Managers. While not exclusively directed at children's data, Rule 4(2) suggests that Consent Managers must be interoperable across platforms and capable of supporting real-time consent logs.[40] However, the Rules stop short of detailing verification protocols, user interface standards, or enforcement timelines. This regulatory vagueness may be especially problematic when handling children's sensitive data, where legal obligations and ethical responsibilities should be more stringent.

These implementation ambiguities reveal a broader theme within the Act**:** the burden of meaningful implementation is shifted disproportionately to users, without corresponding institutional or enforcement support. A consent framework that appears robust on paper may fail in practice if critical actors—like Consent

[38]Regulation 2016/679 of the European Parliament and of the Council, art. 7(3), 2016 O.J. (L 119) 1 (EU), https://gdpr-text.com/en/read/article-7/ (last visited May 25, 2025).
[39] Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India).
[40] Ministry of Electronics & Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act*, Rule 4(2), Jan. 2025, available at https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf (last visited June 8, 2025).

Managers—are not governed by enforceable technical standards or if vulnerable groups like children are insufficiently protected by procedural specificity.

C. Statutory Exceptions to Consent: Legitimate Grounds under Section 7 of the DPDP Act, 2023

Section 7 of the Digital Personal Data Protection Act, 2023 (DPDP Act), provides a framework for the lawful processing of personal data without requiring consent from the data principal. Contrary to the language used in earlier drafts and the Srikrishna Committee Report—which introduced the concept of "deemed consent"[41]—the final version of the statute does not employ this terminology. Instead, Section 7 enumerates specific legitimate uses where the obligation to obtain consent is waived, including**:** the performance of state functions, compliance with laws or court orders, public interest objectives, medical emergencies, disaster response, and employment-related purposes[42].

This legislative shift has significant implications. Although the enumeration provides clarity, it omits procedural safeguards that typically accompany non-consensual data processing in mature jurisdictions. For instance, under Article 6(1)(f) of the General Data Protection Regulation (GDPR), data may be processed without consent when it is necessary for the purposes of legitimate interests pursued by the controller—but only after a balancing test is conducted to ensure that such interests do not override the fundamental rights and freedoms of the data subject[43]. This proportionality check, while absent in India's Section 7, is a cornerstone of European data protection jurisprudence.

The GDPR Recitals 47 to 50 further clarify that even where consent is not the basis for processing, transparency, necessity, and proportionality remain fundamental

[41] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, July 2018, available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (last visited June 8, 2025).

[42] Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).

[43] Regulation (EU) 2016/679, art. 6(1)(f), 2016 O.J. (L 119) 1 (EU), https://eur-lex.europa.eu/eli/reg/2016/679/oj (last visited June 8, 2025).

requirements[44]. The Indian DPDP Act, by contrast, does not require data fiduciaries to inform data principals when their data is processed under Section 7. This absence of prior notification contradicts global best practices and weakens informational autonomy. In practice, individuals may remain unaware that their personal data is being used, even when the context involves sensitive operations such as welfare delivery or Aadhaar-based authentication.

The Justice B.N. Srikrishna Committee Report had previously recommended "deemed consent" as a flexible legal fiction—but with strict purpose limitation and audit trails[45]. The removal of that term in the final legislation arguably reflects a legislative attempt to replace a vague standard with enumerated lawful grounds. Yet, without accompanying procedural accountability—such as mandatory Data Protection Impact Assessments (DPIAs) or regulator-reviewed necessity justifications—the Act risks enabling function creep, where data collected for one legitimate use is silently repurposed for another.

This design is particularly vulnerable in high-power asymmetry contexts like state surveillance or welfare schemes. The Supreme Court's ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India mandates that any State action infringing on privacy must meet the tests of legality, necessity, and proportionality[46]. However, Section 7's structure places the onus on individuals to challenge non-transparent processing, despite the constitutional requirement that the State bears the burden of justification.

In sum, while Section 7 outlines legitimate exceptions to consent, the Act lacks statutory mechanisms to ensure transparency, oversight, or redressal. Unlike the GDPR, India's framework does not subject these bases to institutional checks, thereby risking arbitrary or excessive intrusions.

---

[44] Regulation (EU) 2016/679, recitals 47–50, 2016 O.J. (L 119) 1 (EU), https://gdpr-info.eu/recitals/ (last visited June 8, 2025).

[45] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, July 2018, available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (last visited June 8, 2025).

[46] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India), https://indiankanoon.org/doc/91938676/ (last visited June 8, 2025).

VI. CONSENT UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

A. Introduction and Legal Context

The General Data Protection Regulation (GDPR), officially titled Regulation (EU) 2016/679, came into force on May 25, 2018, and marked a major legislative overhaul in the European Union's data privacy regime. It replaced the Data Protection Directive 95/46/EC, introducing a directly applicable regulation that emphasized harmonization, accountability, and user empowerment across all EU member states.[47] One of the most distinctive features of the GDPR is its extraterritorial reach. Under Article 3, the Regulation applies not only to data controllers and processors within the EU but also to those offering goods or services to, or monitoring the behaviour of, EU residents[48]—making it a truly global benchmark.

Among the various lawful bases for processing personal data listed in Article 6(1), consent occupies a uniquely autonomy-driven space. Unlike contractual necessity or legal obligation, which often subordinate the user's choice to functional requirements, consent under Article 6(1)(a) is premised on voluntary, informed, and affirmative user participation in data governance.[49]

The GDPR introduced this heightened emphasis on user agency to address concerns about opaque data practices, manipulative interface design, and coercive digital architectures prevalent under the earlier directive. Consent is thus not only a procedural requirement but also a legal expression of informational self-determination, grounded in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[50]

[47]Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[48]*Id.* art. 3.
[49]*Id.* art. 6(1)(a).
[50]*Charter of Fundamental Rights of the European Union*, arts. 7, 8, 2012 O.J. (C 326) 391.

B. Doctrinal Definition and Legal Preconditions

Article 4(11) of the GDPR defines consent as: "*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.*"[51]

This definition establishes four essential legal conditions:

- **Freely given:** without coercion or imbalance
- **Specific:** purpose-bound
- **Informed:** with adequate notice and understanding
- **Unambiguous:** must involve a clear affirmative act (e.g., ticking a box)

Recital 32 further elaborates that consent should not be inferred from silence, pre-ticked boxes, or inactivity.[52] Consent mechanisms must be opt-in rather than opt-out.

The Article 29 Working Party, and later the European Data Protection Board (EDPB), issued guidelines clarifying that consent is invalid in situations of power imbalance, particularly in employment relationships, where the employee has limited negotiating power.[53] One may argue that this doctrinal clarity reflects GDPR's core normative commitment—to ensure that data subjects are not just participants, but equal stakeholders in the digital economy.

This definition also underpins regulatory interpretation. The EDPB has consistently emphasized that consent obtained through bundling (e.g., requiring consent for unnecessary purposes) or take-it-or-leave-it[54] policies is invalid because it violates the voluntariness requirement[55].

---

[51] *Regulation (EU) 2016/679*, art. 4(11).
[52] *Id.* recital 32.
[53] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, Version 1.1 (May 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited May 25, 2025).
[54] European Data Protection Board, *Guidelines 02/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, at 10 (Oct. 8, 2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.
[55] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, at 7 (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

C. Procedural Safeguards and Operational Conditions

The GDPR places substantive procedural duties on data controllers to ensure consent is not only lawfully obtained at the time of data collection but is also demonstrable and easily revocable throughout the processing lifecycle. Under Article 7(1), the burden of proof lies on the data controller to establish that valid consent was obtained prior to any processing activity. This requirement mandates the maintenance of audit trails, capturing when, how, and under what conditions consent was given.[56]

In addition, Article 7(3) reinforces that withdrawal of consent must be as straightforward as its provision, prohibiting obstructive or convoluted opt-out mechanisms, in other words withdrawal must be "as easy as giving consent."[57] This provision ensures that no undue technical or legal hurdles hinder the data subject's control over their personal information.

In practical terms, this obligation requires the adoption of user-centric interface designs that support:

- **Granular consent:** allowing users to selectively approve specific processing activities,
- **Easy revocation mechanisms:** such as user-friendly dashboards or preference centres, with clear opt-out functionality,
- **Comprehensive logging systems:** that transparently record how, when, and for what purposes consent was obtained.

These principles are reinforced by Recital 32, which unequivocally states that consent cannot be inferred from silence, inactivity, or pre-ticked boxes, and must be obtained through a clear affirmative act.[58] Controllers are also expected to maintain audit trails to document the method, scope, and timing of consent. This is not merely for internal compliance, but also to withstand inspections by Data Protection Authorities (DPAs).

[56] *Regulation (EU) 2016/679*, art. 7(1).
[57] *Id.* art. 7(3).
[58] *Id.* recital 32.

Significantly, the European Data Protection Board (EDPB) issued Guidelines 05/2020 on consent, which clarify the interpretation of Articles 4(11), 6(1)(a), and 7 in light of post-*Schrems II* compliance pressures.[59] The Guidelines emphasize that controllers must avoid "consent fatigue" through layered notices and encourage the use of dynamic, context-aware mechanisms that do not condition access to services on unrelated data processing consents. The EDPB also warns against the bundling of consent with contractual terms, especially in imbalanced power relationships, thereby reinforcing that voluntariness must be genuine and not merely formal. It is further emphasized that consent must be freely given, informed, specific, and unambiguous, and cannot be bundled with unrelated terms or obtained through pre-ticked boxes. The guidelines also clarify that in the wake of the *Schrems II* judgment, controllers must be especially diligent in consent-based international transfers of personal data, ensuring that data subjects are informed of the risks in jurisdictions lacking equivalent safeguards[60].

A landmark case that prominently tested GDPR's procedural safeguards and reflected its enforcement expectations was *Commission Nationale de l'Informatique et des Libertés (CNIL) v. Google LLC*. In January 2019, the French data protection authority (CNIL) imposed a €50 million fine on Google for its Android ad personalization practices, citing failures to provide users with transparent information and valid consent mechanisms. The CNIL found Google's consent mechanisms to be opaque, lacking adequate information, and making it excessively difficult for users to exercise meaningful choice.[61]

Notably, in June 2020, France's highest administrative court, the *Conseil d'État*, agreed that Google's approach to user information and consent fell short of the GDPR's transparency and specificity requirements, and upheld the CNIL's decision, though

[59] European Data Protection Board, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, Version 1.1 (May 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited May 27, 2025).
[60] European Data Protection Board, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, Version 1.1 (May 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited May 27, 2025).
[61] Commission Nationale de l'Informatique et des Libertés (CNIL), *Deliberation SAN-2019-001* (Jan. 21, 2019), https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf (last visited May 25, 2025).

slightly adjusting the rationale by clarifying the scope of CNIL's territorial competence.[62] This appellate affirmation has solidified the precedent that procedural lapses and incomplete or misleading consent interfaces, even by major corporations or tech giants, will attract stringent regulatory scrutiny and severe penalties under Article 83(5) of the GDPR.

Moreover, Article 83 of the GDPR imposes severe penalties for violations, with fines for breaches of basic principles (like consent under Articles 6 or 7) reaching up to €20 million or 4% of global annual turnover, whichever is higher.[63] This significant deterrent aims to prevent superficial or exploitative consent practices. Consequently, through these stringent provisions and related developments, the GDPR elevates consent beyond a mere checkbox, establishing it as a multidimensional legal instrument that demands voluntary, verifiable, easily withdrawable, and contextually respected agreement, thereby empowering data subjects and institutionalizing accountability.

D. Consent and Risk-Based Oversight: DPIAs and Enforcement Guidance

The GDPR adopts a risk-based approach to data protection, evaluating the appropriateness of consent in light of the specific context, power asymmetries, and technological complexity. While the GDPR recognizes consent as a legitimate basis for personal data processing under Article 6(1)(a)[64], it does not elevate it as the default or superior legal ground. This framework becomes especially critical in cases involving large-scale, sensitive, or high-risk processing—such as biometric surveillance, behavioural profiling, or automated decision-making. In such scenarios, controllers are obligated to conduct Data Protection Impact Assessments (DPIAs) under Article 35, [65] which require a pre-processing evaluation of the nature, scope, and potential risks to data subjects' rights.

---

[62] *Google LLC v. CNIL*, No. 430810 (Conseil d'État June 19, 2020), https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/430810.
[63] *Regulation (EU) 2016/679*, art. 83(5).
[64] *Regulation (EU) 2016/679*, art. 6(1)(a).
[65] *Regulation (EU) 2016/679*, art. 35.

A DPIA must:

- Identify the purpose and means of processing,
- Evaluate necessity and proportionality,
- Assess risks to data subjects' freedoms, and
- Propose measures to mitigate identified harms.

Notably, DPIAs are not confined to consent-based processing alone. However, where consent is relied upon—particularly in high-risk or sensitive contexts—the DPIA serves as a safeguard to ensure that consent mechanisms are not only valid but also sufficiently informed, voluntary, and proportionate to the processing risk.

The EDPB Guidelines 05/2020, issued after the *Schrems II* judgment, further caution controllers against over-reliance on consent in structurally imbalanced contexts—such as employment relationships or essential service platforms—where users may lack meaningful alternatives.[66] These guidelines reiterate that consent should not be used as a "legal workaround" where a more appropriate basis, like contract or legal obligation, exists.

Importantly, the EDPB clarifies that "freely given" consent cannot be presumed where access to a service is conditioned upon consent to process data that is not necessary for that service. Such conditioning violates the core of Article 4(11) [67] and Recital 42, which require voluntariness and real choice.

Moreover, supervisory authorities across the EU—such as CNIL in France, the ICO in the UK, and BfDI in Germany—have developed DPIA templates and sector-specific DPIA trigger lists to aid controllers. Some Member States also require prior consultation with regulators if a DPIA reveals residual high risk, as mandated under Article 36.[68]

---

[66] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679,* Version 1.1 (May 4, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited June 8, 2025)..

[67] *Regulation (EU) 2016/679*, art. 4(11).

[68] *Regulation (EU) 2016/679*, art. 36.

This layered enforcement and guidance architecture positions consent not as a standalone safeguard but as part of a broader, dynamic mechanism of regulatory accountability and proportionality-driven compliance.

VII. CONSENT UNDER THE CCPA AND CPRA

A. Introduction and Legal Background

The California Consumer Privacy Act (CCPA), enacted in 2018 and enforced from January 1, 2020, was a landmark attempt by a U.S. state to legislate comprehensive data protection rights for individuals. The act emerged in the absence of a federal data privacy law, underscoring California's role as a legislative frontrunner in digital rights governance.[69] Its provisions reflect an increasing public demand for transparency and control over how businesses collect and use personal information.

The California Privacy Rights Act (CPRA), passed through a ballot initiative in November 2020 and effective from January 1, 2023, amended the CCPA to introduce more granular rights and stricter business obligations.[70] The CPRA introduced stricter obligations for businesses and enhanced individual rights, including the right to correct inaccurate information and limit the use of sensitive personal data. Notably, it established the California Privacy Protection Agency (CPPA), a dedicated enforcement body.[71] Following these reforms, the legal regime is now collectively referred to as the "CCPA, as amended."

Unlike the opt-in consent models seen in the GDPR[72] or India's Digital Personal Data Protection Act, 2023 (DPDP Act),[73] the CCPA, as amended, predominantly relies on a notice-and-opt-out structure, particularly for the sale or sharing of personal data.[74] While consent plays a role in specific contexts, the framework places more emphasis on user control after collection, not before it. Consent is only required in specific

[69] Cal. Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–.199 (West 2018), https://oag.ca.gov/privacy/ccpa (last visited May 25, 2025).
[70] Cal. Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq. (West 2020).
[71] Cal. Civ. Code § 1798.199.10(a) (West 2020).
[72] Regulation (EU) 2016/679, art. 4(11), 2016 O.J. (L 119) 1
[73] Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023, § 6(1) (India).
[74] Cal. Civ. Code §§ 1798.120, .135 (West 2018).

circumstances—such as the collection of data from minors under 16 years of age, or the use of sensitive personal data beyond originally disclosed purposes.[75]

By emphasizing post-collection control mechanisms over pre-collection consent, the CCPA, as amended, assumes a relatively high degree of user awareness and digital literacy. Although this approach enhances business flexibility, it may inadvertently place a disproportionate burden on consumers. Nevertheless, it remains the most comprehensive state-level privacy law in the U.S., serving as a model for similar statutes in Colorado, Virginia, Utah, and Connecticut,[76] and continues to influence discussions around a potential federal privacy framework.

B. The Legal Scope and Meaning of Consent

Though not central to the act's general architecture, consent is explicitly defined under the CPRA as: *"Any freely given, specific, informed and unambiguous indication of the consumer's wishes by a statement or by a clear affirmative action."*[77] This definition is strikingly similar to Article 4(11) of the GDPR, suggesting conceptual borrowing. However, in practice, the deployment of consent under the CCPA, as amended, is limited and context-specific.

Key areas where affirmative, opt-in consent is required include:

- Processing of sensitive personal information for purposes other than those initially disclosed;[78]
- Collection or sharing or sale of personal data of minors under the age of 16, which requires opt-in consent (with parental consent for children under 13);[79]

[75] Cal. Civ. Code §§ 1798.121, 1798.120(a) (West 2020).
[76] Sara H. Jodka, *The Privacy Tug-of-War: States Grappling With Divergent Consent Standards*, Reuters (Mar. 27, 2025), https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27/ (last visited June 5, 2025).
[77] Cal. Civ. Code § 1798.140(h) (West 2020).
[78] *Id.* § 1798.121(a).
[79] *Id.* § 1798.120(c); § 1798.130(a)(2)(B).

- Extended retention or use of information for materially different purposes than those disclosed at the time of collection.[80]

In most other situations, businesses are required only to provide a "just-in-time" privacy notice at or before data collection and give users the right to opt out of the sale or sharing of personal information.[81] A defining feature of California's regime is it opt-out default model, especially for data sales and cross-context behavioural advertising. Businesses are statutorily required to provide a "Do Not Sell or Share My Personal Information" link or equivalent mechanism.[82] In this regard, the Global Privacy Control (GPC) has emerged as a significant technical tool for operationalizing user rights.

The GPC mechanism is a browser- or device-level setting that signals a user's intent to opt out of the sale or sharing of their personal information across all sites that recognize the signal.[83] The CPRA explicitly acknowledges the validity of such signals under Cal. Civ. Code § 1798.135(b)(1), requiring businesses to treat a user-enabled GPC as a valid opt-out request.[84] Furthermore, CPPA Regulation § 7025(c) mandates that such opt-out preference signals must be honoured in a frictionless and binding manner.[85]

By automating opt-out choices, the GPC minimizes cognitive burden on users and counters the fatigue associated with repetitive privacy disclosures. This aligns with the broader CPRA objective of enhancing user control post-collection, even in the absence of explicit prior consent.

Still, the default orientation of the California regime remains consumer-centric, placing responsibility on individuals to recognize data practices and exercise their rights. While the GPC reduces interface friction, it does not eliminate structural

[80] *Id.* § 1798.121(a), (c), (d).
[81] *Id.* § 1798.100(b).
[82] *Id.* § 1798.135(a)(1).
[83] Global Privacy Control, *Technical Specification*,https://globalprivacycontrol.org/ (last visited May 25, 2025).
[84] Cal. Civ. Code § 1798.135(b)(1) (West 2020).
[85] Cal. Priv. Prot. Agency, *Final Regulations Under the CPRA* § 7025(c) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited June 8, 2025)

asymmetries—particularly for digitally marginalized groups who may be unaware of such tools or lack the technical knowledge to enable them.

However, despite advancements in data privacy, critics argue that the CCPA, as amended, adopts a reactive rather than a proactive model, unlike the GDPR's approach. While it uses the language of consent, its default posture often leads to passive acquiescence, placing the burden on users to discover, interpret, and exercise opt-out choices. This task is frequently hindered by factors like low digital literacy, user fatigue, and deceptive interface designs known as "dark patterns," which can be particularly disempowering for consumers.

C. Enforcement Architecture and Practical Limitations

The California Privacy Rights Act (CPRA) created the California Privacy Protection Agency (CPPA)—a dedicated regulatory body empowered to enforce the CCPA, as amended.[86] The CPPA holds authority to promulgate rules, investigate violations, and impose administrative fines.[87] This significantly enhances the enforcement architecture, which previously relied solely on the California Attorney General, whose bandwidth was limited by broader responsibilities.

Businesses subject to the CCPA, as amended, must comply with a host of operational requirements, including:

- Presenting "just-in-time" notices at the point of data collection;[88]
- Offering accessible opt-out mechanisms, including toll-free numbers, web portals, and mobile app settings;[89]
- Establishing contractual safeguards with service providers, contractors, and third parties.[90]

[86] Cal. Civ. Code § 1798.199.10(a) (West 2020); see also California Privacy Protection Agency (CPPA), About Us, https://cppa.ca.gov/ (last visited May 27, 2025).
[87] Cal. Civ. Code §§ 1798.199.15–.199.40 (West 2020).
[88] *Id*. § 1798.100(a)(1).
[89] *Id*. § 1798.130(a)(1).
[90] *Id*. §§ 1798.140(v)(1), (w)(2).

In high-risk contexts—particularly involving children's data or sensitive personal information—businesses are required to obtain and retain affirmative, verifiable consent, although the law does not mandate a Data Protection Impact Assessment (DPIA) equivalent pre-processing review.[91] This absence of forward-looking risk assessment protocols could expose users to harm, especially in complex data ecosystems like behavioural advertising or automated decision-making.

The Global Privacy Control (GPC) is an important enforcement touchpoint.[92] The CPPA has recognized that regulated businesses must honour user-enabled opt-out signals sent via GPC-compliant browsers.[93] This enforces compliance even without users needing to navigate confusing interfaces.

However, concerns remain about the CPPA's institutional capacity. As a newly formed agency regulating some of the world's largest technology firms, the CPPA faces resource constraints and operational scaling challenges. While its rulemaking has advanced privacy protections—particularly by banning deceptive dark patterns under § 7004 of the CPRA Regulations—practical oversight may lag in the face of sophisticated evasive design strategies.[94]

D. Normative Framework and Policy Critique

From a regulatory theory perspective, the CCPA, as amended adopts a consumer-centric, rather than rights-centric, model of data governance. Although it borrows definitional language from the GDPR—such as requiring that consent be "freely given, specific, informed, and unambiguous"—the statutory scheme does not require affirmative consent for general data processing.[95] Instead, user autonomy is

[91] *Id.* §§ 1798.120(c), 1798.121(a).
[92] Global Privacy Control, *Technical Specification*,https://globalprivacycontrol.org/ (last visited May 25, 2025).
[93] Cal. Priv. Prot. Agency, *Final Regulations Under the CPRA* § 7025(b)(1) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited June 8, 2025).
[94] Cal. Priv. Prot. Agency, *Final Regulations Under the CPRA* § 7004(a) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited June 8, 2025).
[95] Cal. Civ. Code § 1798.140(h) (West 2020) (defining consent); see also Regulation (EU) 2016/679, art. 4(11), 2016 O.J. (L 119) 1 (EU).

operationalized primarily through transparency, disclosure notices, and opt-out defaults, particularly with respect to data sales and sharing.[96]

This architecture assumes a digitally literate user capable of navigating complex privacy policies, identifying opt-out signals, and proactively managing preferences—an assumption that may not hold true across all demographics. As a result, the burden to detect, interpret, and exercise privacy rights rests largely on the individual. In communities with lower digital literacy or limited access to user education, this can result in illusory autonomy, undermining the democratic function of consent.

One of the most innovative mechanisms introduced under the CPRA is the ban on "dark patterns"—deceptive user interface designs that subvert meaningful choice.[97] Section 7004 of the CPRA Regulations prohibits practices such as pre-selected checkboxes, overly complex navigation paths to opt-out, or misleading button placements.[98] While this represents a substantial advance in design-based privacy enforcement, scholars have noted that these interventions do not fully neutralize manipulative default architectures.

As Julie E. Cohen argues, contemporary data ecosystems often obfuscate structural asymmetries under the guise of user consent.[99] Even where dark patterns are formally banned, interface design can still exploit cognitive biases, creating a manufactured perception of choice without substantively altering underlying power dynamics between users and data controllers.

It must be acknowledged, however, that the CCPA, as amended, has pioneered U.S. privacy reform. Its influence is already evident in newer laws in Colorado, Connecticut, Utah, and Virginia, many of which replicate core features of the CCPA–

[96] Cal. Civ. Code § 1798.120(a) (West 2020); Cal. Priv. Prot. Agency, Final Regulations Under the CPRA § 7025 (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited May 27, 2025).
[97] Id. § 7004.
[98] Cal. Priv. Prot. Agency, *Final Regulations Under the CPRA* § 7004(b)–(d) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited June 8, 2025).
[99] Julie E. Cohen, *Turning Privacy Inside Out*, 20 Theoretical Inquiries L. 1, 14–15 (2019), https://scholarship.law.georgetown.edu/facpub/2539/.

CPRA model.[100] While these frameworks remain distinct from the GDPR in terms of scope and enforceability, they demonstrate modular potential to evolve into a federal U.S. privacy law that could harmonize consumer choice with rights-driven accountability.

VIII. COMPARATIVE ASSESSMENT AND POLICY RECOMMENDATIONS

A. Philosophical Divergence in Consent Architecture

The architecture of consent under data protection regimes reflects not only regulatory intent but also underlying conceptions of autonomy, rights, and accountability. While the terminology of "consent" appears harmonized across legal systems, its legal enforceability, normative basis, and procedural structure vary significantly. This becomes particularly evident in a comparative analysis of the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act and Privacy Rights Act (CCPA/CPRA), and India's Digital Personal Data Protection Act, 2023 (DPDP Act).

Under the GDPR, consent is not merely a procedural formality but a manifestation of dignity and informational self-determination, grounded in Article 8 of the Charter of Fundamental Rights of the European Union[101]. Article 4(11) and Article 7 of the GDPR require that consent be freely given, specific, informed, unambiguous, and revocable[102]. In addition, consent must be supported by institutional accountability mechanisms, such as Data Protection Impact Assessments (DPIAs) and oversight by independent Data Protection Authorities (DPAs)[103].

In contrast, the CCPA, as amended, does not centre its privacy regime around consent. Instead, it relies heavily on transparency and opt-out mechanisms, emphasizing a consumer-choice paradigm. The CPRA introduces concepts like sensitive personal

[100] Sara H. Jodka, *The Privacy Tug-of-War: States Grappling With Divergent Consent Standards*, Reuters (Mar. 27, 2025), https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27/ (last visited June 5, 2025).
[101] Charter of Fundamental Rights of the European Union, arts. 7-8, 2012 O.J. (C 326) 391.
[102] Regulation (EU) 2016/679, General Data Protection Regulation, art. 4(11).
[103] *Id.* art. 7.

information, limits on secondary use, and a prohibition on dark patterns, but consent is explicitly required only in narrowly defined cases, such as data sales involving minors[104]. Its architecture assumes that agency resides with the consumer, who must act to protect their rights[105].

The Indian DPDP Act, on the other hand, adopts a hybrid framework. It recognizes consent as the primary basis for lawful data processing but introduces "legitimate use without consent" under Section 7, allowing processing without explicit user approval for public interest, employment, medical emergencies, or state functions[106]. While modelled structurally on the GDPR, the DPDP Act lacks the procedural depth to make its consent framework meaningfully enforceable.

Furthermore, unlike the GDPR—which restricts international transfers to countries with "adequate" legal protections—India's law currently does not meet EU adequacy standards, raising concerns about the future of cross-border data interoperability[107].

B. Operational Mechanisms and Accountability

The effectiveness of consent regimes depends not only on their textual articulation but also on the institutional ecosystems that support them. This includes enforcement authorities, procedural obligations like DPIAs, and clear redressal mechanisms.

The GDPR obliges data controllers to conduct DPIAs for high-risk processing under Article 35. This obligation ensures a risk-aware, rights-preserving framework for data governance. Supervisory bodies like France's CNIL have used this mandate to enforce transparency in practice. Notably, in *CNIL v. Google* (2019), the regulator imposed a €50 million fine for failing to provide users with adequate information and valid consent[108].

The CCPA, as amended, has similar rule-making powers and enforcement capacity. It has published guidance to ensure that consent is not manipulated through dark

[104] Cal. Civ. Code § 1798.120 (West 2020).
[105] *Id.* § 1798.121.
[106]Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).
[107] Regulation (EU) 2016/679, General Data Protection Regulation, art. 45.
[108] CNIL, *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 concerning GOOGLE LLC*,https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf (last visited May 26, 2025).

patterns, reinforcing the need for fair UI/UX design[109]. However, despite these mechanisms, empirical studies have shown that consent fatigue—where users click through disclosures—remains a major obstacle to true user control[110].

India's DPDP Act establishes a Data Protection Board, but its operational and financial independence is yet to be guaranteed. The law lacks an equivalent of DPIAs, nor does it provide for prior consultation with the regulator before undertaking high-risk data processing[111]. This absence creates a compliance vacuum, where consent becomes a checkbox formality rather than a substantive protection.

In the landmark decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court held privacy to be a fundamental right under Article 21, drawing attention to the fiduciary obligations of the State and private actors in handling personal data[112]. However, the DPDP Act does not fully translate this jurisprudence into statutory obligations for "data fiduciaries."

To operationalize consent meaningfully, India's regime must:

- Enforce design standards to prevent dark patterns;
- Introduce mandatory DPIAs;
- Ensure the functional independence of the Data Protection Board; and
- Require privacy notices and dashboards that reflect linguistic and accessibility diversity[113].

These measures are essential if consent is to function as more than symbolic compliance in a data-saturated society. The need for dynamic consent—a flexible, real-time mechanism for managing user preferences—is particularly urgent in sectors like

[109] California Privacy Protection Agency (CPPA), *About Us*, https://cppa.ca.gov/ (last visited May 26, 2025).
[110] Sara H. Jodka, *The Privacy Tug-of-War: States Grappling With Divergent Consent Standards*, Reuters (Mar. 27, 2025), https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27/ (last visited June 5, 2025).
[111] Digital Personal Data Protection Act, No. 22 of 2023, §§ 27–30 (India).
[112] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[113] Digital Personal Data Protection Act, No. 22 of 2023, § 6(3) (India).

health, AI-based services, and personalized finance[114]. Finally, unless India institutionalizes these structural reforms, it may struggle to achieve adequacy status under GDPR, limiting its ability to engage in lawful international data transfers and undermining digital trust in its global platforms[115].

In addition to general compliance mechanisms, sector-specific regulatory frameworks in India further reinforce and operationalize the consent architecture envisioned under the DPDP Act, particularly in finance and capital markets. These regimes mandate granular safeguards that complement the DPDP Act's broad protections, creating a multi-layered compliance structure.

The Reserve Bank of India (RBI), through its *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023*, issued under Section 35A of the Banking Regulation Act, requires regulated financial entities to align their data governance and IT systems with privacy-centric principles. Clause 4.1.4 of the Master Direction mandates that financial institutions adopt adequate mechanisms for data classification, retention, consent, and purpose limitation—principles also central to the DPDP Act[116]. In particular, the framework highlights the need to obtain and maintain records of informed consent when processing sensitive personal financial data, thereby embedding accountability into sectoral operations.

Similarly, the Securities and Exchange Board of India (SEBI) has issued updated guidance for market intermediaries through its *Cybersecurity and Cyber Resilience Framework for SEBI-Regulated Entities*, August 2024. This circular obligates stockbrokers, depositories, and mutual fund houses to implement real-time consent-based access controls and privacy-aware data handling procedures. Clause 6 of the SEBI Framework requires regulated entities to implement "*data lifecycle management*" protocols, which include consent verification and audit mechanisms for any personal

[114] Regulation (EU) 2016/679, General Data Protection Regulation, art. 35, https://gdpr-info.eu/art-35-gdpr/ (last visited May 26, 2025).
[115] *Id.* art. 45.
[116] Reserve Bank of India, *Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices* (Nov. 7, 2023), https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited June 8, 2025).

data processed by market participants[117]. These obligations are particularly significant given the DPDP Act's designation of "significant data fiduciaries,"[118] many of whom fall within the ambit of SEBI regulation.

Together, these sectoral instruments provide a concrete foundation for translating the DPDP Act's consent obligations into enforceable, industry-specific standards. They serve not only as compliance blueprints but also as testbeds for operationalizing privacy by design in India's complex digital economy. These provisions operationalize the DPDP Act within financial and capital market sectors, anchoring compliance in real-time transaction environments.

C. Cross-Border Data Transfers: Consent in Transnational Context

The global nature of digital markets necessitates robust cross-border data transfer frameworks that uphold data protection standards irrespective of jurisdiction. Among the three regimes analysed—GDPR, CCPA (as amended), and India's DPDP Act—only the GDPR embeds a structured, consent-compatible framework backed by enforceable adequacy mechanisms and legal safeguards.

Under Chapter V of the GDPR, transfers of personal data outside the EU/EEA are permissible only where:

- The European Commission has issued an adequacy decision under Article 45;
- the transfer is supported by appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) under Articles 46–47; or
- the data subject has explicitly consented, under Article 49(1)(a), having been informed of the potential risks involved in the absence of such protections.[119]

[117] Securities & Exchange Board of India, *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI-Regulated Entities* (Aug. 2024), https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (last visited June 8, 2025).
[118] Digital Personal Data Protection Act, No. 22 of 2023, § 10 (India).
[119] Regulation (EU) 2016/679, arts. 44–50.

This fallback clause on consent has become increasingly important since the Court of Justice of the European Union's landmark ruling in *Schrems II* (2020), which invalidated the EU–U.S. Privacy Shield. The Court emphasized that contractual safeguards must be accompanied by enforceable rights and effective legal remedies in the recipient jurisdiction[120]. Consequently, consent remains not only a last-resort legal basis but also a crucial tool in risk mitigation where institutional safeguards are lacking.

By contrast, the California CCPA, as amended, impose no territorial restrictions on data flows and do not require consent for foreign transfers.[121] Instead, it relies on a notice-and-opt-out structure that applies regardless of the recipient jurisdiction. The absence of a formal adequacy mechanism or Transfer Impact Assessment (TIA) framework under U.S. law exposes American residents to regulatory fragmentation and weaker procedural safeguards for international data transfers than Europeans[122].

In the post-Brexit context, the EU–UK Trade and Cooperation Agreement (TCA), effective since January 2021, plays a crucial role in facilitating cross-border personal data transfers. The European Commission granted the United Kingdom an adequacy decision in June 2021[123], thereby allowing data to flow freely from the EU to the UK without the need for additional safeguards under Articles 45–49 of the GDPR[124]. This decision is subject to periodic review and can be revoked if UK laws diverge from EU data protection standards. Such mutual recognition illustrates how cross-border arrangements can preserve regulatory interoperability even amid sovereignty shifts.

A parallel development has been the adoption of the EU–U.S. Data Privacy Framework (DPF) in July 2023, which replaces the invalidated Privacy Shield following the *Schrems II* judgment. The DPF attempts to restore transatlantic data flow legitimacy by instituting new U.S. oversight mechanisms, including the creation of an

[120] *Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, para. 184 (July 16, 2020).*
[121] *Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA*, COOLEY LLP, https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/ (last visited May 25, 2025).
[122] Cal. Civ. Code § 1798.120(a) (West 2020).
[123] European Commission, United Kingdom – Adequacy Decision under the General Data Protection Regulation (June 28, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited June 8, 2025).
[124] Regulation (EU) 2016/679, arts. 44–50.

independent redress mechanism through a Data Protection Review Court (DPRC), as well as Executive Order 14086 outlining proportionality and necessity limits on surveillance.[125] This framework is vital for digital trade and underscores the increasing reliance on dynamic adequacy mechanisms grounded in both legislative commitments and executive assurances.

India's DPDP Act, by contrast, provides no comparable infrastructure for adequacy-based transfers. Section 16 merely empowers the Central Government to restrict transfers to specific countries without a transparent evaluation of data protection equivalency or procedural safeguards. The absence of a fallback clause akin to GDPR Article 49, or any mandate for Transfer Impact Assessments (TIAs), underscores the risk of fragmented data diplomacy. This omission raises concerns about the data sovereignty and fundamental rights of Indian data principals. It also complicates India's prospects for EU adequacy recognition, a precondition for seamless data flows between Indian entities and EU-based partners.[126] For Indian companies engaging with EU or U.S. entities, this regulatory lacuna can lead to compliance burdens, legal uncertainty, and barriers to global data interoperability.

The Reserve Bank of India (RBI) and SEBI further impose localization or data handling norms in specific sectors, but there is no overarching national framework for transfer governance consistent with GDPR standards. Without procedural obligations—such as explicit consent for high-risk transfers or cross-border accountability disclosures—India's model remains limited in ensuring interoperable, rights-preserving transfers.

Accordingly, India should adopt a tiered adequacy and risk-based transfer framework, aligned with Article 45 of the GDPR. Where adequacy is absent, the law should require explicit consent, coupled with transfer impact disclosures. Such reforms would promote trust and compliance in transnational data partnerships and reflect India's commitment to safeguarding informational privacy beyond its borders.

[125] European Commission, *EU–U.S. Data Privacy Framework – Adequacy Decision* (July 10, 2023), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited June 8, 2025).
[126] Digital Personal Data Protection Act, No. 22 of 2023, § 16 (India).

D. Civil Society, Consent Literacy, and Participatory Regulation

The effectiveness of any consent regime depends not only on legislative design but also on the capacity of civil society to interpret, challenge, and inform its implementation. In this respect, both the GDPR and the U.S. ecosystem offer institutional pathways that India's DPDP Act has yet to replicate.

The GDPR allows non-profit organizations to file representative complaints on behalf of data subjects, even without individual mandates (Article 80).[127] Groups like NOYB (None of Your Business) have initiated strategic complaints that influenced policy at a pan-European level — such as those that led to the GDPR's first multimillion-euro fines. Similarly, Privacy International has used advocacy and litigation to challenge mass surveillance and opaque processing practices.

In the U.S., although federal privacy laws are fragmented, civil society plays an active role. The Electronic Frontier Foundation (EFF) has challenged the misuse of biometric data and facial recognition, while the Centre for Democracy & Technology (CDT) regularly testifies before Congress on deceptive data practices.[128]This participatory approach fills institutional gaps and applies pressure on both regulators and corporations.

India's civil society, though increasingly vocal on digital rights, is limited in regulatory integration. Organizations like the Internet Freedom Foundation (IFF) and SFLC.in have filed public interest litigations and created privacy awareness campaigns[129],

Yet the DPDP Act fails to:

- Recognize representative complaints;
- Establish a mechanism for public consultation on draft regulations;
- Mandate transparency reports from the Data Protection Board.

[127] Regulation (EU) 2016/679, art. 80, https://gdpr-info.eu/art-80-gdpr/ (last visited May 25, 2025).
[128] *Biometrics*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/biometrics (last visited May 25, 2025).
[129] *Digital Rights*, INTERNET FREEDOM FOUND., https://internetfreedom.in/tag/digital-rights/ (last visited May 25, 2025).

One key reform would be to allow third-party advocacy in grievance redressal and enforcement — particularly for marginalized, low-literacy users who may not be in a position to self-advocate.

Equally important is the issue of consent literacy. In a multilingual, socioeconomically diverse country like India, written notices are ineffective if the population cannot comprehend or interact with them. Consent, to be meaningful, must be multimodal and accessible.

Thus, the government must launch a Consent Literacy Initiative, including:

- Privacy education modules in school curricula and public broadcasting;
- Regional-language voice- and image-based disclosures;
- Grants for civil society to develop and audit usable privacy interfaces.

UNESCO and the OECD have emphasized the need for such participatory digital rights frameworks — recognizing that data literacy is foundational to digital citizenship.

E. Reform Proposals Based on the above Analysis: Towards a Balanced Consent Ecosystem in India

1. Institutionalize Data Protection Impact Assessments (DPIAs)

- Mandate DPIAs for high-risk processing, including profiling, AI-based decisions, biometric authentication, and cross-border transfers.
- Adopt a risk-tiered framework, akin to Article 35 of GDPR, with oversight by the Data Protection Board.

2. Refine "Legitimate Uses Without Consent" under Section 7

- Clarify and limit the scope of non-consensual lawful bases under Section 7 by creating an **exhaustive list and ensuring independent review** before application.
- Narrow "legitimate uses without consent" to exhaustively listed **contexts, such as emergencies or state health programs**.

- Replace vague discretionary terms (e.g., "public interest") with concrete criteria and require a **data minimization standard**.

3. Strengthen Institutional Autonomy and Transparency

- Grant the Data Protection Board of India operational independence, budgetary allocation, and binding adjudicatory powers.
- Mandate annual transparency reports, and enforcement decisions to be published with reasoned justification.

4. Operationalize Multilingual and Accessible Consent Infrastructure

- Mandate multilingual user interfaces for all consent mechanisms, with minimum support for 10+ official Indian languages under the Eighth Schedule of the Constitution;
- Introduce consent infrastructure accessibility standards, including voice-based prompts, visual icons, and screen-reader compatibility to support users with limited literacy or visual impairments;
- Empower the Data Protection Board to issue enforceable design regulations under the DPDP Act and monitor digital services for compliance;
- Require that state-facing platforms offer alternative consent collection modes, such as assisted registration and offline form-based consent;
- Compliance certification mechanisms for multilingual consent architecture, audited by the Data Protection Board.
- These proposals comply with the **MeitY Draft Rules (2025),**[130] and enable meaningful exercise of consent rights by all users, including non-digitally literate and non-English speakers, thereby advancing constitutional mandates of equality and inclusion under Article 14.

[130] Ministry of Electronics and Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act,* Jan. 2025, https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf .

5. **Mandate Consent Interface Standards and Anti-Dark Pattern Design**

- Legally enforce UX/UI guidelines that prohibit interface manipulation and deceptive design, as seen under CPRA §7004[131].
- Introduce certification standards for privacy-by-design interfaces.

6. **Align Sectoral Regulations with the DPDP Act**

- Harmonize data protection standards under the DPDP Act with sector-specific frameworks issued by RBI and SEBI.
- Mandate financial entities to align RBI's 2023 IT Governance Directions with obligations under the DPDP Act, particularly on customer data protection and lawful processing[132].
- Require SEBI-regulated market intermediaries to incorporate DPDP-consistent consent and data privacy safeguards within the 2024 Cybersecurity and Cyber Resilience Framework (CSCRF) [133].
- The Data Protection Board should coordinate with RBI and SEBI to issue joint implementation guidance, especially on cross-sector data flows and financial data compliance.

7. **Synchronize Cross-Border Rules with International Frameworks**

- To secure GDPR adequacy and promote interoperability, India must adopt layered transfer mechanisms, including:
- Country-specific white-listing based on adequacy assessments;
- Mandatory Transfer Impact Assessments (TIAs) in absence of such white-listing;

[131]Cal. Priv. Prot. Agency, *Final Regulations Under the CPRA* § 7004(a) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (last visited June 8, 2025).
[132] RBI, *Master Direction on IT Governance, Risk, Controls and Assurance Practices*, 2023, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited May 26, 2025);
[133] SEBI, *Cybersecurity and Cyber Resilience Framework (CSCRF) Circular*, Aug. 8, 2024, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (last visited May 26, 2025).

- Explicit, documented user consent where risks remain.
- Additionally, regulators must closely monitor recent developments such as the EU–UK Trade and Cooperation Agreement and the EU–US Data Privacy Framework to benchmark India's safeguards against accepted global norms[134].

8. Operationalize Consent for Minors and High-Risk Groups

- Implement verifiable consent procedures for children under Section 9 of the DPDP Act, including parental authentication and age-appropriate design standards.
- Ensure harmonization with MeitY's Draft Rules (2025) for Consent Managers to include standards for verifiability, traceability, and revocation[135].

IX. CONCLUSION AND SUGGESTIONS

A. Concluding Reflections

The architecture of consent under data protection regimes is both a procedural necessity and a philosophical commitment. As evidenced through this comparative inquiry into the Digital Personal Data Protection Act, 2023 (DPDP Act), the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act and Privacy Rights Act (CCPA, as amended), it becomes clear that while legislative definitions of consent may converge, their practical effect and normative underpinnings diverge considerably.

The GDPR, regarded globally as a rights-based gold standard, treats consent as a manifestation of dignity and informational self-determination.[136] Its emphasis on

[134] European Commission, *Adequacy Decision on EU–US Data Privacy Framework*, July 10, 2023, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited May 26, 2025); *EU–UK Trade and Cooperation Agreement*, 2021 O.J. (L 444) 14.

[135] Ministry of Electronics and Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act*, Jan. 2025, https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf (last visited May 26, 2025).

[136] Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

explicit, informed, and revocable consent is reinforced through procedural tools like Data Protection Impact Assessments (DPIAs) and supervisory oversight by independent Data Protection Authorities (DPAs).[137] It also provides a framework for cross-border transfers, ensuring that individuals' data rights are preserved even beyond EU borders.[138] This rights-based orientation draws doctrinal support from the European Court of Human Rights' interpretation of Article 8 of the European Convention on Human Rights, particularly in *S. and Marper v. United Kingdom* and *Bărbulescu v. Romania,* which stressed proportionality, necessity, and purpose limitation as core facets of privacy governance[139].

The CCPA, as amended, while progressive within the American context, offers a consumer-choice paradigm wherein consent is mostly implied and opt-out based. Its utility lies in its user-control features—such as the "Do Not Sell" mechanism and Global Privacy Control (GPC) signals[140]—but it lacks the robust procedural scaffolding seen in the EU.[141] Though these signals offer technical empowerment, their enforceability remains limited, especially in cases of dark pattern deployment and user fatigue. One may argue that the U.S. framework assumes a more digitally literate, agency-driven user, which may not hold true across all demographics.

India's DPDP Act, in its present form, occupies a liminal space between the two. It espouses an opt-in model and contains GDPR-like provisions in language, but simultaneously dilutes their impact through open-ended exceptions (such as "*legitimate use without consent* under Section 7") and executive-driven rulemaking.[142] The absence of mandatory DPIAs, procedural enforcement guarantees, or class-action redress mechanisms further weakens its implementation architecture. However, sector-specific regulators like the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have begun integrating data protection duties aligned

[137] *Id.* art. 35.
[138]Eur. Comm'n, *Adequacy Decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited May 25, 2025).
[139] *S. and Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 1169, ¶¶ 103–106 (2008); *Bărbulescu v. Romania,* App. No. 61496/08, 45 Eur. Ct. H.R. 10, ¶¶ 120–122 (2017).
[140] Global Privacy Control, https://globalprivacycontrol.org/ (last visited June 9, 2025).
[141] Cal. Civ. Code §§ 1798.100– 1799.100 (West 2020).
[142]Digital Personal Data Protection Act, No. 22 of 2023, § 7, (India).

with the DPDP Act[143]. These developments signal early institutional momentum toward comprehensive compliance.

What the Indian regime lacks, and what this paper emphasizes, is a systemic recognition that consent must be backed by enforceable fiduciary responsibilities. The concept of a "data fiduciary," borrowed from *Puttaswamy v. Union of India (2017)*,[144] implies duties of care, accountability, and good faith—yet these are under-developed in the DPDP framework. Without such obligations, consent can easily become illusory, especially for individuals with limited digital literacy or bargaining power.

Thus, the evolution of consent should not be isolated to checkbox compliance. Instead, India should move toward a "consent-plus" regime—a hybrid model that preserves individual autonomy while layering it with structural safeguards, technological transparency, and institutional support.

This comparative framework is particularly valuable for legal practitioners, compliance officers, and in-house counsel, who must interpret evolving statutory obligations in light of both sectoral regulations and global adequacy benchmarks. As data protection obligations evolve, practitioners—especially in regulated sectors like finance and healthcare—must anticipate how the DPDP Act's consent mechanisms and related enforcement rules will shape contract drafting, internal policy frameworks, and risk mitigation strategies. The paper thus offers a roadmap not only for academic inquiry but also for anticipatory compliance planning in India's dynamic regulatory landscape.

B. Future Directions and Policy Implications

Going forward, the efficacy of consent mechanisms under the DPDP Act will depend on how regulators translate legislative intent into enforceable obligations across diverse sectors. To that end, these ten priority directions are critical**:**

[143] Reserve Bank of India, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf

[144] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).*

1. Adoption of Dynamic and Contextual Consent Frameworks

Static, one-time consent models are increasingly obsolete in ecosystems shaped by AI, IoT, and real-time analytics. The concept of dynamic consent—used in clinical research and health tech—enables continuous, modular, and revocable permissions.[145] Regulators must facilitate modular, revocable, and purpose-specific consent interfaces. Its application in broader digital contexts could better reflect evolving user preferences and contextual risks. Health, fintech, and ed-tech sectors may lead this transition, where evolving user expectations necessitate adaptive dashboards and granular permissions.

2. Considering Consent as One Layer in a Multi-Tiered Framework

In environments where informed consent is infeasible (e.g., passive surveillance, algorithmic profiling), regulators should introduce purpose-based processing limits, legitimate interest tests, and algorithmic accountability standards. Consent alone cannot act as a gatekeeper in data-rich, opaque systems.

3. Institutionalizing Data Fiduciary Obligations

The fiduciary model of data governance should be operationalized through:

- Mandatory transparency reports
- User-friendly grievance redressal
- Periodic compliance audits

Fiduciaries should be legally obliged to act in the best interests of the data principal, with higher standards of care in sensitive sectors (e.g., finance, health, and education)[146].

[145] *What Is Dynamic Consent?* NHS Health Rsch. Auth., https://www.hra.nhs.uk/about-us/news-updates/what-dynamic-consent/ (last visited May 25, 2025).
[146] *Obligations of a Data Fiduciary Under the Digital Personal Data Protection Act*, LinkedIn, https://www.linkedin.com/pulse/obligations-data-fiduciary-under-digital-personal-protection-act (last visited May 25, 2025).

4. Cross-Border Consent and Adequacy Aspirations

As India seeks alignment with global data flows, its consent regime must meet adequacy thresholds under instruments like GDPR.

This entails:

- Limiting discretionary "Legitimate uses without consent" clauses
- Ensuring cross-border data transfer safeguards
- Creating Transfer Impact Assessments or equivalent tools

Doing so would not only enable interoperability with international partners like the EU and the UK[147] but also elevate domestic trust in digital infrastructure.

5. Creation of a Consent Management Standards Framework

As India transitions to a consent-centric digital economy, standardized operational frameworks for Consent Managers under Section 6(7) of the DPDP Act are vital. The January 2025 Draft Rules issued by MeitY provide preliminary guidance, but further refinement is needed to ensure Consent Managers

- Operate independently from data fiduciaries;
- Offer multilingual, accessible, and UI-tested interfaces;
- Maintain verifiable logs for audit trails;
- Are regulated by clear grievance redressal and accountability standards.

The institutionalization of technical and procedural standards for Consent Managers will not only enhance user autonomy but also enable interoperability across public and private digital platforms. This recommendation is further elaborated in Section VIII.E.7, which outlines procedural safeguards for children's data, including traceable and verifiable consent mechanisms under the MeitY Draft Rules. These systems may serve as India's functional equivalent to mechanisms like the Global Privacy Control

[147] *Cross-Border Data Transfers Under India's Proposed Data Protection Law*, Lexology, https://www.lexology.com/library/detail.aspx?g=d5715e1d-4b25-40b2-a817-38966662c69f (last visited May 25, 2025).

(GPC) under the CCPA or the interface design requirements under GDPR Recital 42 and Article 7, reinforcing user agency in diverse digital environments.[148]

6. Regulatory Design for Legitimate Uses and Transparency

Section 7 of the DPDP Act outlines valid grounds for non-consensual processing. However, purpose limitation, notice obligations, and minimum data use standards should be operationalized via sectoral guidelines. This includes requiring periodic publication of legitimate-use registries and purpose-based audits.

7. Harmonization with Sectoral Frameworks (RBI and SEBI)

Financial and securities regulators must align existing cybersecurity and data governance standards with the DPDP Act. A detailed statutory roadmap for harmonization is outlined in Section VIII.E.5, which recommends joint guidance by the Data Protection Board in coordination with RBI and SEBI on sectoral data protection obligations.

- The RBI Master Direction on IT Governance (2023) mandates data protection and access controls, aligning well with DPDP safeguards[149].
- The SEBI Cybersecurity and Cyber Resilience Framework (2024) requires entities to protect client data and report breaches, forming the basis for coordinated enforcement[150].

8. Alignment with International Transfer Frameworks

India's consent architecture must anticipate cross-border interoperability. Drawing on the EU–UK Trade and Cooperation Agreement and the EU–US Data Privacy Framework, Indian regulators should establish tiered adequacy reviews, encourage standard contractual clauses, and publish Transfer Impact Assessment (TIA)

[148] Ministry of Electronics and Information Technology, *Draft Rules under the Digital Personal Data Protection Act, 2023*, rr. 5–7 (Jan. 2025), https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf

[149] Reserve Bank of India, *Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices, 2023*, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited June 9, 2025).

[150] Securities & Exchange Board of India, *Cybersecurity and Cyber Resilience Framework Circular*, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (last visited June 9, 2025).

templates. This suggestion builds upon Section VIII.E.6, which identifies specific international benchmarks and layered mechanisms such as TIAs and country-specific white-listing essential to ensure GDPR adequacy.

9. Training and Compliance for Legal Practitioners and Institutions along with Legal Practitioners' Capacity and Role Clarity

Successful enforcement of consent norms will depend on legal professionals' capacity to interpret, audit, and advise on compliance. Bar Councils and the proposed Data Protection Board must collaborate with law schools and professional bodies to offer certification modules**,** practical handbooks, and compliance advisory guidelines for in-house teams and external counsels.

For consent reforms to succeed in practice, legal professionals—especially those advising data fiduciaries—must play an anticipatory role. While detailed implications for lawyers and compliance experts are discussed in subsequent Subsection D, it bears noting that sector-specific counsel will need to adapt to evolving requirements in cross-border data flows, fiduciary design obligations, and sectoral compliance (e.g., fintech, health tech, and e-governance). Future regulatory advisories should explicitly define professional duties and documentation standards under the DPDP regime.

10. Civil Society and Participatory Regulation

Finally, public engagement must not be viewed as an afterthought.

A robust consent ecosystem requires:

- Representative actions by civil society groups
- Consent literacy initiatives in schools, colleges and digital literacy programs.
- Consultation mechanisms that allow public feedback on rules, enforcement, and data policy evolution[151]

[151] *Transfer in India – Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/index.html?c=IN&t=transfer (last visited May 25, 2025).

- Awareness campaigns, based on my opinion, to spread the message "*Think Before You Click*" to make everyone thoughtful and cautious before clicking ALLOW anywhere.

C. Summary Table: Future Directions for Strengthening Consent Architecture in India

Policy Area	Recommendation	Objective	Specific Regulatory Action Required	Implementation Timeline
Consent for Minors (Children's Data)	Mandate verified parental consent and age assurance for all processing involving children under 18	Ensure safe digital participation of minors	MeitY to notify DPDP Rules under § 9(1) requiring biometric or OTP-based parental authentication and trusted device verification[152]	Within 9 months of DPDP Rules notification
Consent Manager Regulation	Certify Consent Managers and impose UI/UX and transparency standards	Improve trust and ensure user-friendly, rights-based interfaces	MeitY to finalize and operationalize Consent Manager Rules as per Draft Rules, Ch. III, r.	By Q4 FY 2025–26

[152] Digital Personal Data Protection Act, No. 22 of 2023, § 9(1), Acts of Parliament, 2023 (India).

			7(1)– (3) (Jan. 2025)[153]	
Accessibility & Multilingual Consent Literacy	Enforce delivery of privacy notices in regional languages and formats accessible to persons with disabilities	Promote inclusive digital rights and informed choice	Data Protection Board to issue binding circulars referencing 8th Schedule languages and mandate voice/text alternatives under § 6(3)(b)[154]	Within 6 months of DPDP enforcement
Dynamic Consent Dashboards	Require real-time, purpose-specific, revocable consent interfaces for all fiduciaries	Operationalize user autonomy and fine-grained control	MeitY to certify UX interfaces based on global best practices (e.g., My Data Finland, GDPR-compliant dashboards)[155]	Phase-wise rollout beginning Q1 FY 2026
Cross-Border Transfers	Require Transfer Impact	Align Indian cross-border	Central Govt. to create adequacy	Within 12–18 months of

[153] Ministry of Electronics and Information Technology, *Draft Rules Under the Digital Personal Data Protection Act, 2023* (Jan. 2025), Ch. III, r. 7(1)–(3), available at https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf

[154] Digital Personal Data Protection Act, No. 22 of 2023, § 6(3)(b), Acts of Parliament, 2023 (India).

[155] Regulation (EU) 2016/679, art. 7(3), 2016 O.J. (L 119) 1 (GDPR) (EU).

	Assessments (TIAs) and white-listing of adequate jurisdictions	data flows with global norms	framework modeled on GDPR art. 45 and incorporate benchmarks from EU–UK TCA[156] and EU–US Data Privacy Framework (2023)[157]	DPDP Act enforcement
Mandatory DPIAs for High-Risk Processing	Introduce compulsory DPIAs for profiling, biometric processing, and AI-based decisions	Ensure risk-aware, rights-centric processing compliance	Amend DPDP Rules to mandate DPIAs for all processing under § 10, following Article 35 GDPR model[158]	Within 12 months of Data Protection Board (DPB) becoming operational
Sector-Specific Data Governance	Require RBI- and SEBI-regulated	Harmonize industry-specific privacy	RBI to amend 2023 IT Master Directions[159];	By FY 2025–26 Q3

[156] *Trade and Cooperation Agreement*, EU–UK, Dec. 24, 2020, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22021A0430%2801%29.

[157] European Commission, *EU–U.S. Data Privacy Framework*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited June 9, 2025).

[158] Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119) 1 (EU).

[159] Reserve Bank of India, *Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices*, 2023, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited June 9, 2025).

	entities to align with DPDP consent and accountability norms	regimes with national law	SEBI to revise CSCRF Circular[160] to require DPDP-aligned privacy policies and consent logs	
Consent Audit Trails and Record-Keeping	Enforce timestamped, auditable consent logs for all data fiduciaries	Enhance accountability and auditability for enforcement	DPB to release technical compliance standards for consent storage, withdrawal, and verification logs under § 7(1)– (3)[161]	Within 6 months of DPB becoming operational
Grievance Redressal Training for Professionals	Equip compliance officers, privacy professionals, and advocates with capacity-building on consent law	Strengthen implementation and resolve data subject complaints efficiently	Law Ministry to collaborate with BCI, NLU Consortium, and IBBI for rolling certification programs on	Initiate by Q2 FY 2025–26

[160] Securities & Exchange Board of India, *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI-Regulated Entities*, Circular No. SEBI/HO/ISD/ISD/CIR/P/2024/85 (Aug. 2024), https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html.

[161] Digital Personal Data Protection Act, No. 22 of 2023, § 7(1)– (3), Acts of Parliament, 2023 (India).

			DPDP obligations	
Public Awareness and "Think Before You Click" Campaigns	National outreach on privacy rights, dark patterns, and safe digital habits	Empower citizens to engage meaningfully with consent interfaces	MeitY and PIB to co-launch targeted campaigns via AIR/Door darshan in regional languages, including semi-literate populations	Rolling campaign beginning within 3 months of DPDP Rules coming into force

D. Implications for Legal Practitioners and Compliance Professionals in India

Building on the comparative analysis and reform roadmap presented throughout this paper, several concrete implications emerge for legal practitioners and compliance officers operating within India's evolving data protection ecosystem. The insights offered in this study not only trace the normative evolution of consent across jurisdictions but also distil actionable compliance obligations and regulatory anticipations under the DPDP Act, 2023.

First, the shift from notice-based collection to informed and verifiable consent — emphasized throughout Section VI on the GDPR — requires that practitioners reevaluate consent acquisition mechanisms within client organizations. Law firms advising technology, healthcare, or fintech sectors must now ensure that consent is not bundled, vague, or coercive, and that records of consent (including time, manner,

and scope) are securely auditable. This is particularly important for companies that rely on behavioural analytics, algorithmic decision-making, or cross-border data flows.[162]

Second, as Section VII illustrates, the "opt-out" architecture of the CCPA, as amended, highlights the pitfalls of relying solely on consumer action to invoke privacy rights. Legal professionals in India must therefore educate corporate clients that while transparency remains foundational, the Indian framework — unlike its Californian counterpart — demands affirmative, opt-in consent, with very limited exceptions under Section 7 of the DPDP Act.[163] Even so, these legitimate uses are not loopholes; they impose high fiduciary expectations that practitioners must clearly interpret for clients navigating public interest or state-authorized processing grounds.[164]

Moreover, compliance officers in sectors such as banking and securities — now subject to RBI and SEBI obligations — must ensure that internal governance aligns with the DPDP Act's accountability principles. As outlined in the Section IX.C policy roadmap, regulatory implementation is not just a question of technical controls but institutional design. This includes deploying consent managers compliant with MeitY's Draft Rules (Jan. 2025)[165] and preparing sector-specific audit trails that demonstrate compliance both with the DPDP Act and with regulatory circulars (e.g., RBI's *2023 IT Master Directions*[166] and SEBI's *2024 Cybersecurity Framework*[167]).

A practical illustration underscores this imperative: a Fintech startup handling transaction metadata and onboarding users via mobile apps must ensure that consent

[162] Regulation (EU) 2016/679, art. 6(1)(a), 2016 O.J. (L 119) 1.
[163] Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).
[164] *Id.*
[165] Ministry of Electronics and Information Technology (MeitY), *Draft Rules under the Digital Personal Data Protection Act*, Jan. 2025, https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf (last visited May 26, 2025)
[166] Reserve Bank of India, *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*, 2023, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited May 26, 2025).
[167] Securities and Exchange Board of India, *Cybersecurity and Cyber Resilience Framework (CSCRF) Circular*, Aug. 8, 2024, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (last visited May 26, 2025).

is verifiable (*Section 6*)[168], children's data is handled per Section 9[169], and any third-party processors adhere to contractual safeguards and transfer protocols. Similarly, a telemedicine platform relying on cloud infrastructure must conduct purpose limitation reviews and prepare for possible audit scrutiny under the Data Protection Board's enhanced oversight framework.

Finally, this paper's policy roadmap (Subsection IX.C) provides a layered approach to consent governance — from DPIAs and interface standards to institutional independence and dark-pattern bans. Legal practitioners and compliance professionals should use this roadmap as a baseline to draft client-specific compliance programs, conduct due diligence for cross-border engagements, and anticipate regulatory inquiries with readiness.

In sum, this paper equips practitioners not merely with abstract legal theory, but with a comparative, jurisdiction-bridging framework for adapting to the DPDP Act's consent requirements. In a rapidly digitizing economy, the ability to translate evolving statutory language into enforceable practice will define the next generation of legal compliance leadership in India.

E. Concluding Note

In conclusion, this study offers not only a comparative framework for understanding consent under the Digital Personal Data Protection Act, 2023 (DPDP Act), the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act, as amended by the CPRA (CCPA, as amended), but also an actionable blueprint for legal harmonization, regulatory enforcement, and practitioner preparedness. As India navigates the complex interface between individual rights and digital innovation, the legal and institutional reforms outlined herein serve as both a roadmap and a call to action for lawmakers, compliance professionals, and civil society stakeholders alike.

[168] Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India).
[169] *Id.* § 9.

X. REFERENCES

- *Adequacy Decisions*, Eur. Comm'n, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited May 25, 2025).
- Alan F. Westin, *Privacy and Freedom* 7 (Atheneum 1967).
- *Biometrics*, Elec. Frontier Found., https://www.eff.org/issues/biometrics (last visited May 25, 2025).
- Cal. Civ. Code §§ 1798.100–.199.100 (West, Westlaw through Ch. 1 of 2025 Reg. Sess.), https://oag.ca.gov/privacy/ccpa (last visited May 25, 2025).
- Cal. Consumer Privacy Act, Cal. Civ. Code (West 2018), https://oag.ca.gov/privacy/ccpa (last visited May 25, 2025).
- Cal. Priv. Prot. Agency, *Enforcement Advisory No. 2024-02* (Sept. 2024), https://cppa.ca.gov/pdf/enfadvisory202402.pdf (last visited May 25, 2025).
- Cal. Privacy Rights Act, Cal. Civ. Code (West 2020), https://oag.ca.gov/privacy/ccpa (last visited May 26, 2025).
- California Privacy Protection Agency, *Enforcement Framework Summary* (2023), https://privacy.ca.gov/enforcement/ (last visited May 25, 2025).
- California Privacy Protection Agency, *Final Regulations Under the California Privacy Rights Act* § 7001(l) (2023), https://cppa.ca.gov/regulations/pdf/cpra_regulations.pdf (last visited May 25, 2025).
- Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd. (Schrems II Case)*, ECLI:EU:C:2020:559 (July 16, 2020).
- Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT (last visited May 26, 2025).

- Children's Law Centre, *Lost in Translation: Language Barriers Hinder Vaccine Access*, WebMD Health News (May 2021), https://childrenslawcenter.org/news/webmd-health-news-lost-translation-language-barriers-hinder-vaccine-access/ (last visited May 25, 2025).
- Chris Jay Hoofnagle & Jennifer M. Urban, *New Challenges to Data Protection Study – Country Report: United States* (Berkeley Ctr. for Law & Tech. 2018), https://www.law.berkeley.edu/center-article/new-challenges-to-data-protection-study-country-report-united-states/ (last visited May 25, 2025).
- *Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practices*, Open Soc'y Founds. (Feb. 2020), https://www.opensocietyfoundations.org/publications/civil-society-organizations-and-general-data-protection-regulation-compliance (last visited May 25, 2025).
- Commission Nationale de l'Informatique et des Libertés (CNIL), *Deliberation SAN-2019-001* (Jan. 21, 2019), https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf (last visited May 25, 2025).
- *Cross-Border Data Transfers Under India's Proposed Data Protection Law*, Lexology, https://www.lexology.com/library/detail.aspx?g=d5715e1d-4b25-40b2-a817-38966662c69f (last visited May 25, 2025).
- *Cross-Border Data Transfers Under the DPDP Act*, Leegality, https://www.leegality.com/consent-blog/cross-border-data-transfer (last visited May 25, 2025).
- *Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA*, Cooley LLP, https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/ (last visited May 25, 2025).
- Daniel J. Solove, *Understanding Privacy* 97 (Harv. Univ. Press 2008).

- Digital Personal Data Protection Act, No. 22 of 2023, (India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited May 26, 2025).
- *Digital Rights*, Internet Freedom Found., https://internetfreedom.in/tag/digital-rights/ (last visited May 25, 2025).
- EFF, *EFF's Legal Cases*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases (last visited May 27, 2025); CDT, *Policy Work*, CTR. FOR DEMOCRACY & TECH., https://cdt.org (last visited May 27, 2025).
- European Commission, *EU–U.S. Data Privacy Framework*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited June 9, 2025).
- European Data Protection Board, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, Version 1.1 (May 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited May 25, 2025).
- Global Privacy Control, *Technical Specification*, https://globalprivacycontrol.org/ (last visited May 25, 2025).
- Human Rights Watch, *India: Identification Project Threatens Rights* (Jan. 13, 2018), https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights (last visited May 25, 2025).
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, May 11, 2011.
- Julie E. Cohen, *Turning Privacy Inside Out*, 20 Theoretical Inquiries L. 1 (2019), https://scholarship.law.georgetown.edu/facpub/2539/ (last visited May 25, 2025).

- Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Gov't of India 2018), https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited May 25, 2025).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India), https://indiankanoon.org/doc/91938676/ (last visited May 26, 2025).
- Ministry of Electronics and Information Technology, *Draft Rules Under the Digital Personal Data Protection Act,* 2023 (Jan. 2025), Ch. III, r. 7(1)–(3), available at https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf
- NHS Digital, Consent and Your Health Records, NHS DIGITAL, https://digital.nhs.uk/services/summary-care-records-scr (last visited May 27, 2025)..
- *Obligations of a Data Fiduciary Under the Digital Personal Data Protection Act*, LinkedIn, https://www.linkedin.com/pulse/obligations-data-fiduciary-under-digital-personal-protection-act (last visited May 25, 2025).
- Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html (last visited May 24, 2025).
- Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
- Reserve Bank of India, *Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices,* 2023, https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited June 9, 2025).

- Securities & Exchange Board of India, *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI-Regulated Entities,* Circular No. SEBI/HO/ISD/ISD/CIR/P/2024/85 (Aug. 2024), https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html.
- *The Privacy Tug-of-War: States Grappling With Divergent Consent Standards*, Reuters (Mar. 27, 2025), https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27/ (last visited May 26, 2025).
- Trade and Cooperation Agreement, EU–UK, Dec. 24, 2020, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22021A0430%2801%29 .
- *Transfer in India – Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/index.html?c=IN&t=transfer (last visited May 25, 2025).
- *Volkszählungsurteil* (Census Act Case), BVerfGE 65, 1 (1983) (F.R.G.).
- *What Is Dynamic Consent?*, NHS Health Rsch. Auth., https://www.hra.nhs.uk/about-us/news-updates/what-dynamic-consent/ (last visited May 25, 2025).