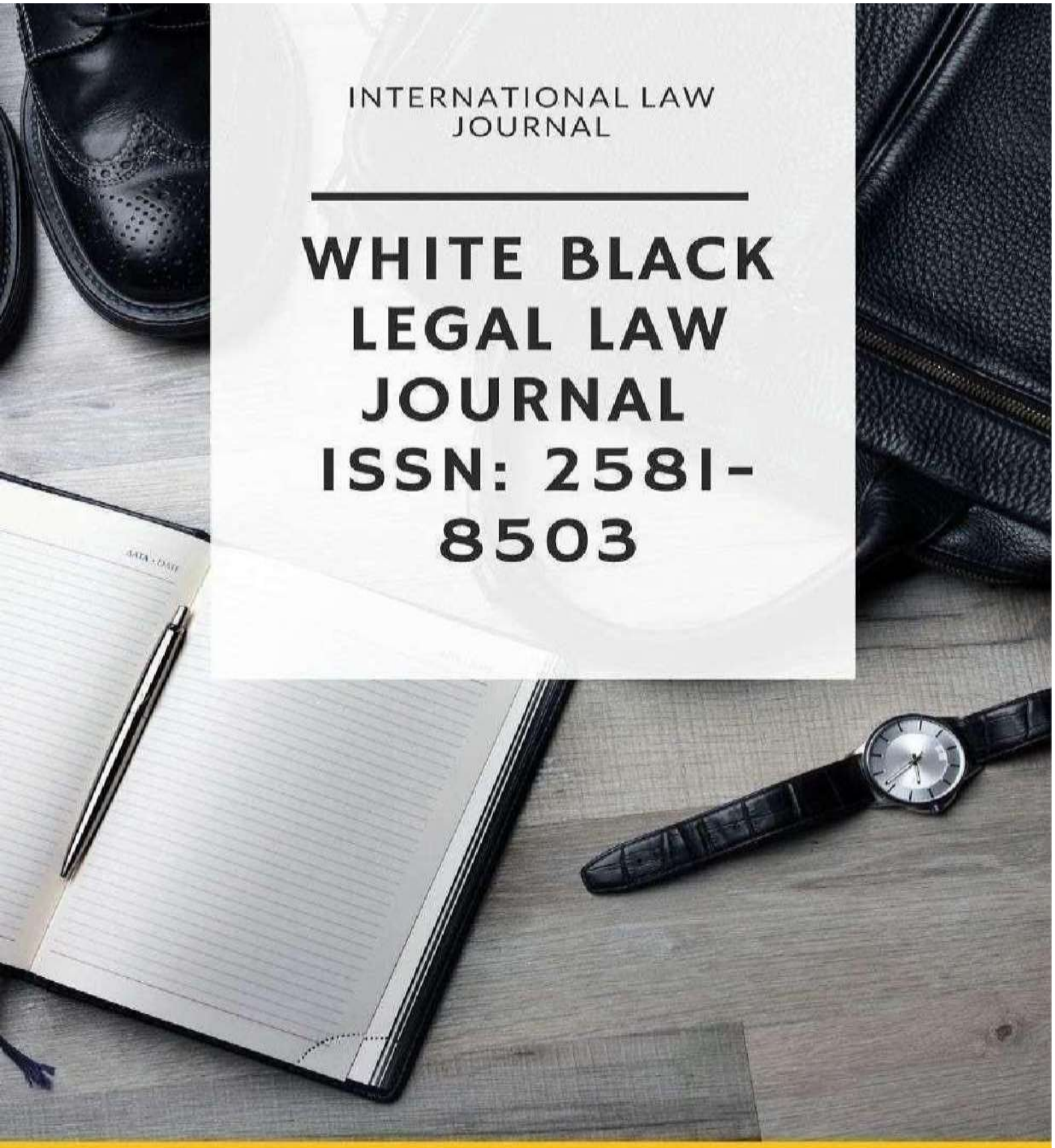

INTERNATIONAL LAW JOURNAL

# WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

## Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

# DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

# ABOUT WHITE BLACK LEGAL

*White Black Legal – The Law Journal* is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

# AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

# CONSENT MANAGERS AND THE PRACTICAL ARCHITECTURE OF CONSENT - OPERATIONALIZING THE CONSENT FRAMEWORK FOR DATA FIDUCIARIES

AUTHORED BY - HITEN LAKHANI

## Introduction: The Consent Management Problem

Consent forms the backbone of the Data Protection Act's framework for personal data processing. The conditions outlined above, regarding valid consent, apply to all personal data processed by Digital Platforms. There are six conditions: consent must be freely given, for a specific purpose (i.e., legitimate), informed, without undue influence or pressure from anyone involved in the decision-making process (including third parties) and expressed in an unequivocal manner. In addition, the Act stipulates that consent can only be granted through a positive action and that a person should receive fair notice about how their personal data will be used before they provide consent. Finally, the Act states that consent can be withdrawn with equal ease as it is provided. When these requirements are extended to the scale at which Digital Platforms process and use Personal Data, creating a compliance issue of significant real-world complexity arises.

To illustrate this point, consider a large digital platform that has fifty million registered users who each have access to dozens of different functions on the site including but not limited to social media functions, targeted advertising, third party application integration, geolocationbased applications, financial transactions, and communication. Additionally, each individual function may require that personal data be collected for a unique reason with a corresponding legal basis for such collection and potentially be shared with multiple third-party data processors. Creating mechanisms to administer and manage user consent for such a complex array of personal data uses creates additional technological challenges beyond those created solely by the volume of personal data being collected and stored.

In response to the problem posed by managing consent at scale, the Act introduces the concept of a 'consent manager' (a type of Registered Intermediary). A consent manager enables Data Principals to grant, modify, view, and revoke consent with respect to the Processing of their Personal Data. Section 6(7) states that Data Principals may utilize a Consent Manager registered with the Board to both grant and revoke consent. This chapter reviews the Consent Manager Framework focusing upon its structural components, regulatory intent and design, compliance

implications for corporations using this mechanism, potential conflicts-of-interest inherent in utilizing this mechanism, and the Technical Requirements and Governance Mechanisms required to make effective use of this mechanism.[1]

## The Legal Architecture of Consent Managers under the DPDP Act

### *Statutory Framework*

Section 6(7) of the Act states that data principals may use a consent manager to give, manage, review, and withdraw their consent to data fiduciaries. Consent managers act as agents for data principals and have to register with the Data Protection Board. The DPDP Rules will establish the registration requirements, operational standards, technical specifications and accountability obligations for consent managers.

Three important features of consent managers emerge from the statutory provisions. First, consent managers act on behalf of data principals i.e., they are agents for individuals, but not for data fiduciaries. Second, consent managers must be registered with and subject to regulation by the Data Protection Board. Third, consent managers must perform a specific range of functions i.e., providing, managing, evaluating and revoking consent.

## The Corporate Compliance Dimension: What Data Fiduciaries Must Do

The establishment of a consent manager structure imposes significant technical and operational obligations on data fiduciaries. In particular, a data fiduciary must be able to work with consent manager systems i.e., accept consent grants, record why consent was granted, recognize when consent is withdrawn and stop processing when consent is withdrawn. Thus, this interoperability obligation requires that data fiduciaries cannot develop their own consent management systems independently; instead, they must be designed to communicate with an outside network of registered consent manager systems.

A second compliance obligation arises for data fiduciaries in terms of verifying whether a consent granted via a consent manager is valid i.e., whether the consent manager is registered, whether the data principal has appointed the consent manager as his/her representative and whether the consent was specifically provided for the purposes for which the data fiduciary

[1] Dr. Srinivas Yanamandra, Towards Accountable Consent: Dissecting India's Consent Management Architecture under DPDP, DELHI SCHOOL OF OPEN LEARNING, https://sol.dau.ac.in/thought-leadership/l2wozwdu8flvxrozkrrbvtq6/towards-accountable-consentdissecting-indias-consent-management-architecture-under-dpdp-by-dr-srinivas-yanamandra-400322

seeks to process the relevant personal data.[2]

## Regulatory Design of the Consent Manager Ecosystem

### Registration and Accountability

Under Section 6(7) of the Act[3], consent managers must be registered with the Data Protection Board. The DPDP Rules will presumably provide detail about what conditions must be satisfied before a consent manager may be registered e.g., financial stability, technological capabilities, good corporate governance practices, independence from data fiduciaries, security requirements and operational guidelines. Registration of consent managers will create a new category of regulated entities.

The accountability of registered consent managers will be critical to the success of the consent architecture established in the Act. Misrepresenting or manipulating a data principal's preferences regarding consent or failing to properly communicate a decision to withdraw consent could result in serious negative consequences for both the data fiduciary who relies on such representations and the broader public interest in protecting privacy. Therefore, the Data Protection Board must possess adequate powers to oversee and regulate registered consent managers, receive complaints and remove registration where necessary.

### The Independence and Conflict of Interest Problem

Perhaps the biggest regulatory hurdle facing the development of a consent manager regime is establishing that consent managers will truly remain independent of the data fiduciaries whose consents they help process. A consent manager that receives compensation from a data fiduciary based on the number or dollar amount of consent transactions processed will have incentives to grant and/or renew consent in ways that benefit the commercial interests of the data fiduciary at issue rather than the privacy interests of the underlying data principal. This represents perhaps the clearest example of the agency problem.

To prevent this type of conflict-of-interest problem in the consent manager framework, the DPDP Rules must clearly define how conflicts of interest can arise. At least four types of actions by the DPDP Rules are required to eliminate potential conflicts of interest: first, prohibitions against payment to a consent manager by a data fiduciary contingent on either the quantity or quality of consent transactions facilitated by that consent manager; secondly, prohibitions

[2] Consent Managers under India's DPDP Act and DPDP Rules, AZB & PARTNERS, https://www.azbpartners.com/bank/consent-managersunder-indias-dpdp-act-and-dpdp-rules/
[3] Digital Personal Data Protection Act, 2023, § 6(7), No. 22, Acts of Parliament, 2023 (India).

against a consent manager having equity interests in a data fiduciary whose consents it manages; thirdly, requirements for a consent manager to disclose all commercial relationships with data fiduciaries; and lastly, requirements that a consent manager publish the criteria used in presenting consent options to data principals.

**Technical Standards and Interoperability**

The consent manager framework will only work as intended when all stakeholders within the ecosystem agree on how to do so. in order to communicate the results of consent decision making reliably (and in real time), in standardized data formats and protocols, the consent managers, data fiduciaries and data processors must be able to communicate with one another. when a data principal withdraws his/her/its consent through a consent manager, this message must get to the data fiduciary's processing system quickly enough that it can actually stop the processing of his/her/it personal data.

Therefore, the DPDP rules should set down technical interoperability standards for consent managers. examples of these could include aspects such as technical standards used by consent managers to receive consent decisions from data fiduciaries, technical standards for the format in which consent decisions are recorded and communicated, technical standards for timestamps and audit trails to ensure that consent withdrawal messages sent by a consent manager were received by the data fiduciary in a timely manner, and maximum response times for consent withdrawal messages sent by a consent manager to data fiduciaries.

India could use some of the technical standards being developed under the EU's MyData initiative, UK's Smart DATA projects and open banking frameworks.

## The Data Principal's Perspective: Empowerment or Displacement?

Another key issue in determining whether the consent manager framework gives control back to the user (the DATA PRINCIPAL) or simply shifts the burden of obtaining consent away from the user onto the consent manager is the degree to which the consent manager framework actually gives control to the user. There is an obvious danger of shifting the burden. If a consent manager is presenting complex choices regarding consent to a DATA PRINCIPAL using interfaces that are hard to understand, or if it defaults to granting consent unless actively overridden, then the framework would likely result in nominal COMPLIANCE with regard to consent management without actual control provided to the user.

Real control implies that consent MANAGERS need to provide clear and understandable ways

for users to express their preference of grant or deny for consent, in addition to providing explanation in plain language about what processing of their personal DATA each expression of preference will enable. Real control further implies that users should be easily able to withdraw their consent (i.e. Just as easily as they can give it). Finally, real control requires that users be given a way to view their entire history of consents (e.g. An audit log).

In terms of digital literacy, in the Indian context: India has millions of first-generation internet users who typically interact with digital service providers using mobile devices in local languages, with limited exposure to the concepts of digital privacy. Therefore, the DPDP rules should mandate that consent MANAGERS provide multi-lingual interfaces and design their platforms for ease of use regardless of digital literacy level.

## Consent Managers and the Corporate Compliance Strategy

From an enterprise PERSPECTIVE, the consent manager framework creates two types of COMPLIANCE-related challenges/opportunities for corporate entities. From the challenge PERSPECTIVE, corporations must implement technology capable of interfacing with registered consent MANAGERS' platforms. Corporations must develop new internal consent management policies based upon consent granted/denied through channels beyond their direct control. And corporations must maintain audit logs for every transaction involving consent via a consent manager platform along with the audit logs maintained for consent gathered directly by the corporation.

As far as COMPLIANCE opportunities go, a successful consent manager ecosystem could substantially decrease the costs and complexities associated with complying with consentrelated regulations for corporations. Instead of having to manage the operational aspects of obtaining and maintaining consent for every single DATA PRINCIPAL, corporations using consent manager technologies can shift significant portions of the day-to-day operational burden related to obtaining and maintaining consent to regulated third party intermediary services. Similar to payment gateway services for financial transactions.

Consent manager technologies may also benefit Significant Data Fiduciaries (those subject to DATA Protection Impact Assessment requirements) by establishing a reliable record of transactions regarding consent that is necessary to perform a legitimate DATA Protection Impact Assessment.

## Conclusion: The Consent Manager as Infrastructure for Accountability

The consent manager framework represents perhaps the Act's most creative contribution to DATA protection governance in terms of creating a new type of structure designed to create ACCOUNTABILITY throughout the DATA processing lifecycle. Through recognition of the inherent impracticality of achieving scalable consent management directly between DATA principals and DATA fiduciaries, the Act establishes regulated intermediaries as a viable method for addressing a problem that other jurisdictions have identified but not formally codified into law.

Ultimately, whether or not the consent manager framework ultimately succeeds depends entirely upon how well the DPDP rules define the technical architecture for the consent manager ecosystem - specifically by defining independent requirements, usability guidelines for interfaces, interoperability standards for technical communication, and adequate oversight mechanisms. Ultimately, how well the DPDP rules address these issues will dictate whether or not the consent manager framework realizes its potential as an ACCOUNTABILITY INFRASTRUCTURE, or if it serves as little more than a hollow COMPLIANCE vehicle.

WHITE BLACK
LEGAL