The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

NEED FOR A 'JOINT DATA FIDUCIARY' FRAMEWORK IN INDIA: LESSONS FROM THE GDPR'S JOINT CONTROLLERS CONCEPT

~Hitesh Bhootra

ABSTRACT:

India's Digital Personal Data Protection Act, 2023 (DPDPA) establishes a framework centred on the distinction between Data Fiduciaries and Data Processors. While this model is suitable for conventional data-processing relationships, it does not adequately reflect the realities of today's interconnected digital economy, where multiple entities frequently participate in determining how and why personal data is processed. Digital lending arrangements, healthcare platforms, online marketplaces, advertising technology, and other collaborative digital ecosystems increasingly involve shared decision-making, creating uncertainty over accountability when privacy obligations are breached.

This paper argues that the absence of an explicit framework governing entities that jointly determine the purposes and means of processing personal data constitutes a significant structural gap in India's data protection regime. Drawing on comparative developments in European data protection law, the paper demonstrates that accountability can be allocated according to the actual influence exercised by participating entities over specific processing activities, rather than relying solely on formal contractual designations. It further contends that a functional approach to shared responsibility would better protect data principals while providing greater legal certainty to businesses operating in collaborative digital environments. The paper proposes the introduction of a "Joint Data Fiduciary" framework through subordinate legislation or regulatory guidance under the DPDPA. It recommends recognising shared decision-making based on substance rather than form, requiring transparent allocation of compliance responsibilities among participating entities, limiting liability to the processing activities over which an entity exercises genuine control, and ensuring that data principals may

effectively enforce their statutory rights without navigating complex contractual arrangements. Such a framework would strengthen accountability, align the DPDPA with India's constitutional commitment to informational privacy, and provide a more practical regulatory foundation for the country's rapidly evolving digital ecosystem.

INTRODUCTION:

When two hospitals share a patient database, when a fintech app runs on the rails of a bank, or when an e-commerce seller lists its products via a common Open Network for Digital Commerce (ONDC)-style platform, a question that sounds simple can turn out to be weirdly hard to pin down: who is actually responsible for the data? Under Indian data protection law, as it is currently written in the Digital Personal Data Protection Act, 2023 ("DPDPA"), the story is kind of linear a Data Fiduciary decides what happens to personal data, and a Data Processor just carries out its instructions. But in real digital ecosystems, things rarely line up like that. More often, several entities end up at the same table, each adding their bit to the call on why and how the data is processed, without any single one of them truly steering the whole show on its own.

This paper suggests that India's data protection regime needs an explicit, actually workable framework for what might be called "Joint Data Fiduciaries" entities that jointly decide the purpose and the means for processing personal data, and who therefore should bear shared responsibility in a clear and allocated way toward the data principal. The paper leans quite a lot on the jurisprudence crafted by the ***Court of Justice of the European Union (CJEU)*** under the ***General Data Protection Regulation (GDPR),*** especially the thread of cases that starts with ***Wirtschaftsakademie Schleswig-Holstein*** and ends up in ***Fashion ID***, to show both the promise, and the complications, of a joint controllership model. After that it looks at why the DPDPA's silence on this issue is not just some minor drafting gap but more like a structural weakness with real consequences for accountability. It finally wraps up with practical recommendations about how such a joint fiduciary framework could be built into India's data protection architecture through subordinate legislation or regulatory guidance.

THE DATA FIDUCIARY IDEA UNDER THE DPDPA, 2023 :

Section 2(i) of the DPDPA kind of sketches a Data Fiduciary as any person who, either by themselves or with other people, ends up deciding the purpose and the means for processing personal data. In a way it has this close cousin like feel to Article 4(7) of the GDPR, where a

"controller" is described as the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data. The resemblance really isn't just a coincidence, because the whole India data protection discussion has been shaped pretty substantially by European ideas since the ***Justice B.N. Srikrishna Committee's 2018 report***, and that report stayed in close dialogue with the GDPR too, while putting forward India's first comprehensive data protection bill.

What is a bit striking though is how differently the two instruments handle the phrase "in conjunction with" or "jointly with" others. The GDPR does not just stop at definition. Article 26 then goes on to build an entire operative provision around joint controllership, it asks joint controllers to determine, via an arrangement between them, their respective responsibilities for compliance with the GDPR's obligations, especially where the exercise of the rights of the data subject is concerned, and also their duties to give information. It further requires that the core of this arrangement be made available to the data subject, and critically it lets the data subject exercise their rights against each controller, irrespective of what the internal terms of that arrangement say, in other words the data subject is not "locked" into the arrangement.

The DPDPA, by contrast, uses the phrase "in conjunction with other persons" only once, right inside the definition clause, and then it's kind of never goes back to that idea again, even when it would seem useful. There isn't a Section that really corresponds to Article 26 GDPR. Chapter II of the Act, where it sets out the general duties of Data Fiduciaries including the consent requirements under Section 6, the notice duties under Section 5, and the security safeguards under Section 8 is drafted all the way through in the singular, like a single identifiable fiduciary is always standing in back of every processing activity. And as commentators have already started to mention in the broader context of India's financial data ecosystem, this leads to something that could be called an invisible risk: several entities can, in practice, collectively map out how a data principal's information is used, while none of them is clearly the fiduciary that the Act seems to envisage, and each one can redirect blame to the other when things go wrong.

THE GDPR'S JOINT CONTROLLERS' IDEA: DOCTRINE AND CASE LAW:

GDPR's joint controllership setup didn't just appear fully formed from Article 26 text, no, it was really shaped a lot, and in a few places sort of "rescued" from the ambiguity, by the CJEU.

Three decisions are especially useful for an Indian reader who is trying to picture how this kind of doctrine might work, in real life.

A. WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN[1]

In this 2018 Grand Chamber ruling, the CJEU had to answer whether an education provider running a "fan page" on Facebook can be treated as a controller for the personal data that Facebook collects from people who land on that page, even though Facebook alone manages the technical infrastructure and the cookies. The Court said the term "controller" should be read broadly, to secure effective protection of data subjects, and it concluded that Wirtschaftsakademie became a joint controller because it chose to set up the page , and it used Facebook's audience-insight tools, so it in practice contributed to defining the purposes and also the means of processing even if it never got actual access to the raw personal data. The decision also made this point, joint controllership doesn't need a perfectly mirrored control setup, it doesn't require equal access to data, and it does not even ask that both entities directly handle the data themselves. It's enough that each party's choices have a real, material effect on why and how the processing goes on.

B. JEHOVAN TODISTAJAT / JEHOVAH'S WITNESSES[2]

This was decided not long after, and honestly the case was about door-to-door religious canvassing where one religious community organised and coordinated the gathering of personal notes about the people its members visited. Even if the actual taking of the notes happened when individual members went to the doors. The CJEU really leaned on the same idea from Wirtschaftsakademie: joint responsibility does not automatically mean that every controller has direct access to the personal data in question. The key point is whether there is participation in figuring out the aims and methods of the processing, and that is looked at, more like substance rather than mere form or wording.

---

[1] Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, ECLI:EU:C:2018:388. (2018)

[2] Case C-25/17, *Tietosuojavaltuutettu v. Jehovan todistajat—Uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551.

C. FASHION ID[3] :

The 2019 Fashion ID judgment refined the doctrine a bit more and, for present purposes, is basically the most helpful precedent, since it also sketches the outer boundary of joint controllership. In short, Fashion ID was an online clothing retailer and it had put a Facebook "Like" button on its website. That button, without any real notice, passed visitors' personal data over to Facebook the moment the webpage loaded. This happened even if the visitor never clicked anything, and even if the visitor did not really have a Facebook account.

The CJEU decided that Fashion ID and Facebook were joint controllers, but only in relation to the collection and the onward transmission of the data meaning the particular processing operation for which Fashion ID had real influence, because it selected to embed the plugin for its own marketing goals and its own reach. The Court also made a point of saying that Fashion ID should not be treated as a controller for whatever Facebook did later with that data once it had already left Fashion ID's website. The reason being, Fashion ID had no control, or not much say, over those later purposes and also the means.

So, put differently, joint controllership under the GDPR is tied to what is happening and at which stage, not some wide, blanket label meant to cover the entire data relationship from start to finish.

When you read them together, these three judgments sort of give the GDPR's joint controller doctrine three key features, and they're directly relevant to any Indian equivalent. So first, you assess control in a functional way, like by looking at who really influences the purpose or means of a particular processing operation, not just who signed a contract that was titled, "controller". Second, the fact that control is unequal, or that one party has unequal access to the data, doesn't stop joint controllership from showing up. Third, joint responsibility is kept within the limits of the specific processing operation that the parties jointly decide on, it doesn't automatically spill over to the upstream or downstream parts of the data's life cycle.

[3] Case C-40/17, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629.

WHY INDIA NEEDS AN ANALOGOUS FRAMEWORK:

India's digital economy already shows these fact patterns, that are functionally the same as Wirtschaftsakademie and Fashion ID, yet there is no real statutory way to assign responsibility when something goes wrong. Not like, not in a clean allocation, you know.

A few recurring scenarios keep coming up. Digital lending apps often run on a shared stack: a regulated non-banking financial company sits somewhere in the middle, a technology platform hosts the app and uses its own scoring analytics for borrowers, and then sometimes a co-lending partner bank joins in. Each actor affects what borrower data gets collected and how it is used for credit decisions, which really echoes that SCC Online note about an "invisible risk" in financial data ecosystems, where the DPDPA does not expressly acknowledge joint fiduciaries. In other words, you end up with different parties steering different parts of the system, but the law does not clearly say who is answerable, when and for what.

Healthcare aggregator platforms look similar. They connect a diagnostic laboratory, a hospital, and a booking platform, and together they decide how a patient's health data among the most sensitive categories of personal data is processed. And advertising technology on Indian platforms, in the same way the Facebook "Like" button did in Fashion ID, commonly places third-party trackers and plug-ins on Indian websites and apps. So, an Indian publisher and a foreign ad-tech company effectively co-decide what visitor data is collected and transmitted, even if the publisher's engineers never personally view a single row of that data.

In each of these situations, the DPDPA's current architecture kind of forces an artificial choice, like either treat every participant as an independent Data Fiduciary, bearing the Act's full obligations on its own, which is frankly unrealistic where one party genuinely has no ability to give notice get consent, or honour a data principal's erasure request because it just does not control that layer of the stack. Or, you could allow parties to privately negotiate responsibility away through contract, leaving the data principal to untangle a commercial arrangement they were never actually part of, and maybe even never saw, in the first place. Neither of those outcomes matches what the statute says in its Preamble, which is to protect the interests of data principals while also enabling lawful processing, but in a workable way. The constitutional backdrop makes this sort of gap even harder to justify.

In ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[4] a nine-judge Bench of the Supreme Court of India held that the right to privacy, including informational privacy, is a fundamental right, protected under Article 21 of the Constitution, and that any interference with it has to pass the tests of legality, necessity, and proportionality. A statutory design that spreads accountability thinly across multiple data handlers, so that no single entity can be relied on to answer for a breach of a data principal's informational autonomy, sits a bit awkwardly with the proportionality and accountability rationale that drove Puttaswamy. Then in the Supreme Court's later data-related jurisprudence, including its engagement with Aadhaar in ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[5] the Court similarly stressed that safeguards have to be real and enforceable, not just something on paper, almost notional. And a fragmented, unclear joint-fiduciary landscape tends to struggle with that requirement, at least, in practice.

COMPARATIVE ANALYSIS: WHAT THE DPDPA CAN BORROW, AND WHAT IT SHOULD NOT:

A joint fiduciary framework for India should not be a wholesale transplant of Article 26 GDPR; it should be adapted to the DPDPA's own consent-driven, notice-based architecture. Three lessons stand out.

First, India should codify the functional test used in Wirtschaftsakademie and Jehovah's Witnesses rather than a formal, contract-based test. If two or more persons in substance decide the purpose or means of a processing activity, they should be treated as joint fiduciaries regardless of how their commercial agreement labels them, and regardless of whether each has direct access to the personal data. A test built around labels alone would allow sophisticated players to contract their way out of the DPDPA simply by designating a smaller partner as the sole "fiduciary" on paper.

Second, India should adopt Fashion ID's insight that joint responsibility must be scoped to the specific processing operation the parties jointly control, rather than imposing blanket, undifferentiated liability across an entire data value chain. This protects smaller participants — a local publisher embedding a plug-in, a small NBFC partnering with a larger technology platform from being saddled with obligations over processing stages they have no practical

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

[5] Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1

ability to influence; while still holding them accountable for the specific stage they do control, such as the initial collection or transmission of data.

Third, and most importantly, India should adopt something like Article 26's transparency mandate. Whatever internal arrangement joint fiduciaries reach about who handles consent notices, who responds to a Data Principal's rights under Sections 11 to 14 of the DPDPA (such as the right to access information, correction, erasure, and grievance redressal), and who bears liability for penalties under Section 33, the essence of that arrangement should be disclosed to the Data Principal, and the Data Principal should be entitled to exercise their rights against any one of the joint fiduciaries without having to first work out the internal allocation of responsibility. This is precisely where a bare replication of ordinary contract law would fail data principals: contractual indemnities between fiduciaries are a private matter between those parties, but a data principal seeking to correct an error or withdraw consent should not be made to first identify which of several corporate entities is contractually responsible before their rights can be honoured.

THE CONSENT MANAGER QUESTION:

A further complication is peculiar to India's own architecture and has no direct GDPR analogue: the Consent Manager introduced under Section 6(7) and (8) of the DPDPA, an intermediary registered with the Data Protection Board through whom a Data Principal may give, manage, review, or withdraw consent. Where several fiduciaries jointly determine the purpose and mean of processing but route consent through a common Consent Manager, questions immediately arise about whether the Consent Manager's registration and technical interface can substitute for each joint fiduciary's independent notice obligation under Section 5, or whether it merely aggregates consent while each fiduciary remains separately responsible for the underlying lawfulness of its own processing. A joint fiduciary framework should clarify that the Consent Manager mechanism is a facilitative layer for capturing and recording consent, and does not by itself resolve the deeper question of how obligations and liability are apportioned among the fiduciaries on whose behalf that consent is captured. Without this clarification, joint fiduciaries may be tempted to treat the presence of a Consent Manager as a complete answer to their compliance obligations, when in substance it addresses only one narrow procedural aspect of the relationship.

RECOMMENDATIONS:

Building on this comparative analysis, four concrete steps could give India a working joint fiduciary framework without requiring a full legislative overhaul.

First, the Ministry of Electronics and Information Technology could use its rule-making power under Section 40 of the DPDPA to notify rules that define "joint Data Fiduciary" relationships, adopting the functional, substance-over-form test discussed above. The Digital Personal Data Protection Rules, 2025, already occupy this space for other operational questions and would be a natural vehicle for this addition.

Second, any such rules should require joint fiduciaries to enter into a written arrangement comparable to Article 26 GDPR allocating responsibility for notice, consent, grievance redressal, and breach reporting, with a mandatory requirement to make a plain-language summary of that arrangement available to data principals, for instance through a combined privacy notice.

Third, the rules should make clear, echoing the Fashion ID limitation, that a joint fiduciary's obligations extend only to the processing operation over which it exercises real influence, so that liability tracks actual control rather than mere participation in a value chain. This is important to avoid over-deterring innovation and partnerships in India's growing fintech, health-tech, and platform economy sectors.

Fourth, and perhaps most important from an enforcement standpoint, the Data Protection Board of India should be empowered whether by rule or by early adjudicatory practice to hold joint fiduciaries jointly and severally liable to the data principal for breaches connected to the jointly-controlled processing activity, while leaving the fiduciaries free to apportion loss between themselves through indemnity or contribution claims inter se. This mirrors how joint controllership operates in practice across the European Economic Area and ensures that data principals are never left navigating corporate structures to vindicate a statutory right.

CONCLUSION:

The lack of a joint fiduciary framework in the DPDPA isn’t only a technical oversight, it is a gap that will be tested sooner rather than later by the same digital ecosystems the Act is meant to regulate co-lending setups, ad tech partnerships, healthcare aggregators, and the many joint ventures that actually shape India’s platform economy. The GDPR’s experience, refined over

three major CJEU judgments, suggests a joint controller structure is workable: it can keep multiple parties functionally answerable, without it turning into either blanket, undifferentiated liability or a sort of sprint to the bottom on contractual disclaimers. India does not need to copy the GDPR line for line, but it does need to stop pretending that every instance of data processing has one, and only one, author. A Joint Data Fiduciary framework functionally defined, proportionately scoped, and transparently disclosed to data principals would bring the DPDPA's text closer to the digital reality it was written to govern, and closer to the constitutional promise of accountable, proportionate data governance that the Supreme Court articulated in Puttaswamy.

BIBLIOGRAPHY:

STATUTES AND RULES

Digital Personal Data Protection Act, 2023 (India).

Digital Personal Data Protection Rules, 2025 (India).

General Data Protection Regulation (Regulation (EU) 2016/679), Articles 4(7) and 26.