*Page 3278 - 3292*


# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

## [ISSN 2581-5369]

**Volume 9 | Issue 3**

**2026**

# The Clash of Sovereign Data Regimes: Extraterritoriality, Conflicting Obligations and the Search for Interoperability Between the GDPR and India's Digital Personal Data Protection Act, 2023

ANANYA S. RAI[*] AND LAKSH GERA[**]

## ABSTRACT

*Two of the world's most consequential data-protection regimes now reach beyond their own frontiers and claim authority over the very same act of processing. The European Union's General Data Protection Regulation binds controllers located anywhere where they offer goods or services to, or monitor the behaviour of, individuals within the Union; India's Digital Personal Data Protection Act, 2023, operationalised through Rules notified in November 2025, asserts a parallel extraterritorial grip over processing connected with the offering of goods or services to Data Principals in India. Where a single enterprise serves both populations, it falls simultaneously under two sovereigns whose commands on lawful basis, cross-border transfer, erasure and State access diverge sharply and at one point contradict outright. This paper argues that the resulting difficulty is not one of imperfect compliance but of architecture: each statute projects itself globally while no treaty, adequacy finding or choice-of-law rule presently sits above the two to coordinate them. Drawing on the divergence between the European adequacy-led model and the Indian negative-list model, the reasoning of the Court of Justice in Schrems II, the prohibition in Article 48 of the Regulation on compelled third-country disclosure, and the proportionality standard of Justice K.S. Puttaswamy v. Union of India, this paper distinguishes genuine conflicts of obligation from differences of degree, and locates the sharpest conflict in the field of State-compelled access. It contends that unilateral extraterritoriality has reached the limit of its usefulness, and that the path forward lies not in louder assertions of jurisdiction but in interoperability instruments: calibrated reform of the Indian State-access exemptions, a bespoke adequacy or transfer framework, and eventual accession to a modernised multilateral instrument such as Convention 108+. The conceptual distance between the two systems, this paper concludes, is smaller than their operative defaults suggest; what is missing is the bridge.*

[*] Author is a student at Institute of Law, Nirma University, Ahmedabad, Gujarat, India.
[**] Author is a student at Institute of Law, Nirma University, Ahmedabad, Gujarat, India.

 [ISSN 2581-5369]

***Keywords:*** *Cross-border data transfer, extraterritoriality, GDPR, Digital Personal Data Protection Act 2023, conflict of laws, data sovereignty, adequacy, interoperability.*

## I. INTRODUCTION: TWO SOVEREIGNS, ONE ACT OF PROCESSING

Data does not respect the borders that law presumes. A photograph uploaded in Munich may rest on a server in Mumbai, be analysed by an engineer in Bengaluru, and be retrieved by a customer in Madrid, all within a single second and a single contractual relationship. The architecture of modern data protection has responded to this borderlessness by following the data outward, extending the reach of domestic law to wherever the processing occurs. The European Union led this movement; India has now joined it. The consequence, however, is not a seamless global order but a collision: where two regimes each follow the data across frontiers, an enterprise can find itself standing on the territory of two sovereigns at once, each issuing instructions the other does not contemplate.

This paper examines that collision in its sharpest contemporary form, namely the relationship between the General Data Protection Regulation (the "GDPR" or "the Regulation") and India's Digital Personal Data Protection Act, 2023 (the "DPDP Act" or "the Act"), as operationalised by the Digital Personal Data Protection Rules, 2025. Both instruments are deliberately extraterritorial.[1] Both purport to govern processing carried out beyond their own soil, and both, when applied to the same enterprise serving European and Indian individuals alike, generate obligations that pull in different directions. The argument advanced here is twofold. First, the difficulty between the two regimes is not a transitional problem of an immature Indian statute catching up with a mature European one; it is a structural feature of unilateral extraterritoriality itself, which, when practised by every major jurisdiction at once and without any coordinating norm, predictably produces divergent and occasionally irreconcilable commands. Second, and by way of corrective, this paper insists on a distinction too often blurred in the literature: between true conflicts of obligation, where compliance with one regime entails breach of the other, and mere differences of architecture or degree, which the existing toolkit of transfer mechanisms is designed precisely to bridge. Identifying which is which is the precondition of any sensible reform.

The argument proceeds in eight parts. Part II maps the two extraterritoriality clauses and shows where, and how far, their fields of application overlap. Part III sets out the principal points of

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India) [hereinafter DPDP Act]; Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

 [ISSN 2581-5369]

divergence in the substantive obligations of the two regimes, distinguishing genuine conflict from difference of degree. Part IV isolates the one field, State-compelled access and disclosure, in which the divergence hardens into a true conflict of laws. Part V draws the lesson of the European experience with transatlantic transfers through Schrems II and its successors. Part VI turns to the Indian constitutional anchor, the proportionality standard of *Puttaswamy*, and asks what it demands of the Act's own exemptions. Part VII surveys the interoperability instruments, namely reform, adequacy and multilateral accession, that might supply the missing bridge. Part VIII concludes.

## II. THE TWO LONG ARMS: MAPPING THE OVERLAP

Article 3 of the GDPR establishes its territorial scope in two registers. It applies, first, to processing in the context of the activities of an establishment in the Union, irrespective of where the processing actually occurs; and second, in its genuinely extraterritorial limb, to controllers and processors not established in the Union where their processing relates either to the offering of goods or services to individuals in the Union or to the monitoring of the behaviour of such individuals within it.[2] An Indian software firm with no European office, no European staff and no European servers is nonetheless fully bound by the Regulation the moment it offers a subscription application to users in France or tracks the browsing of users in Germany. This outward reach was not an invention of 2016; it was prefigured in *Google Spain*, where the Court of Justice applied European data-protection law to a non-European operator by treating the advertising activity of its European establishment as inextricably linked to the processing.[3] The Regulation thus inherited and codified a jurisprudence already committed to following the data.

The DPDP Act mirrors this logic in the opposite direction, though not symmetrically. Section 3 applies the Act both to the processing of digital personal data within the territory of India and, in its extraterritorial limb, to processing outside India where that processing is connected with any activity related to the offering of goods or services to Data Principals within India.[4] A European or American enterprise serving Indian customers is thereby drawn within the Indian statute much as the Indian firm is drawn within the European one. Each legislature has reached across the same ocean, and from opposite shores. The asymmetry, easily missed, is instructive: the Indian provision contains no counterpart to the "monitoring of behaviour" limb of Article

[2] GDPR, *supra* note 1, art. 3(2).

[3] Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317 (May 13, 2014) (applying European data-protection law to a non-EU-established operator through the activities of its EU establishment).

[4] DPDP Act, *supra* note 1, § 3 (applying the Act to processing within India and, extraterritorially, to processing outside India "in connection with any activity related to offering of goods or services to Data Principals within the territory of India").

 [ISSN 2581-5369]

3(2), so that a foreign enterprise which merely tracks the conduct of Indian users, without offering them goods or services, may fall outside the Act while an equivalently placed European user would be protected by the Regulation.[5] The two long arms are of unequal length.

Crucially, the reach of a statute over a processing operation and the rules that statute imposes on the export of data are distinct questions. The European Data Protection Board has confirmed that the transfer rules in Chapter V of the Regulation apply even where the data importer is itself already subject to the GDPR by virtue of Article 3(2).[6] Territorial application and transfer regulation are cumulative, not alternative. It follows that an enterprise may be simultaneously bound by both regimes as a matter of scope, and then bound again, separately, by each regime's rules on moving the data across the frontier. The overlap zone is not exotic; it is the ordinary condition of any globally traded digital service. A cloud provider, a payments processor, a travel platform or an outsourced analytics vendor will routinely hold the personal data of both Europeans and Indians within one undifferentiated system. For such an enterprise the two long arms close around the same processing operation at once. The question is no longer which law applies, for both do, but what happens when they demand different things.

## III. Points of Divergence: Conflict and Difference of Degree

The two regimes diverge at several junctures. Intellectual honesty requires separating the divergences that amount to genuine conflict, where an enterprise cannot obey both at once, from those that are differences of architecture or degree, real and consequential but ultimately bridgeable by careful design. This Part addresses three areas of substantive divergence; the field of true conflict is reserved for Part IV.

### A. Lawful basis: six grounds against two

The GDPR permits processing on any of six lawful bases, among which the "legitimate interests" ground allows a controller to process personal data without consent where its interests are not overridden by the fundamental rights of the data subject.[7] This open-textured balancing test, structured by the Court of Justice into an enquiry into purpose, necessity and balance, is the workhorse of a great deal of routine commercial processing: fraud prevention, network

[5] The Indian provision contains no counterpart to the "monitoring of behaviour" limb of GDPR Article 3(2): the Act's extraterritorial reach is confined to the offering of goods or services. *Compare* GDPR, *supra* note 1, art. 3(2)(b), *with* DPDP Act, *supra* note 1, § 3.

[6] Eur. Data Prot. Bd., Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR, at 4-6 (Feb. 14, 2023) (confirming that Chapter V transfer rules apply even where the importer is itself subject to the GDPR under Article 3(2)).

[7] GDPR, *supra* note 1, art. 6(1).

 [ISSN 2581-5369]

security, and direct marketing within reason.[8] The DPDP Act contains no equivalent. It permits processing only on the basis of consent or a closed and enumerated list of "legitimate uses," and conspicuously omits any open-textured balancing ground of the European kind.[9] Where the Regulation offers six doors, the Act offers two, one of which opens only onto a fixed set of statutorily defined rooms.[10] Both regimes demand that consent, where relied upon, be free, specific, informed and unambiguous,[11] but the Act gives the controller no fallback comparable to legitimate interests when consent is impracticable.

The practical consequence is that processing perfectly lawful in Europe on a legitimate-interests footing may have no lawful basis at all under Indian law unless it can be brought within one of the enumerated uses or fresh consent is obtained, and the reverse asymmetry holds for processing that an Indian fiduciary undertakes as a "legitimate use" which would require a documented balancing exercise in Europe.[12] This is a serious difference of architecture. It is not, however, a true conflict: an enterprise can satisfy both regimes by collecting consent or by confining its processing to grounds valid under each. The cost is operational complexity and the loss of a single global processing logic, not the impossibility of compliance.

**B. Cross-border transfer: adequacy against negative list**

The starkest architectural divergence concerns the direction of the default on outbound transfer. The GDPR restricts transfers of personal data out of the Union: a transfer is permissible only where the destination benefits from an adequacy decision, or where the exporter has put in place appropriate safeguards such as standard contractual clauses or binding corporate rules, or where a narrow derogation applies.[13] Adequacy is a finding by the European Commission that a third country ensures a level of protection essentially equivalent to that guaranteed within the Union.[14] Failing adequacy, the burden sits on the exporter to construct a lawful gateway.[15] India, by contrast, has chosen the inverse architecture. Section 16 of the Act, operationalised by Rule

[8] *Id.* art. 6(1)(f). The three-part test (purpose, necessity and balancing) is drawn from Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiksme"*, ECLI:EU:C:2017:336 (May 4, 2017).

[9] DPDP Act, *supra* note 1, § 4 (permitting processing only on the basis of consent or certain legitimate uses), § 6 (consent), § 7 (legitimate uses).

[10] *Id.* § 7 (enumerating, in a closed list, the "legitimate uses"—voluntary provision of data, State functions and benefits, legal compliance, court orders, medical emergencies, employment, and disaster or public-health response—for which consent is dispensed with).

[11] GDPR, *supra* note 1, art. 7 (conditions for consent).

[12] DPDP Act, *supra* note 1, § 8 (general obligations of the Data Fiduciary, including accuracy, security safeguards, breach notification and erasure on completion of purpose).

[13] GDPR, *supra* note 1, ch. V, arts. 44-49.

[14] *Id.* art. 45 (adequacy decisions).

[15] *Id.* art. 46 (appropriate safeguards, including standard contractual clauses and binding corporate rules); *id.* art. 49 (derogations for specific situations).

 [ISSN 2581-5369]

15 of the 2025 Rules, permits transfer to any country except those the Central Government may specifically restrict by order, a negative-list model under which transfer is free until prohibited.[16] A separate provision preserves any stricter transfer restriction imposed by other Indian law, so that sectoral localisation rules continue to bite.[17] As matters stand, no restricted country has been notified, and the transfer provisions of the Rules are in any event scheduled to commence only some eighteen months after publication, so that outbound transfers from India are for the present effectively unrestricted.[18] An Indian payments enterprise must nonetheless reckon with the Reserve Bank's standing requirement that payment-system data be stored within India, a sectoral localisation rule that predates and survives the Act.[19] The two defaults are mirror images: Europe says "no unless," India says "yes unless."

It is tempting to call these models irreconcilable, but the description is imprecise. Both are, at bottom, conditional-transfer regimes; they differ in where they place the default and the burden, not in kind. The collision they produce is concrete enough: an Indian enterprise may be entirely free under Rule 15 to repatriate European customer data to its Indian servers while the Regulation treats that same flow as unlawful absent a transfer mechanism, because India holds no adequacy decision and its legal environment may not guarantee essential equivalence, so that Indian permission and European prohibition attach to the identical movement of bytes. Yet the European architecture itself supplies the instruments to manage the divergence: standard contractual clauses, supplementary measures, and ultimately adequacy. The transfer models are in tension, not in logical contradiction, and the constructive question is which bridging instrument is apt, a question Part VII takes up.

### C. Erasure and retention: a convergent core

A third divergence, frequently described as a conflict, turns out on inspection to be largely convergent. The GDPR confers a broad right to erasure, the celebrated right to be forgotten, entitling the data subject to require deletion across a range of grounds; but that right is expressly subordinated to a list of exceptions, including retention required for compliance with a legal

[16] DPDP Act, *supra* note 1, § 16; The Digital Personal Data Protection Rules, 2025, r. 15, Gazette of India, pt. II sec. 3(i) (G.S.R. 846(E), Nov. 13, 2025) [hereinafter DPDP Rules].

[17] DPDP Act, *supra* note 1, § 16(2) (preserving any higher protection or stricter transfer restriction imposed under other Indian law).

[18] As of June 2026 the Central Government had notified no restricted country under § 16 or Rule 15; the negative list therefore remained un-populated, and outbound transfers were in practice unrestricted. The cross-border transfer provisions are scheduled to commence approximately eighteen months after publication of the Rules. *See* DPDP Rules, *supra* note 16, r. 1(2)-(4).

[19] Reserve Bank of India, Storage of Payment System Data, Notification No. DPSS.CO.OD.No.2785/06.08.005/2017-2018 (Apr. 6, 2018) (requiring payment-system operators to store payment data only in India).

 [ISSN 2581-5369]

obligation and for the establishment or defence of legal claims.[20] The DPDP Act recognises a narrower, conditional right: erasure must follow on the withdrawal of consent or the fulfilment of purpose, but is defeated where retention is necessary for the specified purpose or for compliance with any law for the time being in force.[21] The two provisions share the same core rule: erasure yields to a genuine legal duty to retain. A European data subject's deletion demand and an Indian tax or anti-money-laundering retention duty do not, therefore, collide head-on; each regime already builds in the priority of the retention obligation. The divergence is at the margins, in the breadth of the public-interest and State-processing exceptions each regime recognises, rather than at the centre. To describe erasure against retention as a genuine conflict of obligation is to overstate; the real conflict lies elsewhere.

**D. Children, profiling and the texture of the two regimes**

A further divergence illustrates how the same regulatory anxiety can produce differently shaped rules. Both regimes treat the personal data of children with special caution, but they do so by different techniques. The European Regulation embeds the protection of children within its general architecture, requiring that information be intelligible to a child and treating children as meriting specific protection in the legitimate-interests balance, while leaving the age of digital consent to be fixed by each Member State within a permitted range. The Indian Act, by contrast, adopts a categorical rule: it requires verifiable parental consent for the processing of the data of any person below the age of eighteen, and prohibits both behavioural tracking and targeted advertising directed at children. The European technique is calibrated and contextual; the Indian technique is bright-line and prohibitory. An enterprise serving both populations cannot simply apply the stricter of the two rules everywhere, because the rules are not arranged on a single axis of strictness: the Indian age threshold is higher and its prohibition on tracking absolute, while the European regime tolerates more but demands a documented, context-sensitive justification. The divergence is once again one of texture rather than of irreconcilable command, but it compounds the operational burden of serving the two markets through one system, and it shows that even where the regimes agree on the value to be protected they disagree on the means.

Three points of divergence, then, none of which amounts to a true conflict of obligation. In each, an enterprise can comply with both regimes at the price of complexity, duplication and the surrender of a single global design. The temptation, common in the practitioner literature,

[20] GDPR, *supra* note 1, art. 17 ("Right to erasure ('right to be forgotten')"); *id.* art. 17(3) (exceptions for freedom of expression, legal obligation, public-interest tasks, public health, archiving and research, and legal claims).
[21] DPDP Act, *supra* note 1, § 12(3) (the Data Fiduciary "shall erase … personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force").

 [ISSN 2581-5369]

to describe every such divergence as a clash of laws should be resisted, for it obscures the one divergence that genuinely deserves the name, and to which the argument now turns.

## IV. THE TRUE CONFLICT: STATE-COMPELLED ACCESS AND DISCLOSURE

The field in which divergence hardens into genuine conflict, where obedience to one regime entails breach of the other, is that of State-compelled access. Here the structure of the problem is not a difference of default but a direct clash of commands. The Regulation provides, in Article 48, that a judgment or administrative decision of a third country requiring a controller or processor to transfer or disclose personal data may be recognised or enforced only if it is grounded in an international agreement, such as a mutual legal assistance treaty, in force between the requesting State and the Union or a Member State.[22] The provision is, in effect, a blocking statute: absent the requisite treaty, European law forbids the controller from complying with the foreign demand. An enterprise subject to both regimes that receives an Indian State demand for disclosure unsupported by any such agreement is then caught precisely: the Act, through its expansive State-access provisions, may compel production, while the Regulation forbids it. Compliance with the one is breach of the other. This is the authentic conflict-of-laws structure, and it is not dissolved by any amount of diligence.

The Indian side of this clash is broad. The Act empowers the Central Government to exempt by notification any instrumentality of the State from the substantive discipline of the statute on grounds including the sovereignty and integrity of India, the security of the State, friendly relations with foreign States and the maintenance of public order.[23] It further provides that, where the State or an instrumentality of the State processes personal data, the obligation to erase and certain related duties do not apply.[24] These exemptions are not, on their face, bounded by a statutory test of necessity or proportionality, nor subjected to independent oversight or a structured route of redress for the affected individual. It is this architecture, far more than any divergence over lawful basis or erasure, that places Indian and European law on a collision course, because it is precisely the kind of unchecked State access that European law has held

[22] GDPR, *supra* note 1, art. 48 (a third-country court or administrative decision requiring transfer or disclosure of personal data is enforceable only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting State and the Union or a Member State). *See* Eur. Data Prot. Bd., Guidelines 02/2024 on Article 48 GDPR (Version 2.1, June 2025).

[23] DPDP Act, *supra* note 1, § 17(2)(a) (empowering the Central Government to exempt by notification any instrumentality of the State in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, the maintenance of public order, or the prevention of incitement to a cognizable offence relating to any of these).

[24] *Id.* § 17(4) (in respect of processing by the State or any instrumentality of the State, disapplying section 8(7) and section 12(3), and, where the processing is for a purpose not involving a decision affecting the Data Principal, section 12(2)).

 [ISSN 2581-5369]

incompatible with the protection the Regulation guarantees. To that European jurisprudence the paper now turns.

It is worth dwelling on why this conflict, unlike the others, cannot be engineered away. In the cases of lawful basis, transfer and erasure, the enterprise retains a course of conduct that satisfies both regimes at once: it can collect consent, deploy contractual clauses, or honour a retention duty that both systems already recognise. The compelled-disclosure scenario admits of no such reconciling conduct. Once a lawful Indian demand for disclosure is made in circumstances unsupported by an international agreement, the enterprise faces a binary choice each branch of which is a breach: to disclose is to violate the European prohibition, and to refuse is to defy the Indian State. No technical measure, no contractual clause and no amount of advance planning can occupy a middle ground, because the conflict is not about the conditions under which data may be processed but about a specific act of disclosure that one sovereign commands and the other forbids. This is the signature of a genuine conflict of laws, and it is why the field of State access, narrow though it is, carries an analytical weight out of all proportion to its breadth. Much of the friction between the two regimes is ultimately a matter of cost and duplication; this part of it is a matter of impossibility, and it is impossibility, not expense, that marks the true frontier between the systems.

## V. The lesson of Schrems II and its successors

The European experience with transatlantic data flows is the most instructive precedent for what awaits the India-European relationship. In *Schrems II*, the Court of Justice of the European Union invalidated the EU-US Privacy Shield, the adequacy framework on which thousands of transatlantic transfers had rested, and did so with immediate effect.[25] The Court's objection was not to the commercial privacy commitments of the framework but to the surrounding legal environment of the destination State, measured against the standard that a third country must ensure protection essentially equivalent to that guaranteed within the Union.[26] United States surveillance law, the Court found, permitted access to transferred data on a footing that lacked the limitations and safeguards proportionality requires,[27] and afforded affected individuals no effective judicial remedy, the Ombudsperson mechanism being an inadequate substitute for a

[25] Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems*, ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020) (declaring Commission Implementing Decision 2016/1250 (the EU-U.S. Privacy Shield) invalid), ¶ 202 (immediate effect) [hereinafter *Schrems II*].

[26] *Id.* ¶¶ 94-96 (essential-equivalence standard), ¶ 105 (factors for the adequacy assessment).

[27] *Id.* ¶¶ 168-185 (disproportionate United States surveillance under Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333).

 [ISSN 2581-5369]

court.[28] An adequacy decision built on commercial undertakings could not survive a State-access regime that European law regarded as disproportionate.

Two features of the judgment matter for the present argument. First, the Court did not strike down the standard contractual clauses; it upheld them, while placing on the exporter the burden of verifying, case by case, whether the law of the destination State undermines the protection they promise, and of suspending the transfer if it does.[29] The clauses thus survive as an instrument, but only as one whose use requires an honest assessment of the destination's law and practice. Second, the judgment was the second of its line: the Court had already invalidated the earlier Safe Harbour arrangement in *Schrems I*, where it first articulated the essential-equivalence approach and affirmed the power of national supervisory authorities to scrutinise transfers notwithstanding a Commission decision.[30] The pattern is one of repeated judicial insistence that commercial arrangements cannot paper over a structural deficiency in State access. The framework's eventual successor, the EU-US Data Privacy Framework, was adopted only after substantial reform of the American surveillance and redress architecture; it has been upheld at first instance, though that judgment assessed adequacy on the facts as they stood in 2023 and is now under appeal, so that the matter cannot be regarded as finally settled.[31] The lesson is not that adequacy is unattainable but that it is exacting, and that what it scrutinises most severely is exactly the feature the Indian Act leaves least constrained.

The parallel to India is direct and uncomfortable. The features that doomed the Privacy Shield, namely broad State access and thin individual redress against it, are mirrored in the DPDP Act's expansive State exemptions. The same analytical method that the Court applied to the United States would, if applied to India, raise serious doubt about any future adequacy finding. That adequacy is achievable in principle is shown by the decisions in favour of Japan, the Republic of Korea and the United Kingdom, each of which required demonstrable safeguards on government access and an independent supervisory authority before the Commission was satisfied.[32] The contrast throws India's position into relief: it is not the negative-list default that

---

[28] *Id.* ¶¶ 191-192 (absence of an effective judicial remedy contrary to Article 47 of the Charter), ¶¶ 193-197 (inadequacy of the Ombudsperson mechanism).

[29] *Id.* (operative pt. 2) (upholding the validity of the standard contractual clauses in Commission Decision 2010/87/EU, subject to the exporter's duty to verify and, where necessary, suspend the transfer).

[30] Case C-362/14, *Schrems v. Data Prot. Comm'r*, ECLI:EU:C:2015:650, ¶¶ 73, 96 (Oct. 6, 2015) (invalidating the Safe Harbour decision and articulating the essential-equivalence approach).

[31] Commission Implementing Decision 2023/1795, of 10 July 2023, 2023 O.J. (L 231) 118 (adequacy under the EU-U.S. Data Privacy Framework). The decision was upheld at first instance in Case T-553/23, *Latombe v. Commission*, ECLI:EU:T:2025:831 (Gen. Ct. Sept. 3, 2025), a judgment of the General Court assessing adequacy on the facts as they stood at the date of adoption of the decision and now under appeal to the Court of Justice.

[32] *See* Commission Implementing Decision 2019/419, 2019 O.J. (L 76) 1 (Japan); Commission Implementing Decision 2022/254, 2022 O.J. (L 44) 1 (Republic of Korea); Commission Implementing Decision 2021/1772, 2021 O.J. (L 360) 1 (United Kingdom).

 [ISSN 2581-5369]

imperils adequacy, but the unbounded character of the State-access exemptions and the absence of independent oversight. Recent practice confirms the concern; a European institution's proposed transfer of personal data to India was directed onto the footing of derogations rather than safeguards, a determination later clarified as procedural but telling nonetheless.

The deeper lesson of the European line of cases is methodological, and it bears directly on how India should read its own situation. The Court of Justice has consistently refused to treat the question of adequacy as one of formal commitments on paper, insisting instead on an assessment of the law and practice of the destination State as they actually operate, including the powers of its intelligence and law-enforcement agencies and the remedies in fact available to the individual. The European Data Protection Board has translated this into an exacting methodology for exporters relying on contractual clauses, requiring them to look past the text of the importer's undertakings to the legal environment that surrounds them. The implication for India is that neither the elegance of the Act's consent architecture nor the existence of the Data Protection Board will, by itself, secure European confidence; what will be examined is whether the State-access exemptions are genuinely constrained and whether an individual whose data is accessed has a real remedy. On that examination, the Act as presently drafted is exposed not because its commercial provisions are weak, for they are not, but because the exemptions sit outside the disciplines that the rest of the statute observes. The European jurisprudence is, in this sense, less a foreign imposition than a mirror, reflecting back to the Indian legislature the very questions its own Constitution, through the proportionality standard, already requires it to answer.

## VI. The constitutional anchor: Puttaswamy and proportionality

If the European jurisprudence supplies the cautionary precedent, Indian constitutional law supplies the standard against which India's own choices must ultimately be measured. In *Justice K.S. Puttaswamy v. Union of India*, a nine-judge bench of the Supreme Court of India recognised informational privacy as a facet of the fundamental right to privacy under the Constitution.[33] The Court held that any State restriction upon that right must satisfy a structured proportionality enquiry: the restriction must rest on a valid law, pursue a legitimate State aim, bear a rational connection to that aim, be necessary in the sense of being the least intrusive means available, and strike a fair balance between the public interest and the right of the individual.[34] The

[33] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) [hereinafter *Puttaswamy*].

[34] *Id.* (Conclusions) (recognising informational privacy as a facet of the right to privacy under Article 21 and articulating the threefold test of legality, legitimate State aim and proportionality). *See also Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (India) (applying the proportionality standard in the Aadhaar context).

proportionality standard is thus not a European import smuggled in through the language of adequacy; it is a domestic constitutional command, binding on the Indian State in its own right.

That command cuts in two directions relevant to the present argument. First, it furnishes an indigenous yardstick by which the breadth of the Act's State-access exemptions can be tested. A discretion to exempt instrumentalities of the State, or to compel disclosure, that is unbounded by transparent criteria and unaccompanied by independent oversight sits uneasily with the necessity and least-intrusive-means limbs of the very test the Supreme Court has laid down. The constitutional vulnerability of the broadest readings of the exemptions is, on this view, a matter of Indian law before it is ever a matter of European adequacy. Second, and more hopefully, the shared commitment to proportionality suggests that the eventual reconciliation between Indian and European law need not be a one-way capitulation to Brussels. The Indian constitutional order already contains, in proportionality, the very analytical vocabulary that European adequacy assessment speaks. The conceptual distance between the two systems is, at the level of principle, considerably smaller than the divergence of their operative defaults would suggest. What is missing is not shared principle but an instrument that translates shared principle into mutual recognition, and a measure of legislative discipline in the drafting of the exemptions so that the principle is honoured in practice as well as in constitutional theory.

## VII. Towards interoperability: three calibrated paths

If the disease is unilateral extraterritoriality without coordination, the cure cannot be yet more unilateralism. Three interoperability instruments, in ascending order of ambition, offer the realistic routes out of the impasse. None requires either regime to abandon its values; each supplies, in different measure, the coordinating norm whose absence is the root of the problem.

The first and most immediate is the existing European transfer toolkit, deployed honestly. Standard contractual clauses, supplemented where necessary by technical and organisational measures of the kind the European Data Protection Board has prescribed, already permit lawful transfer to India in the absence of adequacy, provided the exporter conducts the destination-law assessment *Schrems II* requires and is willing to suspend where the assessment fails.[35] This is not a solution to the structural problem so much as a means of living with it, but it is available now, and it places a salutary pressure on the Indian State: the more constrained and transparent the Act's exemptions, the more readily an exporter can certify that the clauses will hold.

[35] Eur. Data Prot. Bd., Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (June 18, 2021) (setting out a six-step methodology requiring exporters to assess the law and practice of the destination State).

 [ISSN 2581-5369]

The second path is calibrated reform leading to a bespoke adequacy or transfer framework. India could narrow and structure the State-access exemptions of the Act, introducing an express test of necessity and proportionality, a measure of independent oversight, and a route of redress for the affected individual, sufficiently to make a European adequacy finding defensible; the European Commission could in turn engage with India's negative-list model on its own terms rather than insisting on a mirror of its own architecture, for adequacy is a finding of essential equivalence, not of identity. The histories of the Japanese, Korean and United Kingdom adequacy decisions show that this is achievable for States willing to discipline government access and guarantee independent supervision. The cautionary counter-lesson of the transatlantic saga is equally plain: a framework built on unaddressed structural divergence will be challenged and may fall, so durability depends on genuine convergence rather than diplomatic papering-over. It is worth recalling that India once contemplated a far more localising regime, in the data-localisation provisions of the Bills that preceded the Act, before settling on the lighter-touch negative-list model; the legislative trajectory shows a system still finding its settled position, and therefore still open to calibration.[36]

The third and most durable path is multilateral. Accession by India to a modernised multilateral instrument, most plausibly the updated Convention 108+ of the Council of Europe, which is open to accession by non-member States and articulates principles broadly compatible with both regimes, would supply precisely the superior coordinating norm whose absence Part IV identified as the root of the difficulty.[37] The instrument is not a panacea, and a candid account must note its present limitations: the modernising Protocol has not yet entered into force, several ratifications short of the threshold, and India is party neither to it nor to the underlying Convention.[38] Accession would therefore be a deliberate act of policy rather than the ratification of an existing commitment. But a shared multilateral floor would not erase the differences between the European and Indian defaults; it would give both systems a common reference against which mutual recognition could be calibrated, replacing the present vacuum with a

[36] Comm. of Experts Under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018); *see also* the Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (introduced in the Lok Sabha on Dec. 11, 2019, and subsequently withdrawn on Aug. 3, 2022), which contained mandatory data-localisation provisions abandoned by the 2023 Act.

[37] Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, opened for signature Oct. 10, 2018, C.E.T.S. No. 223 (not yet in force) [hereinafter Convention 108+], amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

[38] As of mid-2026 the modernising Protocol had secured thirty-four of the thirty-eight ratifications required for entry into force. Non-member States of the Council of Europe—among them Argentina, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay—are party to the underlying Convention; India is party to neither instrument.

 [ISSN 2581-5369]

framework, and it would do so on terms that neither subordinates India to European institutions nor leaves the enterprise caught between two unilateralisms.

Across all three paths runs a single condition. The obstacle to interoperability is not the negative-list default, which the European toolkit can accommodate, but the unbounded State-access architecture, which it cannot. Reform of the exemptions is thus the hinge on which every route turns; without it, clauses will not certify, adequacy will not issue, and accession will not bridge.[39]

## VIII. Conclusion

The GDPR and the DPDP Act are not poorly drafted statutes that happen to disagree. They are carefully drafted statutes that disagree precisely because each was built to project its own values across the globe without provision for the day when another sovereign would do the same. Extraterritoriality served a purpose when one regime reached outward into a world of regulatory vacuums; it becomes self-defeating when every regime reaches outward at once and their commands meet in the middle. Yet the meeting is not, for the most part, a head-on collision. The divergences over lawful basis and erasure are differences of architecture and degree, real and burdensome but bridgeable by careful design; the transfer models are in tension rather than contradiction, and the European toolkit already contains the instruments to manage them. The genuine conflict, the one place where obedience to one regime entails breach of the other, is the narrow but sharp field of State-compelled access, where the Regulation's prohibition on unauthorised disclosure meets the Act's expansive State exemptions.

Locating the conflict precisely is what makes a remedy possible. The path forward is not a louder assertion of jurisdiction but the patient construction of interoperability: honest use of the existing transfer tools in the short term; reform of the Indian State-access exemptions, anchored in India's own proportionality jurisprudence, as the indispensable medium-term condition; and, in the longer term, a bespoke adequacy framework or accession to a multilateral instrument that supplies the coordinating norm the present order lacks. *Schrems II* warns that arrangements built on unaddressed structural divergence will not endure; *Puttaswamy* shows that the principled foundation for convergence already exists within Indian law. The conceptual distance between the two regimes is smaller than their quarrelling defaults suggest. What remains is to build,

[39] On the practical obstacles to an Indian adequacy finding, see, for example, the European Data Protection Supervisor's 2024 decision concerning a proposed transfer of personal data by the European Investment Bank to India, which directed reliance on Article 49 derogations in the absence of demonstrated Article 46 safeguards (clarified in May 2025 as a procedural determination rather than an assessment of the DPDP Act).

 [ISSN 2581-5369]

across the narrow water that genuinely divides them, the bridge that two long arms, reaching past one another, have so far failed to make.

*****

 [ISSN 2581-5369]