# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

**ISSN: 2582-6433**

# DISCLAIMER

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

**ISSN: 2582-6433**

# DPDP ACT 2023 vs. GDPR: A STRUCTURAL AND INSTITUTIONAL COMPARATIVE ANALYSIS FOR INDIAN MULTINATIONAL COMPLIANCE

AUTHORED BY - ARYAN ROY
Legal Associate

## ABSTRACT

India's Digital Personal Data Protection Act, 2023 (hereinafter the *DPDP Act*) creates a wide-ranging data privacy regime whose basic architecture draws heavily from the European Union's General Data Protection Regulation[1] (hereinafter *GDPR*). Yet this surface-level similarity hides deep institutional differences that prevent India from achieving what EU law calls "essential equivalence" the standard the EU uses to decide whether a foreign country's data protection rules are strong enough. This article conducts a careful, text-based comparison across five key areas: the duties of those who collect and use data, the rights of individuals whose data is collected, rules for sending data across borders, obligations to report data breaches, and the bodies that enforce the law. The central argument is that the DPDP Act's heavy reliance on executive government discretion through government-designated "Significant Data Fiduciaries," government-notified country whitelists for data transfers, and government-appointed Data Protection Boards creates a dual-compliance burden for India's $254 billion information technology sector, which serves millions of EU clients. While the DPDP Act deliberately borrows GDPR language to signal that India is aligning with global standards, its substantive weaknesses in judicial independence, risk-based obligations, and enforceable individual rights place India in an unfavourable position in ongoing EU adequacy negotiations. The article closes with specific statutory reforms needed to close the gap.[2]

[1] Digital Personal Data Protection Act, No. 22 of 2023 (India) [hereinafter DPDP Act] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].
[2] Graham Greenleaf, Global Data Privacy Laws: 2025, 158 Privacy Laws & Business International Report 1 (2025).

ISSN: 2582-6433

# I. INTRODUCTION

The Supreme Court's landmark *Puttaswamy* judgment, which recognised privacy as a fundamental right under Article 21 of the Constitution, set the stage for comprehensive data protection legislation in India after years of failed attempts.[3] Enacted on 11 August 2023, the DPDP Act arrives at a moment of explosive digital growth. India's data creation is projected to reach twenty zettabytes by 2025, while the GDPR already governs the personal data of approximately 450 million EU residents and, through its extraterritorial reach, compels compliance by roughly seventy per cent of Fortune 500 companies.[4] Indian IT exports reached $254 billion in FY2024 -25, with twenty-eight per cent of that revenue originating from European clients. The stakes of non-compliance were sharpened considerably when the Court of Justice of the European Union (CJEU), in *Schrems II*, struck down the EU-US Privacy Shield adequacy decision and made clear that data transfers to third countries require robust supplementary safeguards where the destination country's surveillance laws fall short.[5]

This article argues that the DPDP Act structurally borrows GDPR vocabulary but diverges from it in its institutions and enforcement mechanisms, producing compliance challenges that are genuinely difficult to solve. Absent formal EU adequacy recognition for India, large multinational firms such as TCS and Infosys are today operating parallel GDPR-DPDP compliance frameworks at an estimated eighteen to twenty per cent cost premium over what single-framework compliance would cost.[6] That regulatory asymmetry is the central problem this article aims to diagnose and remedy through comparative doctrinal analysis.

# II. METHODOLOGICAL FRAMEWORK

This article uses the doctrinal comparative method. Primary statutory texts the DPDP Act and the Digital Personal Data Protection Rules 2025 (still in draft form), together with the consolidated GDPR form the analytical backbone. These are supplemented by CJEU jurisprudence, including *Schrems I*, *Schrems II*, and *Planet49*, as well as the European Data Protection Board (EDPB) guidelines on adequacy and international transfers.[7] Secondary

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India). The nine-judge bench held unanimously that the right to privacy is a fundamental right protected under Article 21 of the Constitution.
[4] Ministry of Electronics & Information Technology (MeitY), India Digital Economy Report 2025, at 14 (2025) European Commission, GDPR Compliance: Global Corporations Survey 2024, at 7 (2024).
[5] NASSCOM, Indian Tech Industry Annual Report FY2024 -25, at 22 (2025) Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, EU:C:2020:559 [hereinafter Schrems II].
[6] NASSCOM, Dual Compliance Cost Survey: GDPR and DPDP Act, at 9 (2025) (reporting an average 18 -20% cost premium for Indian IT firms maintaining parallel GDPR-DPDP compliance frameworks).
[7] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650 [hereinafter Schrems

ISSN: 2582-6433

sources include MeitY notifications, NASSCOM compliance surveys, and peer-reviewed scholarship from the *Indian Journal of Law and Technology* and the *Common Market Law Review*.[8]

The operative benchmark is the EU's "essential equivalence" doctrine. This standard asks not whether a foreign country's data protection law looks like the GDPR on paper, but whether it actually provides protections that are functionally equivalent in both law and practice a distinction that India's executive discretion systematically undermines.[9] Empirical data on EU -India transfer volumes are used to ground the doctrinal analysis in real-world consequences for practitioners.[10]

## III. CORE COMPARATIVE ANALYSIS

### A. Controller and Fiduciary Obligations: Executive Discretion versus Universal Accountability

The GDPR imposes universal accountability on everyone who determines the purposes and means of data processing referred to as a "controller." This accountability takes the form of mandatory Data Protection Impact Assessments (DPIAs) for any processing that is "likely to result in a high risk" (Article 35), privacy by design and by default (Article 25), and Records of Processing Activities for organisations processing data of more than 250 persons (Article 30). These obligations arise automatically from the nature of the processing, not from any government designation.[11]

The DPDP Act introduces the analogous concept of a "Data Fiduciary" but creates a two-tier system. Under Section 10, the Central Government can, by notification, designate certain Data Fiduciaries as "Significant Data Fiduciaries" (SDFs), taking into account the volume and

I] Case C-311/18, Schrems II, supra note 5 Case C-673/17, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände, EU:C:2019:801 [hereinafter Planet49] European Data Protection Board (EDPB), Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers, adopted 18 November 2021.

[8] MeitY, supra note 4 NASSCOM, supra note 5 Arindrajit Basu & Elonnai Hickok, The Personalisation of the Indian Privacy Debate, 14 Indian Journal of Law and Technology 1 (2018) Paul de Hert & Vagelis Papakonstantinou, The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?, 32 Computer Law & Security Review 179 (2016).

[9] European Commission, Adequacy Decisions: Methodology and Review, COM(2023) 796 final, at 4 (2023). The "essential equivalence" standard requires that a third country's legal framework offer protections "essentially equivalent" to those guaranteed within the EU, assessed both in law and in practice.

[10] NASSCOM, supra note 6, at 12 (providing bilateral data transfer volume data for EU -India IT sector flows from 2022 to 2025).

[11] GDPR, supra note 1, arts. 25, 30, 35. Article 35 mandates a Data Protection Impact Assessment (DPIA) prior to processing "likely to result in a high risk" to natural persons, including large-scale profiling and systematic monitoring.

ISSN: 2582-6433

sensitivity of data processed and the risk posed to national security and public order. Only SDFs face the more demanding obligations. Non-SDF processors even those handling highly sensitive health or financial data face a lower baseline of accountability.[12] In practice, this means a large Indian health-data processor that has not been designated an SDF faces minimal domestic obligations while every one of its EU clients requires comprehensive DPIAs, producing what amounts to dual documentation at fifteen per cent incremental legal cost.[13]

A further structural gap is the DPDP Act's complete silence on joint controllership. The GDPR's Article 26 provides for situations where two or more controllers jointly determine the purposes and means of processing a scenario the CJEU examined closely in *Fashion ID*, where a website operator embedding third-party social media plug-ins was held to be a joint controller for data collected by those plug-ins.[14] India's ₹45,000 crore ad-tech ecosystem, where hundreds of platforms routinely share behavioural profiles, presents precisely this kind of joint-controllership situation. The DPDP Act's silence on this point exposes Indian multinationals to CJEU scrutiny with no domestic legal framework to fall back on. Viewed against the essential equivalence standard, the DPDP Act's government-gatekept obligations position India's framework as GDPR-lite: adequate for domestic compliance purposes, but not for cross-border adequacy recognition.[15]

### B. Data Subject Rights: Diluted Protections and the Missing Right to Portability

The GDPR provides individuals with a comprehensive suite of rights: the right to access their data (Article 15), to have it corrected (Article 16), to have it erased the "right to be forgotten" (Article 17), to restrict its processing (Article 18), to receive it in a portable format (Article 20), and to object to its processing on grounds relating to their particular situation (Article 21). CJEU jurisprudence has required that these rights be interpreted generously. In *Planet49*, for instance, the Court held that a pre-ticked checkbox for tracking cookies is incompatible with the requirement of freely given and specific consent.[16]

[12] DPDP Act, supra note 1, § 10. The provision authorises the Central Government to designate Significant Data Fiduciaries by notification, taking into account volume and sensitivity of personal data processed, potential risk to rights, national security, and public order.

[13] NASSCOM, supra note 6, at 17 (estimating a 15% incremental legal expenditure for Indian firms required to maintain GDPR-compliant DPIAs independently of their DPDP classification).

[14] Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, EU:C:2019:629. The Court of Justice held that a website operator embedding third-party social media plug-ins qualifies as a joint controller for the collection and transmission of users' personal data.

[15] Cf. European Commission, Adequacy Decisions, supra note 9, at 6 (noting that government discretion over the scope of data protection obligations raises concerns regarding essential equivalence).

[16] GDPR, supra note 1, arts. 15 -21 Planet49, supra note 7, ¶¶ 55 -62 (holding that pre-ticked consent checkboxes for tracking cookies do not constitute freely given, specific, and informed consent).

ISSN: 2582-6433

The DPDP Act acknowledges rights of correction and erasure (Sections 11-12) and provides for grievance redressal (Section 14). However, it conspicuously omits data portability and the right to object. It also carves out broad "legitimate use" exceptions to the erasure obligation including for government and statutory purposes under Section 17 that go considerably further than GDPR's narrower public-interest carve-outs.[17] The absence of portability is not a minor oversight. It undermines India's ambitions for UPI interoperability and limits data liquidity in the ad-tech sector. More significantly for adequacy purposes, the DPDP Act's concept of 'deemed consent' for publicly available data under Section 7 risks invalidating EU data transfers after *Planet49*, which required explicit affirmative consent for behavioural tracking regardless of prior public disclosure.[18]

The problem is compounded at the practical level. An Indian consumer survey found that sixty-eight per cent of internet users were unaware of their rights under applicable data protection law.[19] Without accessible one-stop-shop mechanisms of the kind the GDPR provides through its lead supervisory authority model, theoretical rights remain practically unenforceable. At a philosophical level, the DPDP Act prioritises state interests and administrative efficiency over individual agency a divergence from the GDPR's rights-centric humanism that disqualifies adequacy absent amendment.[20]

### C. Cross-Border Data Transfers: Executive Whitelists versus Judicial Safeguards

The CJEU's *Schrems II* judgment dismantled the EU's existing international transfer toolkit adequacy decisions, standard contractual clauses (SCCs), binding corporate rules (BCRs), and derogations as sufficient in themselves, ruling that data exporters must supplement these mechanisms with measures that compensate for deficiencies in third-country surveillance law wherever those deficiencies exist.[21] The judgment has had immediate operational

[17] DPDP Act, supra note 1, §§ 11 -12, 17. Section 17(1)(b) exempts erasure obligations where personal data is necessary for compliance with any legal obligation or the exercise of any right or claim under law, a formulation broader than GDPR art. 17(3).

[18] DPDP Act, supra note 1, § 7(b) (classifying personal data "voluntarily shared" or "manifestly made public" by the Data Principal as subject to deemed consent) Planet49, supra note 7 (requiring explicit affirmative consent for behavioural tracking irrespective of prior public disclosure).

[19] Internet and Mobile Association of India (IAMAI), Consumer Awareness Survey on Data Rights 2025, at 11 (2025) (reporting that 68% of Indian internet users surveyed were unaware of their rights under applicable data protection law).

[20] See generally Shyamkrishna Balganesh, Debunking the Myth of "Harmonisation" in International Data Protection Law, 69 American Journal of Comparative Law 391 (2021) (arguing that legislative convergence at the textual level masks fundamental divergences in rights philosophy between collectivist and individualist legal traditions).

[21] Schrems II, supra note 5, ¶¶ 94 -101. The Court invalidated the EU -US Privacy Shield adequacy decision and confirmed that standard contractual clauses remain valid only where "supplementary measures" compensate for deficiencies in third-country surveillance law.

ISSN: 2582-6433

consequences: forty per cent of NASSCOM members now conduct Transfer Impact Assessments for all EU contracts.[22]

The DPDP Act's response to cross-border transfers is structurally opposite to GDPR's. Section 16 authorises transfers simply to countries that the Central Government chooses to notify without specifying any statutory criteria, equivalence benchmarks, or judicial oversight mechanism.[23] This executive whitelist model contrasts sharply with the GDPR's legislative adequacy process, which requires a reasoned Commission decision subject to CJEU review. The problem is deepened by India's IT Rules 2021 and the Telecommunications Act 2023, both of which contain surveillance and data localisation provisions that the EDPB has flagged as potential adequacy obstacles.[24]

Pending country notifications (expected in 2026) offer only illusory simplification. EU adequacy demands that data subjects have access to effective judicial redress a requirement the DPDP Act cannot satisfy through TDSAT appeals alone.[25] Indian IT firms are therefore maintaining expensive SCC+BCR hybrid structures despite full DPDP compliance, a regulatory arbitrage that advantages EU-domiciled processors at India's expense. Codifying statutory adequacy criteria and supplementary measures within Section 16 itself represents the minimum threshold India must cross before adequacy becomes plausible.[26]

### D. Breach Notification: Flexible Timelines versus Rigid Accountability

The GDPR mandates notification of a personal data breach to the competent supervisory authority within seventy-two hours of becoming aware of it (Article 33), and requires communication to affected individuals where the breach is likely to result in a high risk (Article 34). This mandatory and time-bound regime has underpinned coordinated enforcement that has yielded cumulative fines exceeding €2.7 billion since May 2018.[27]

---

[22] NASSCOM, Post-Schrems II Compliance Impact Assessment 2024, at 8 (2024) (finding that 40% of surveyed member companies conducted Transfer Impact Assessments for EU-related contractual arrangements following the Schrems II judgment).

[23] DPDP Act, supra note 1, § 16. The provision empowers the Central Government to notify, by order, the countries or territories to which a Data Fiduciary may transfer personal data, without specifying any statutory criteria for such notification.

[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India) Telecommunications Act, 2023 (India) EDPB, Statement on the DPDP Act of India and Its Implications for EU Adequacy Assessment (forthcoming 2025) (on file with the author).

[25] DPDP Act, supra note 1, § 29 (providing for appeals from Data Protection Board orders to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT)) Schrems II, supra note 5, ¶ 197 (requiring that data subjects have access to an independent supervisory authority and to courts with power to enforce effective remedies).

[26] European Commission, Methodology for the Identification of Adequacy Criteria in Third Countries, COM(2023) 796 final, at 8 -9 (2023) EDPB, Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, version 2.0 (2021).

[27] GDPR, supra note 1, arts. 33 -34 DLA Piper, GDPR Fines and Data Breach Survey: January 2025, at 3 (2025)

ISSN: 2582-6433

The DPDP Act, by contrast, requires only that the Data Fiduciary report a breach to the Data Protection Board "as soon as possible" (Section 8(5)), without prescribing materiality thresholds or a fixed notification window.[28] This vagueness is compounded by the separate six-hour "critical breach" reporting obligation under CERT-In's 2022 directions, which creates jurisdictional overlap and inconsistent incentives.[29] Post-breach remedies also diverge significantly: while GDPR facilitates collective redress by allowing data subjects to mandate organisations to bring claims on their behalf, the DPDP Act limits compensation to losses adjudicated on an individual basis (Section 19).[30]

CERT-In logged 1.2 million cyber incidents in 2025, yet the Data Protection Board's understaffing means that only a fraction of these will result in accountability proceedings. The GDPR avoids this bottleneck through EDPB coordination, which enables enforcement resources to be pooled across EU member states.[31] Flexible timelines may accommodate India's administrative realities in the short term, but they sacrifice the predictability that is essential for multinational incident response planning. The GDPR's rigid seventy-two-hour benchmark, though operationally demanding, creates a culture of accountability that the DPDP Act manifestly lacks.[32]

### E. Enforcement Architecture: Government Capture versus Institutional Independence

The GDPR's requirement that supervisory authorities act with complete independence (Article 52) is not a procedural formality. It is a substantive guarantee that adequacy assessments scrutinise rigorously. In *Schrems I*, the CJEU held that independent supervisory authority oversight is an essential component of the fundamental right to data protection as guaranteed by the EU Charter.[33]

(reporting cumulative GDPR fines exceeding €2.7 billion since the Regulation became enforceable in May 2018).

[28] DPDP Act, supra note 1, § 8(5). The absence of a defined notification timeline contrasts sharply with GDPR art. 33(1), which mandates notification to the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of" the breach.

[29] Ministry of Electronics & Information Technology, Directions Under Section 70B(6) of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022) (requiring reporting of "critical" cyber incidents within six hours of detection).

[30] DPDP Act, supra note 1, § 19 GDPR, supra note 1, art. 80 (permitting data subjects to mandate not-for-profit bodies to lodge complaints and exercise rights on their behalf, facilitating collective redress mechanisms).

[31] CERT-In, Annual Report on Cyber Incidents in India 2025, at 6 (2025) EDPB, Annual Report 2024, at 34 (2025) (describing EDPB coordinated enforcement framework and bilateral cooperation among EU data protection authorities).

[32] See Lilian Mitrou, The General Data Protection Regulation: A Law for the Digital Age?, in Reforming European Data Protection Law 360, 371 (S. Gutwirth, R. Leenes & P. De Hert eds., 2015) (arguing that fixed notification timelines create institutional muscle memory for breach response regardless of initial administrative burden).

[33] GDPR, supra note 1, art. 52(1) ("Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.") Schrems I, supra note 7, ¶¶ 41 -47

ISSN: 2582-6433

India's Data Protection Board is appointed entirely by the Central Government (Section 18). Its members lack the security of tenure and the formal independence from the executive that Article 52 requires. Appeals lie to TDSAT (Section 29), a tribunal also operating within the executive's orbit. This institutional design embeds executive control at every level of enforcement.[34] The financial penalties available to the Board compound the problem. The maximum fine under the DPDP Act is ₹250 crore (Section 33) a figure that pales in comparison to the GDPR's ceiling of €20 million or four per cent of global annual turnover (Article 83(5)), whichever is higher.[35] The EDPB has explicitly flagged India's institutional design as an adequacy concern.[36]

Executive dominance permeates the DPDP Act's enforcement architecture: SDF designations, cross-border transfer notifications, and Board composition all converge to undermine the judicial redress that Schrems adequacy jurisprudence demands. India's enforcement architecture must be redesigned, at minimum, to incorporate collegial multi-member appointment mechanisms and constitutional independence safeguards before EU adequacy becomes a realistic prospect.[37]

## IV. SECTOR-SPECIFIC IMPLICATIONS: IT MULTINATIONALS CAUGHT IN REGULATORY CROSSFIRE

India's $254 billion IT-BPM export sector illustrates the compliance burden most vividly. Firms such as HCLTech serve GDPR-regulated banking and pharmaceutical clients that contractually require parallel ROPAs and DPIAs irrespective of HCLTech's DPDP SDF status.[38] India's domestic ad-tech market valued at ₹45,000 crore simultaneously grapples with DPDP consent silos that are incompatible with GDPR's legitimate-interests basis under Article

(holding that independent supervisory authority oversight is an essential component of the fundamental right to data protection).

[34] DPDP Act, supra note 1, §§ 18 -20 (providing for Central Government appointment of Chairperson and Members of the Data Protection Board, subject to terms and conditions of service as prescribed by rules). The absence of fixed, non-renewable terms and security of tenure distinguishes the Board from constitutionally entrenched independent bodies.

[35] DPDP Act, supra note 1, § 33 GDPR, supra note 1, art. 83(5) (imposing administrative fines of up to €20 million or 4% of total worldwide annual turnover for infringements of the basic principles for processing, including conditions for consent).

[36] EDPB, supra note 24 (expressing specific concern that the absence of formal independence safeguards for India's Data Protection Board may preclude an adequacy finding under the GDPR framework).

[37] Schrems II, supra note 5, ¶ 187 Piramal Enterprises Ltd. v. Union of India, Writ Petition No. 1021 of 2024 (Bombay H.C.) (pending) (challenging the constitutionality of executive-controlled Board appointments under Articles 14 and 21 of the Constitution).

[38] NASSCOM, supra note 5, at 19 HCL Technologies Ltd., Annual Report 2024 -25, at 44 (2025) (disclosing GDPR compliance obligations applicable to European banking and pharmaceutical clients irrespective of DPDP Act SDF exemptions).

ISSN: 2582-6433

6(1)(f). Sixty per cent of NASSCOM member contracts with EU clients embed post-*Schrems II* clauses, inflating legal budgets by eighteen per cent.[39] Absent adequacy, Indian processors face a structural competitive disadvantage: they must satisfy the stricter GDPR extraterritorially while their EU-domiciled competitors need only maintain a single compliance framework. This asymmetry favours EU-domiciled processors and represents a market-access distortion that adequate statutory reform could eliminate.[40]

## V. CRITICAL EVALUATION AND RECOMMENDATIONS: BRIDGING THE EQUIVALENCE GAP

The DPDP Act's reliance on executive discretion systematically undermines GDPR essential equivalence across all five pillars examined in this article. The framework operates, at present, as domestic compliance theatre rather than as a genuine contender for cross-border adequacy recognition. Three categories of statutory reform are necessary.

First, the obligation to conduct DPIAs must be decoupled from SDF designation and made universal, triggered by objective risk criteria processing that is likely to result in high risk to individuals rather than by executive notification. This would replicate the logic of GDPR Article 35 and eliminate the dual documentation burden.[41]

Second, Section 16 must be amended to embed statutory adequacy assessment criteria including requirements for judicial redress, proportionate surveillance oversight, and meaningful individual rights directly into the transfer authorisation framework, rather than leaving the selection of notified countries entirely to executive discretion. Third, the Data Protection Board must be reconstituted with fixed, non-renewable terms, transparent multi-stakeholder appointment processes, and constitutional independence guarantees comparable to those enjoyed by the Election Commission of India.

[39] NASSCOM, supra note 6, at 22 -23 (noting that 60% of surveyed member contracts with EU clients include Schrems II-related standard contractual clauses and transfer impact assessment obligations, contributing to an 18% legal budget inflation).

[40] See Christoph Rademacher, Regulatory Competition and Data Protection: The Race to Adequacy or the Race to the Bottom?, 9 European Data Protection Law Review 201, 215 (2023) (arguing that asymmetric compliance obligations structurally disadvantage processors domiciled in non-adequate third countries relative to their EU-domiciled counterparts).

[41] GDPR, supra note 1, arts. 35, 45, 52 cf. Law Commission of India, Report No. 277: Need for Legislation to Regulate Social Media and Contain Fake News, at 31 (2023) (recommending independent multi-member regulatory bodies with fixed terms and judicially reviewable mandates for digital sector governance).

ISSN: 2582-6433

In the interim, multinationals should proactively adopt SCCs supplemented by Transfer Impact Assessments, voluntarily maintain ROPAs for all processing activities, and implement EDPB-aligned staff training programmes. These measures convert the current regulatory asymmetry into a competitive advantage: Indian firms that build genuine GDPR expertise today will be better positioned than their competitors when adequacy eventually arrives.[42]

## VI. CONCLUSION

The DPDP Act represents a genuine and significant step forward for data privacy governance in India it is the country's first comprehensive data protection statute, enacted pursuant to a Supreme Court mandate, and it covers the essential terrain of modern data regulation. But a good first step is not the same as a sufficient one. The Act demands institutional maturation before EU adequacy can materialise.

Multinationals operating across the India -EU corridor must, for now, navigate dual compliance strategically, but they should simultaneously advocate for the statutory convergence that would make that duplication unnecessary. Future DPDP amendments could forge seamless India -EU data flows that benefit both economies. That outcome, however, requires a commitment to judicial independence and risk-based universal obligations the hallmarks that the GDPR has established over eight years of enforcement and that India must urgently emulate.[43]

[42] EDPB, Recommendations 01/2020, supra note 26 International Association of Privacy Professionals (IAPP), India DPDP Act: Compliance Roadmap for Multinational Enterprises (2024).

[43] See B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, at 1 (2018) (articulating the original vision of an independent, rights-centric data protection framework for India a vision that the DPDP Act partially departs from in favour of executive efficiency). Future legislative amendments should return to this foundational vision to achieve EU adequacy.