EDITORIAL NOTE

Editorial Note

This final issue of the *Global Privacy Law Review* for 2025 (volume 6(4)) appears at a moment when data protection law is being pulled in two directions at once. On the one hand, legislatures and regulators are rapidly expanding formal rulebooks in response to new technologies and geopolitical pressures. On the other, basic questions about how these frameworks redistribute power between state, market and individuals remain unsettled. The three contributions in this issue speak directly to that tension, each from a different vantage point: a doctrinally rich constitutional critique of India's new data protection regime, a practitioner-oriented account of the same framework, and a book review that situates global compliance practice within an increasingly dense web of international norms.

We begin with an article by Medha Kolanu, Rudraksh Lakra and Abhijeet Shrivastava on India's Digital Personal Data Protection Act 2023 (Act 2023) and its implementing Rules 2025 (Rules 2025).[1] Written in the shadow of *Puttaswamy I* and *II* and the Justice B.N. Srikrishna Committee's work, the article asks whether India's first comprehensive data protection framework delivers on its constitutional mandate to protect informational autonomy, and whether it reflects global best practice. The authors' answer is sharply sceptical: the article contends that the Act and the Rules together construct a regime that foregrounds executive power and a data-driven political economy over the protection of individual and collective rights.

At the granular level, the article dissects key provisions of the Act 2023 and the Rules 2025: the broad exemptions for publicly available data and for research and statistical use; the government's power to exempt state instrumentalities and favoured classes of data fiduciaries; and the sweeping information-gathering power in section 36. These, the authors argue, amount to 'legal black holes' and 'grey zones' that do not meet the proportionality standards laid down by the Supreme Court in *PUCL, Puttaswamy* and later cases. The discussion of technical and organizational safeguards highlights how section 8(5) and Rule 6 rely on indeterminate notions of 'reasonable' and 'appropriate' measures, mandate potentially problematic log-retention requirements, and fail to anchor security obligations in recognized standards. The absence of direct statutory duties on data processors is presented as a striking departure from comparative practice.

The rights framework for 'data principals' is examined in similar terms. The authors show how open-ended qualifiers such as 'reasonably practicable' and 'reasonable to assume', combined with the lack of fixed timelines, risk turning notice, erasure and grievance mechanisms into discretionary privileges in the hands of data fiduciaries. The over-reliance on consent, coupled with an expansive 'legitimate use' regime under section 7 that operates without mandatory notice, is criticized as creating informational black holes and placing unrealistic burdens on individuals, particularly in a context marked by low digital literacy. For micro, small and medium-sized enterprises, a consent-only model is said to exacerbate competitive asymmetries, entrenching the dominance of large, data-rich firms.

From this granular critique the article moves to structural silences. It argues that the Act effectively abandons foundational principles such as robust purpose limitation and data minimization, and entirely omits heightened protection for sensitive personal data, despite the trajectory of previous Indian bills and the Supreme Court's differentiated approach in *Puttaswamy II.* The discussion of automated decision-making, algorithmic management and behavioural profiling is particularly forceful. The authors point out that, beyond a vague and arguably *ultra vires* due-diligence obligation for significant data fiduciaries (SDFs) in Rule 13(3), the law offers no explicit rights to explanation, human review or contestation, and no meaningful constraints on profiling or hyper-nudging. In this respect, the framework is described as 'trapped in a bygone paradigm' of individualized consent and one-off breaches, ill-suited to the relational and systemic harms of algorithmic governance.

The article's final sections place the Indian regime within a wider account of digital authoritarianism and the political economy of India's digitalization. The Act 2023 and the Rule 2025 are read alongside recent

Notes

[1] Medha Kolanu, Rudraksh Lakra & Abhijeet Shrivastava, *Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023*, in this issue, at 136.

surveillance-enabling legislation in telecommunications, broadcasting, taxation and postal regulation, and against the rise of Digital Public Infrastructure and Goods, such as India Stack, AgriStack and Health Stack. The authors argue that the data protection framework, far from constituting a constitutional shield, forms part of an 'architecture of control': broad exemptions, executive-dominated institutions, digital-only redress mechanisms that exclude large sections of the population, and an amendment to the Right to Information Act that removes the public-interest balancing test for disclosure of personal data. The result, in this telling, is a fusion of digital authoritarianism and private data extractivism built on unremunerated dispossession of personal and community data, accompanied by what the author terms a 'procedural fetishism' that elevates form over substantive data justice. The article closes by calling for a reconceptualization of Indian data protection law as a genuinely constitutional project that foregrounds both individual and collective rights.

The authors' analysis sets a demanding benchmark against which more practice-oriented treatments of the Act can be read. In that light, the report by Deepa Christopher, Jasel Mundhra, Nandini Pradhan and Aanchal Kabra of Talwar Thakore & Associates (TTA), *India's Data Protection Regime Notified: Overview of the Act and Rules*, provides a valuable counter-point.[2] Where the authors interrogate the Act 2023 as a constitutional statute and a node in a wider surveillance architecture, the TTA authors write from the perspective of advising organizations that must now build, test and run compliance programmes within its parameters.

The report begins with the formal architecture: the notification of the Act in August 2023; the central government's rule-making powers; the publication of the Rules 2025; and a phased enforcement timetable culminating in May 2027, when the main processing, enforcement and government-information powers take effect. Against this backdrop, the authors underline that while SDFs such as large online platforms, electronic commerce actors and financial and health institutions will face the heaviest burdens, the framework applies broadly to all entities processing digital personal data in India or targeting Indian data principals.

A central theme of the report, which resonates with, but does not adopt, the critique by Medha Kolanu, Rudraksh Lakra and Abhijeet Shrivastava, is the Act 2023's shift to a consent-centred model with only limited 'legitimate use' grounds. The TTA authors unpack the detailed notice requirements in section 5 and Rule 3: itemized lists of personal data, specified goods, services and purposes, clear and standalone notices in any of the twenty-two Schedule VIII languages, and obligations to inform existing data principals whose data was collected under pre-Act consents. They are explicit that commonly used, broadly worded privacy notices will not suffice, and recommend comprehensive data-mapping exercises to align internal processing with the new notice and consent architecture.

The report tracks many of the topics that Kolanu, Lakra and Shrivastava problematize, but with a practical, implementation-focused lens. On security, it outlines the minimum controls in Rule 6 (encryption, masking, access controls, backups, detection of unauthorized access) and the obligation to cascade security commitments into contracts with data processors. On breach notification, it explains the 'without delay' duty to notify both data principals and the Board, and the requirement to submit a more detailed report to the Board within seventy-two hours. Here, the TTA authors temper enthusiasm for full transparency with a concern that notification of all breaches, without any harm threshold, may overload both regulators and data principals, and dilute the salience of serious incidents.

The special regime for children and for persons with disabilities with lawful guardians is also addressed, with attention to the practicalities of obtaining 'verifiable consent' and building systems that can accommodate these categories. The discussion of SDFs draws out the heavier obligations to conduct annual data protection impact assessments (DPIAs) and audits, exercise due diligence in relation to algorithmic software, and comply with localization directions where applicable. The TTA authors candidly note uncertainties about the purpose and use of mandatory DPIA and audit submissions to the Board, and the breadth of the state's access rights under section 36 and the Seventh schedule, including their implications for European data-transfer assessments.

Taken together, the TTA report shows the same legislative material that Kolanu, Lakra and Shrivastava subject to constitutional critique being translated into checklists, workflows and governance structures. The interplay between the two pieces will be of particular interest to readers. Kolanu, Lakra and Shrivastava's analysis helps explain why certain provisions feel open-ended or unbalanced in practice, while the TTA authors demonstrate how, despite those structural concerns, organizations must now operationalize them under tight timelines and with incomplete guidance.

The issue concludes with a broader lens on global compliance practice in Prof. Dr Boris Paal's review of Lothar Determann's *Determann's Field Guide to Data Privacy Law. International Corporate Compliance.*[3] If the first two contributions examine in depth how one jurisdiction, India, is attempting to construct and implement a data protection

Notes

[2] Deepa Christopher, Jasel Mundhra, Nandini Pradhan & Aanchal Kabra, *India's Data Protection Regime Notified: Overview of the Act and Rules*, in this issue, at 156.

[3] Boris P. Paal reviews Lothar Determann, *Determann's Field Guide to Data Privacy Law. International Corporate Compliance* 235 (6th ed., Edward Elgar Publishing Cheltenham 2025), ISBN 978-1-0353-3629-6, in this issue, at 163.

framework, Determann's Field Guide exemplifies how multinational organizations are advised to navigate the resulting mosaic of regimes.

Paal situates the book against accelerating digital transformation, the proliferation and fragmentation of data privacy laws, and the corresponding demand for practical, risk-based guidance. He characterizes the Field Guide as a leading standard work that, in its sixth edition, sets a new benchmark for accessible and operationally relevant privacy literature. The book is praised for its dual ambition: to orient non-experts and to support experienced practitioners managing complex, often cross-border, compliance questions.

The review highlights the clarity of the book's architecture. An opening section introduces key concepts and actors, and maps the 'regulatory habitat' across Europe, the United States (US) and other regions. Subsequent chapters provide step-by-step guidance on building privacy programmes, managing international transfers, designing documentation architectures, and maintaining and auditing compliance frameworks, including in light of evolving cybersecurity and breach-notification expectations. Paal singles out the 'Data Privacy A to Z' as a hallmark feature: an alphabetically organized reference that covers topics ranging from anonymization and automated decision-making to dark patterns, children's privacy, tracking technologies and data ethics, combining speed of access with real analytical depth.

What makes the review particularly relevant to this issue is its emphasis on Determann's risk-based and proportionate approach, and on the need to integrate new legal and technological developments into coherent compliance strategies. Paal notes that the Field Guide does not simply catalogue developments such as new US state privacy laws, the latest EU-US transfer mechanisms, intensified scrutiny of artificial intelligence (AI) or, more broadly, the European 'Digital Omnibus' (General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), AI Act). Instead, it weaves them into realistic compliance models that can be implemented without undue burden. Read alongside the Indian contributions in this issue, the review invites reflection on how global compliance literature will engage with jurisdictions such as India, where commentators have highlighted the combination of extensive state powers, open-textured obligations and alleged gaps in core principles such as purpose limitation, data minimization and sensitive-data protection.

Across these three pieces, a common thread emerges. Each, in its own register, grapples with the same underlying problem: how to design and operate data-governance frameworks that are not merely formally comprehensive, but substantively protective of privacy, informational self-determination and democratic accountability in an era of algorithmic decision-making and pervasive surveillance. Kolanu, Lakra and Shrivastava remind us that the constitutional pedigree of privacy rights and the political economy of digital infrastructures matter when evaluating a statute's design. The TTA report demonstrates the scale of the task facing organizations as they translate such statutes into concrete practices under real-world constraints. Paal's review points to the kinds of tools and methodologies on which practitioners increasingly rely as they try to reconcile proliferating local regimes with global business models.

On behalf of the editorial team, I would like to thank our authors and reviewers for their thoughtful contributions throughout the year, and our readers for their continued engagement with the *Global Privacy Law Review.* I wish you all a merry Christmas and a happy new year, and look forward to continuing these conversations on global privacy, data protection and digital regulation in 2026.

Yours sincerely,
Ceyhun Necati Pehlivan
Editor-in-Chief