EDITORIAL

Editorial Note

This issue appears at a critical juncture in the ongoing development of data protection, privacy, and internet law worldwide. Across regions, legal systems are challenged by rapid technological advancement, increasingly complex data practices, and persistent gaps between legislative ambitions, regulatory implementation, and effective enforcement. The pieces assembled here reflect the breadth and diversity of these trends – ranging from the everyday compliance challenges faced by controllers and processors, to deeper conceptual tensions at the intersection of technology, individual rights, and institutional frameworks. They also engage with the pressing question of how rules are drafted and enacted, as well as the practical limitations that may follow.

Our contributors examine both jurisdiction-specific legal developments – such as Georgia's alignment with the European Union's (EU's) General Data Protection Regulation (GDPR), India's innovative Digital Personal Data Protection (DPDP) Act, and Ethiopia's controversial new regime – as well as broader and cross-border concerns. These include the accommodation of blockchain technology within the European data protection framework, new judicial developments on employment-related data processing, and the growing need to reconsider legal notions of inference and profiling in the digital context. A major theme running through this issue is the tension between regulatory ambition and practical reality, whether stemming from institutional cultures, legislative traditions, or the sheer velocity of technological change.

The articles, case note, and opinions collected here are intended not only as timely commentaries but also as starting points for deeper dialogue and future research. Collectively, they reflect optimism about the increasingly prominent role of privacy and data protection on legislative agendas around the world, while also offering a clear-eyed critique of unresolved dilemmas, institutional 'follies', and persistent structural limitations.

Irakli Leonidze opens this issue with an analysis of Georgia's new right of access, positioning it as a significant step toward international standards.[1] His article details how Georgian law mirrors many aspects of the GDPR, particularly in terms of information available to data subjects and the structuring of access rights. However, Leonidze thoughtfully identifies subtle but meaningful distinctions that must be understood for effective compliance.

Drawing from a breadth of European enforcement experience, Leonidze illustrates both positive practices and recurring challenges – such as delayed responses, incomplete information, or insufficient procedural safeguards – that Georgia faces as it builds its regulatory approach. He explores practical implementation issues, stressing the balance required between access rights and the rights of others, and underlining that any restrictions must be both proportionate and supported by law. Increasing engagement with the Personal Data Protection Service of Georgia, reflected in growing numbers of access requests and interventions, highlights the rising prominence of these rights and regulatory expectations.

Ultimately, the article makes clear that the right of access is fundamental: not just a procedural step, but a foundation for public trust, transparency, and the practical exercise of wider data rights. Leonidze's recommendations – for clear processes, accessible request mechanisms, and prompt, communicative responses – serve as a roadmap for Georgia's continued harmonization with the GDPR, supporting both robust national protections and international data flows.

In our second article, Paarth Naithani provides a critical analysis of the novel 'legitimate use' ground introduced by India's DPDP Act, 2023.[2] Naithani contrasts this new basis for processing personal data with the more established concept of consent, noting how DPDP Act, 2023 allows processing when a data principal voluntarily provides their data for a specified purpose and does not indicate non-consent. He argues that this 'specified purpose' should be interpreted narrowly, covering only the explicit activity for which data was provided – and not every conceivable use outlined in broad privacy policies.

Naithani draws on legislative intent and illustrative examples to demonstrate that voluntariness and reasonable expectations are essential. This is especially crucial in the digital sphere, where privacy awareness may be limited, and individuals must not be deemed to consent to secondary or unexpected uses of their data. The article

Notes

[1] Irakli Leonidze, *The Newly Formed Right of Access in Georgian Data Protection Law and the Distant Echo of the GDPR*, in this issue, xxx by 52 (2025).

[2] Paarth Naithani, *Strengthening Legitimate Use in India's Digital Personal Data Protection Act, 2023*, in this issue, xxx by 61 (2025).

stresses the importance of giving data principals a genuine option to opt out of processing, warning that an overly broad reading of legitimate use could erode the safeguards inherent in the consent-based model.

A further distinction is made between India's 'legitimate use' and the EU's 'legitimate interests' ground under the GDPR. While the latter allows for broader processing – such as marketing – Naithani notes that India's version is far narrower, focused solely on specified, voluntarily provided data for expected purposes.

To navigate the challenges of digital consent and the legitimate use ground, Naithani recommends that legitimate use should generally be reserved for non-digital contexts or transactions where obtaining express consent would be unreasonable or impracticable. In online settings, it should apply only where the data principal provides information for a basic, clearly requested service – not for broader processing described only in standard privacy notices.

Naithani concludes with a call for a robust, focused interpretation of the legitimate use ground – ensuring that, as India enters a new era of data protection, legal standards and practical implementation protect the autonomy and rights of individuals.

Turning to the intersection of technology and law, Modestos Gavalas examines whether blockchain's core features – immutability, decentralization, and pseudonymity – can be reconciled with the requirements of the GDPR.[3] Gavalas explores whether blockchain's architecture may inherently conflict with central GDPR principles such as data minimization, data subject rights, and the right to be forgotten.

The article begins by outlining blockchain's rapid adoption and decentralized, peer-to-peer validation, which stand in contrast to the GDPR's focus on individual control and the ability to erase data. Gavalas explains that while blockchain relies on pseudonymization, this does not necessarily exclude transactions from the GDPR's remit: case law, including decisions from the Court of Justice of the EU (CJEU), confirms that transactional data may still be considered personal data when linked with identifying information.

One particular challenge is the allocation of responsibility in such decentralized ecosystems. Drawing on guidance from regulators like the French *Commission nationale de l'informatique et des libertés* (CNIL) and recent case law, Gavalas argues that accountability should reflect the specific roles and power of each participant, rather than blanket liability for all network members. The most acute point of tension remains between blockchain's immutability and GDPR's right of erasure – an issue I previously analysed in an article published in the inaugural issue of the Global Privacy Law Review (GPLR).[4] Gavalas's article reviews possible solutions, including advanced pseudonymization, cryptographic key destruction, and, for permissioned blockchains, supervisory roles for central authorities – but notes that none offer a fully satisfactory answer for public, open networks.

Gavalas concludes that resolving these tensions requires a flexible, context-sensitive approach to regulation, coupled with real cooperation between legal and technical experts. Only by developing mutual understanding – legal professionals learning blockchain basics, technologists designing for privacy by default – can privacy protection and technological innovation be achieved in tandem.

Laroussi Chemlali's case note on *MK v. K GmbH* offers an incisive analysis of the CJEU recent interpretation of Article 88 of the GDPR, which governs Member States' ability to create employment-specific data rules.[5] Chemlali situates the case within the broader tension between national legislative discretion – whether exercised through statute or collective bargaining – and the overarching requirements imposed by the GDPR.

The note explains the factual background: a dispute in Germany concerning the transfer of employee data to a US-based server in possible breach of a works agreement, which raised critical questions about the interplay between detailed national rules and general GDPR obligations. The CJEU clarified that any rules or agreements adopted under Article 88 must satisfy both the specific safeguards required by Article 88(2) and the fundamental GDPR principles of lawfulness, necessity, transparency, and proportionality articulated in Articles 5, 6, and 9.

Chemlali highlights the CJEU's insistence that while collective agreements may reflect professional expertise and confer some discretion regarding data processing needs, this discretion is not beyond judicial scrutiny. Robust judicial review ensures that neither national nor sectoral rules dilute the strong protections established by the GDPR.

The note concludes by considering the broader impact of the ruling: employers across Europe are reminded to look beyond local legal compliance and thoroughly document the necessity of personal data processing, while employees can be confident that GDPR standards will be applied even in complex or hierarchical workplace relationships. The decision also advances harmonization across the EU, reducing the risk of legal fragmentation and reinforcing a high and consistent standard of protection for personal data in employment contexts.

Our book review by Iana Kazeeva and Małgorzata Wilińska of the University of Vienna offers a concise yet

Notes

[3] Modestos Gavalas, *Does Blockchain Technology Per Se Constitute a Breach of the GDPR? An Effort to Harmonize Two Seemingly Opposing Concepts*, in this issue, xxx by 66 (2025).

[4] Ceyhun Necati Pehlivan & Inés Isidro Read, *Blockchain and Data Protection: A Compatible Couple?*, 1 Global Privacy Law Review 39, 46 (2020).

[5] Laroussi Chemlali, *Balancing Employment and Data Protection: Insights from the CJEU on Article 88 of the GDPR in Light of MK v. K GmbH (Case C-65/23)*, in this issue, xxx by 73 (2025).

thorough critique of Prof. Pedro de Miguel Asensio's *Conflict of Laws and the Internet* (secondnd ed.).[6] The reviewers praise the monograph for its breadth, clarity, and analytical depth in addressing the wide-ranging challenges that digitalization poses for private international law.

They highlight the book's structure – six chapters covering foundational principles, digital services, data protection and personality rights, intellectual property, competition law, and contracts. Asensio's account of the cross-border nature of cloud computing, the impact of the Digital Services Act, and the complexities of the GDPR's extraterritorial application is particularly noted. The reviewers observe that, despite significant EU harmonization, complex issues remain, such as enforcing third-country judgments and defining the reach of GDPR rights like the right to be forgotten.

Kazeeva and Wilińska commend Asensio's accessible style and emphasis on practical problems, including jurisdiction, domain names, and concurrent claims. The book's analysis extends to recent regulatory developments and dispute resolution in digital contexts.

Overall, the review concludes that this edition is a comprehensive, authoritative, and up-to-date reference, remarkable for its nuanced, systematic, and practical approach to private international law in the digital age.

The issue also features two opinion pieces that call for fundamental rethinking in the field. First, Divyam Krishna questions the conventional distinction between the direct 'collection' of personal data and the creation of profiles or traits through algorithmic inference.[7] Krishna's central argument is that, from the standpoint of legal harm and fundamental rights, it makes little difference whether personal data is acquired directly or inferred – both trigger risks of manipulation, discrimination, and autonomy violations.

He observes that much of the academic literature treats inference and collection as legally distinct, with proposals ranging from new 'rights to reasonable inferences' to a focus on anti-discrimination protections or procedural safeguards under GDPR's Chapter III. Krishna instead advocates returning to the GDPR's core principle of data minimization, contending that inference and profiling should face the same requirements of necessity and proportionality as direct data collection.

Drawing on recent CJEU jurisprudence, including *Schrems v. Meta Platforms* and *Meta Platforms v. Bundeskartellamt*, Krishna demonstrates how 'strict necessity' and limits on data aggregation can – and should – be extended to algorithmic inferences. This approach, he argues, would provide regulators with a principled framework, resolve textual ambiguity in the GDPR, and enable more proactive enforcement. Ultimately, Krishna suggests that such a reconceptualization is fundamental not just in Europe, but for any regime modelled on the GDPR, including emerging systems in the Global South. He concludes that applying data minimization rigorously to algorithmic inferences is fundamental to distinguishing responsible, rights-respecting data practices from those that are manipulative or exploitative.

In the final opinion, Kinfe Yilma delivers a critical reflection on Ethiopia's new data protection law, focusing in particular on the decision to assign oversight to the Ethiopian Communications Authority – a move he argues fundamentally undermines the independence essential for credible privacy governance.[8] Yilma traces this institutional flaw to broader patterns in Ethiopia's legislative process, such as the marginalization of expert input and the prevalence of last-minute, ad hoc amendments by parliamentary committees or executive agencies. These practices, he contends, frequently result in significant departures from the original aims of draft legislation.

Yilma's critique goes beyond the specifics of the new law to address the dangers posed by weak legislative process more generally. He highlights that effective data protection depends not only on adopting international models but also on ensuring genuinely independent institutions that can command both legal authority and public trust. Drawing parallels with past Ethiopian laws, Yilma identifies a troubling pattern of non-transparent, non-expert revisions that undermine legislative clarity, effectiveness, and the broader rule of law.

He concludes by calling for meaningful legislative and institutional reform – emphasizing the importance of expert involvement, democratic process, and steadfast commitment to the values underpinning both law and personal privacy.

Together, these contributions offer a panoramic view of the field's most pressing issues and future frontiers. Several key themes emerge. First, the global influence of the GDPR remains incontestable, inspiring new laws, animating judicial reasoning, and shaping compliance debates well beyond the EU. Yet, as seen in both the Georgian and Indian contexts, local path-dependencies and policy priorities inevitably generate unique adaptations and challenges – be it the scope of data subject rights, the construction of new legal bases for processing, or the fine balance between facilitating commerce and safeguarding privacy and autonomy.

Second, technology's relentless advance – whether exemplified by blockchain or by the rise of advanced

Notes

[6] Iana Kazeeva & Małgorzata Wilińska review *Conflict of Laws and the Internet by Pedro de Miguel Asensio* (Cheltenham: Edward Elgar Publishing, 2d ed. 2024, 560, GBP 221. ISBN 978 1 03531 512 3), in this issue, xxx by 76 (2025).

[7] Divyam Krishna, *Towards a Legal Reconceptualization of Algorithmic 'Inferences' as 'Collection' of Personal Data under the GDPR*, in this issue, xxx by 80 (2025).

[8] Kinfe Yilma, *Follies of Ethiopia's Data Protection Legislation*, in this issue, xxx by 84 (2025).

algorithmic inferences – continues to stretch the conceptual and operational boundaries of data protection regimes. Our authors demonstrate that sophisticated legal reasoning and regulatory assessment remain essential tools for navigating these tensions, whether in interpreting fundamental rights, clarifying roles and responsibilities, or advancing data minimization as a safeguard against new types of legal harm.

Finally, multiple contributions warn against the risks of weak lawmaking, institutional fragility, and gaps in legislative process. The Ethiopian experience, in particular, shows how even well-designed laws can be compromised by deficiencies in independence, capacity, or political will. Genuine progress in privacy and data protection – across statutes, case law, or administrative practice – rests on continual investment in expertise, transparency, and effective institutions.

This issue thus stands not only as a review of current debates, but as a call to action for all stakeholders – lawmakers, regulators, scholars, and practitioners. Effective and equitable data governance will require not mere rulemaking but ongoing, thoughtful, and inclusive engagement with both the opportunities and the risks of our digital era.

Sincerely,
Ceyhun Necati Pehlivan
Editor-in-Chief