EDITORIAL

Editorial Note

As we wrap up 2024, it is with great pleasure that I present the final issue of this year's Global Privacy Law Review (GPLR). This edition, launched just in time for the festive season, offers a rich tapestry of insights into the multifaceted realm of privacy laws at a time when vigilance and innovation are paramount.

This year has been particularly memorable for me, as I became a father for the second time, welcoming another beautiful baby boy, *Jaime*, into my family. This personal journey has renewed my appreciation for the values of trust and protection, principles so integral to both parenthood and our collective work in privacy law. May this holiday season be a joyous time for you, filled with enriching discussions, and a Happy New Year to follow.

We begin with Patrick O'Connell and Peter Church's incisive examination, *No One Reads Privacy Notices. So Why Do We Have Them?*. The authors delve into the paradox of privacy notices – ubiquitous, yet widely disregarded. They argue that the inundation of lengthy, dense privacy documents alienates rather than informs users, becoming an exercise in 'compliance theatre' that fails to genuinely protect or empower consumers. By exploring the stark engagement gap, the article calls for a radical rethink of how privacy information is conveyed.

O'Connell and Church underscore the necessity for innovation in privacy communications. They propose methodologies that transcend traditional text-heavy notices, such as employing interactive formats, multimedia tools, and user-friendly designs to captivate and educate users. Their insights resonate with regulatory bodies and organizations striving to bridge the gap between compliance and meaningful engagement, ultimately advocating for a paradigm shift towards more effective communication strategies.

The authors illustrate their argument with empirical evidence from UK public bodies, which demonstrates that privacy notices tend to go unread or barely scanned. Highlighting these findings, they challenge both regulators and companies to prioritize clarity and accessibility in privacy notices to ensure users are truly informed about how their data is used.

Next, Tomasz Sowa's article, '*Malicious Insiders' Threats to Personal Data Security: The Hard to Comply Rules of the General Data Protection Regulation (GDPR)*, provides a meticulous exploration of insider threats. Although they constitute a minority of data breaches, Sowa reveals that they are disproportionately costly and difficult to detect. His analysis critiques the GDPR's current approach, which often treats all breaches with similar standards, neglecting the intricacies of insider-initiated incidents.

By elucidating the challenges organizations face in complying with GDPR requirements while managing insider threats, Sowa emphasizes the need for more granular legislative guidance. He proposes strategic adjustments to GDPR's framework to better distinguish between internal and external threats, advocating for specific compliance pathways that respect the unique dynamics of insider threats, thereby improving detection and mitigation.

Sowa calls for organizational introspection and the adoption of robust internal controls that balance compliance mandates with operational realities. His work is a clarion call for policymakers to craft regulations that are not only comprehensive but also flexible enough to adapt to the nuanced challenges of insider threats, ensuring that data protection is thorough and contextually relevant.

Indranath Gupta and Paarth Naithani focus on India's regulatory landscape in their piece, *India's Forthcoming Rules Under the Digital Personal Data Protection Act: An Opportunity to Reduce Gaps in the 'Notice and Consent' Framework for Cookies.* They provide a critical evaluation of the Digital Personal Data Protection Act, 2023, emphasizing the operational challenges inherent in India's socio-economic environment, characterized by high digital illiteracy and low privacy awareness.

The authors use cookies as a lens to explore broader systemic issues within the notice and consent framework. They highlight the inadequacies of current practices that often fail to offer true choices to users, emphasizing the need for reforms that align privacy practices with the realities of India's user base. Gupta and Naithani advocate for simplified, transparent notifications and emphasize the importance of meaningful consent that respects users' autonomy and understanding.

Their article also posits that India's forthcoming regulatory rules hold the potential to dramatically reshape how data privacy is realized on the ground. By aligning India's framework with global standards, while also respecting local contexts, the authors envision a balanced approach that empowers users and fosters trust in digital interactions.

Concluding this edition, Giacomo Bonetto's *case note*, *Which Must Be Determined First, the Purposes of Processing or the Data Controllership?* offers an intricate analysis of the Court of Justice of the European Union's *Norra Stockholm Bygg* judgment, which has sparked significant debate over its interpretations. Bonetto dissects the intricacies of determining data controllership versus processing purposes, advocating for a more nuanced consideration that could prevent conflicts between data protection and civil procedure rules.

Bonetto's critique focuses on how the ruling impacts the balance between judicial procedure transparency and data protection obligations. By highlighting the potential for misalignment between these objectives, Bonetto urges a reexamination of the relationship between data controllership and processing intents, emphasizing the need for clarity and coherence in legal standards to support fair and effective judicial processes.

His analysis brings to the fore the challenges courts face in integrating data protection principles with procedural justice, urging a refined understanding that respects both legal rigor and the fundamental rights of data protection. Through this lens, Bonetto affirms the need for ongoing dialogue between jurisprudence and data protection law to navigate the delicate balance these cases often demand.

As we conclude this richly informative issue, it is evident that while each piece brings a unique perspective, they collectively emphasize the importance of evolving data protection practices that are both innovative and grounded in real-world applicability. These discussions underscore a shared commitment to fostering an ecosystem where privacy is preserved, and trust is built across diverse contexts. The insights shared within these pages demonstrate the diverse challenges faced globally, yet they also highlight an encouraging movement toward resolving them through thoughtful, informed discourse.

As we journey into 2025, may these discussions inspire you to rethink, innovate, and advance privacy practices in ways that resonate with the foundational principles of protection and respect for individual rights. We hope you find these scholarly contributions both stimulating and instrumental as they pave the way for continued engagement and progressive dialogue in privacy law.

Warm regards,
Ceyhun Necati Pehlivan
Editor-in-Chief