EDITORIAL

Editorial Note

As we step into 2025, it is my pleasure to present the first issue of this year's Global Privacy Law Review (GPLR). This edition brings together a diverse range of articles that highlight the changing landscape of privacy law. Each contribution in this issue offers insights into the intersection of legal frameworks and technological advancements, showcasing the importance of protecting personal data in various sectors. Together, these discussions illustrate the need for aligning privacy practices and embracing innovative approaches to meet the challenges in privacy governance.

We begin with the pivotal *article*, 'Understanding Legitimate Interest under the GDPR: A Study of the CJEU Case C-621/22 and the EDPB Guidelines', authored by Sara Bonomi Madec and Georgia Vasileiadou.[1] This comprehensive analysis delves into the recent Court of Justice of the European Union (CJEU) ruling, significantly clarifying the role of commercial interests as legitimate interests under the General Data Protection Regulation (GDPR). The authors unravel the complexities of the case involving the Royal Dutch Lawn Tennis Association's data sharing practices, scrutinizing the balance between commercial gains and individual privacy rights. They highlight how the CJEU's decision marks an interpretative milestone by confirming that direct marketing can be considered a legitimate interest, provided it aligns with the criteria outlined in the GDPR.

Incorporating the European Data Protection Board's (EDPB's) concurrent guidelines, Madec and Vasileiadou emphasize the critical role these guidelines play in dissecting the concept of legitimate interest. Through a structured framework, the EDPB mandates a rigorous assessment of legitimacy, necessity, and proportionality, ensuring data controllers surpass mere commercial motivations with specific, lawful, and concrete justifications for personal data processing. The authors commend the EDPB for filling gaps left by the CJEU, thereby mitigating potential misinterpretations or broader applications that might otherwise arise.

The article also navigates the complexities of the GDPR's balancing test. Madec and Vasileiadou dissect the test's layered considerations – ranging from data sensitivity to the broader socio-economic and personal contexts that underpin data processing decisions. By drawing on practical examples, the authors illustrate the nuanced application of these legal principles, providing invaluable guidance for data controllers as they navigate the delicate interplay between operational needs and data subject rights.

Furthermore, this analysis underscores the ongoing debate triggered by the ruling over the relationship between legitimate interest and consent, particularly in direct marketing contexts. By provoking critical thought about how these legal bases interact, the article invites policymakers and data controllers to engage in deeper dialogues about consent's role within GDPR frameworks amidst shifting commercial landscapes.

In the *reports* section of this issue of the GPLR, Grace Tolin, Gavin Punia, and Jonathan Emmanuel delve into the various dimensions of the European Union (EU) Digital Operational Resilience Act (DORA), examining its practical implications for financial entities and the steps they need to take to achieve compliance.[2]

DORA represents a significant legislative initiative aimed at strengthening the digital operational resilience of financial entities across the EU. Recognizing the increasing reliance on technology within the financial sector, DORA seeks to enhance the ability of financial institutions to withstand, respond to, and recover from all types of information and communication technologies (ICT)-related disruptions and threats. This initiative is part of the broader EU digital finance strategy, which encompasses not only protecting the financial system but also promoting innovation and a more integrated market.

As discussed by the authors, at its core, DORA's scope covers a wide array of financial entities, including banks, insurance companies, investment firms, and critical third-party service providers, such as cloud computing services,

Notes

[1] Sara Bonomi Madec & Georgia Vasileiadou, *Understanding Legitimate Interest under the GDPR: A Study of the CJEU Case C-621/22 and the EDPB Guidelines*, in this issue (2025), at 5.

[2] Grace Tolin, Gavin Punia & Jonathan Emmanuel, *EU Digital Operational Resilience Regulation (DORA)*, in this issue (2025), at 12.

upon which these financial institutions depend. By encompassing such a broad spectrum of participants within the financial ecosystem, DORA ensures that resilience and robust cybersecurity measures are universally implemented across the board, minimizing vulnerabilities throughout the entire digital supply chain.

DORA mandates several key requirements, establishing a comprehensive regulatory framework for digital operational resilience. Financial entities are required to establish robust digital operational resilience testing, which involves regular testing of their ICT systems and controls, including penetration testing, vulnerability assessments, and other cybersecurity evaluations to ensure continuous operational effectiveness against potential cyber threats.

Moreover, DORA places significant emphasis on incident reporting, requiring entities to log, report, and adequately manage ICT-related incidents in a timely manner. The aim here is to foster transparency and enable a coordinated response to system-wide crises, which can mitigate the impact on the financial sector and preserve consumer trust.

Additionally, under DORA, there is a strong focus on third-party risk management. Financial entities are expected to ensure that third-party service providers comply with the same level of operational resilience standards, crucial given the pivotal role these third parties play in maintaining operational continuity and security within the financial institutions they serve.

Importantly, DORA brings together a harmonized set of regulations expected to reduce fragmentation across Member States, fostering a unified approach to cybersecurity and operational resilience within the EU's financial sector. This harmonization is anticipated to eliminate regulatory arbitrage, simplify compliance burdens for entities operating in multiple countries, and create a safer, more stable financial environment within the EU.

The report navigates the critical components of this legislation, offering insights on organizational preparedness, risk management, and the enhanced focus on digital resilience in the evolving landscape of EU financial regulation. As technology continues to shape and transform the financial sector, understanding and implementing DORA's measures will be integral to maintaining robust operational capabilities and securing the financial ecosystem against an array of cyber threats.

In the *case note* 'From Privacy Litigation to Privacy Restoration: How to Manage the Questions of How, When, and Whether. Case Note: *TR v. Land Hessen* (Case C-768/21)', Camilla Della Giustina and Pierre de Gioia Carabellese explore a landmark decision by the CJEU that underscores the discretionary powers of supervisory authorities under the GDPR.[3] This case elucidates how and when these authorities can exercise corrective measures. *TR v. Land Hessen* highlights that supervisory authorities are not mandated to deploy their corrective powers unless necessary to remedy a breach, thereby ensuring compliance while promoting high standards of data protection.

The factual background of the case involves a German savings bank employee who unlawfully accessed personal data without authorization. Despite this breach, the bank did not categorize the incident as high risk and opted for internal remedial measures without informing the affected customers. This prompted a legal question on whether supervisory authorities must always enforce corrective actions under Article 58(2) of the GDPR when a breach occurs.

The authors discuss the Advocate General's opinion, which clarifies that while authorities should diligently investigate breaches, they possess considerable latitude to decide on appropriate measures. This discretion empowers authorities to determine when corrective actions, such as fines, are necessary. Furthermore, the CJEU judgment emphasizes the principle of proportionality in enforcement, suggesting that not all breaches require stringent sanctions, particularly when minor violations occur or when the burden of penalties is disproportionate.

A notable contribution of this case note is the concept of 'autonomous measures', where entities implement corrective actions independently, reducing the need for supervisory authority intervention. This approach proposes a decentralized oversight model, prioritizing severe breaches while managing minor issues internally, akin to alternative dispute resolution principles.

Overall, the case note posits that *TR v. Land Hessen* signifies a shift towards private management of data breaches, emphasizing the discretionary authority of regulators while promoting efficient compliance and robust data protection. The authors suggest that this decision paves the way for rethinking privacy restoration mechanisms within the GDPR framework, highlighting the balance between regulatory oversight and individual accountability.

Finally, the *European Privacy News* segment highlights a range of significant advancements and actions within the sphere of privacy, data protection, cybersecurity, and artificial intelligence (AI) across Europe.[4] Edited and coordinated by Tanguy Van Overstraeten, with contributions from various authors and law firms, the article collates recent advancements and regulatory actions, providing valuable insights into Europe's rapidly evolving privacy landscape.

Notes

[3] Camilla Della Giustina & Pierre de Gioia Carabellese, *From Privacy Litigation to Privacy Restoration: How to Manage the Questions of How, When, and Whether. Case Note*: TR *v.* Land Hessen *(Case C-768/21)*, in this issue (2025), at 22.

[4] *European Privacy News* (Tanguy Van Overstraeten ed.), in this issue (2025), at 28.

The authors who participated in this piece are Tanguy Van Overstraeten, Lilianne Bunk, and Lorenz Wellinger (*Linklaters*) from Belgium; Milka Nikolova (*Kinstellar*) from Bulgaria; Vedran Kopilović and Marija Vuchetich (*Kinstellar*) from Croatia; Petr Bratský and Simona Semanová (*Kinstellar*) from Czech Republic; Sonia Cissé & Célia Moumine (*Linklaters*) from France; Tímea Bana and Daniel Endre Nagy (*Kinstellar*) from Hungary; Eleonora Curreri (*Linklaters*) from Italy; Catherine Freichel (*Linklaters*) from Luxembourg; Szymon Sieniewicz (*Linklaters*) from Poland; Ceyhun Necati Pehlivan and Elena Valin (*Linklaters*) from Spain; and Rupert Dugdale (*Linklaters*) from the UK.

Over the past year, numerous jurisdictions have taken decisive steps to address the evolving challenges in data protection and regulatory compliance. These developments indicate a growing emphasis on ensuring robust privacy standards while balancing the dynamic pace of technological innovation. Across Europe, data protection authorities have been increasingly proactive in enforcing GDPR compliance, with several high-profile fines imposed for violations. These actions underscore a broader commitment to maintaining transparency, accountability, and fairness in data processing practices.

The intersection of privacy laws with emerging technologies, particularly AI, has prompted detailed guidance and frameworks to ensure that AI systems align with established data protection principles. Efforts aim to harmonize the application of regulations like the GDPR with new legislative initiatives, such as the AI Act, ensuring that technological advancements do not undermine individual privacy rights.

Additionally, countries are adjusting their legislative landscapes to address discrepancies and align national practices with overarching EU standards. This includes reevaluating existing laws, introducing new legislative measures, and, in some cases, restructuring data protection bodies to enhance operational effectiveness and independence.

In conclusion, the *European Privacy News* underscores a concerted effort across jurisdictions to fortify privacy protections amid rapid technological advancement, a trend that will likely continue to shape the regulatory landscape in the coming years.

As we navigate through these rich discussions, I invite you to reflect on how these insights can inform your practices and policy formulations. Collectively, these contributions highlight the necessity of continued discourse and innovation in privacy law, ensuring that individual rights are protected within evolving socio-economic frameworks.

Wishing you a prosperous and insightful New Year as we delve into these engaging dialogues in the realm of privacy law.

Sincerely,
Ceyhun Necati Pehlivan
Editor-in-Chief