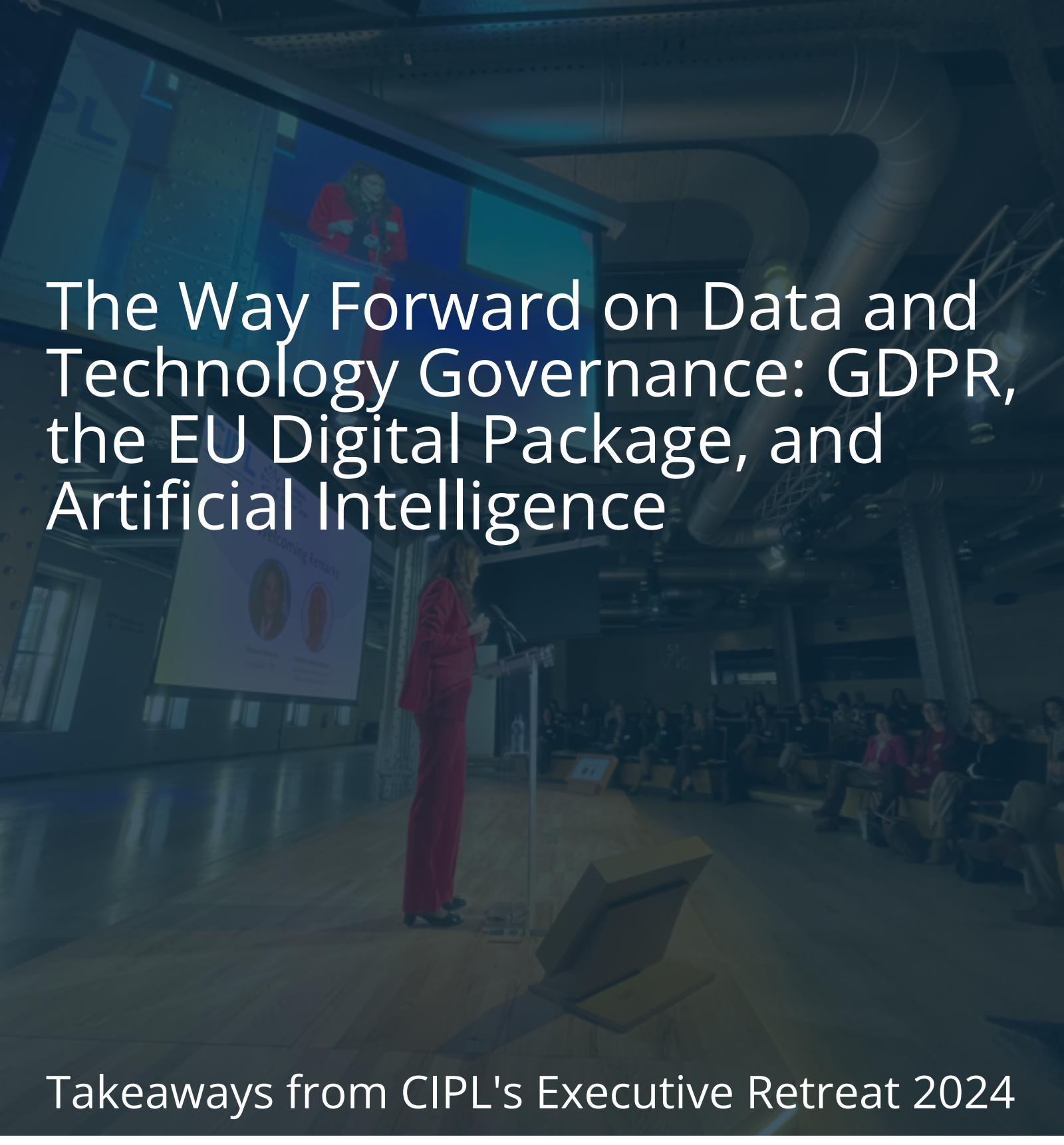


The Way Forward on Data and Technology Governance: GDPR, the EU Digital Package, and Artificial Intelligence

Takeaways from CIPL's Executive Retreat 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

The Way Forward on Data and Technology Governance: GDPR, the EU Digital Package, and Artificial Intelligence

KEY TAKEAWAYS FROM CIPL'S EXECUTIVE RETREAT 2024

On 12-13 March 2024, the Centre for Information Policy Leadership (CIPL) hosted its Annual Executive Retreat in Madrid, Spain. Day One of the retreat featured keynotes, roundtable discussions, and open conversations that sought to reflect on the intended outcomes of data protection legislation and the role of regulators, organisations, and other players in advancing responsible data use. Attendees included industry, data privacy lawyers and officers, data protection regulators, academia, and other thought leaders. The agenda focused on three topics—an "introspective retrospective" on the GDPR; an exploration of the ever-expanding and overlapping digital and data regulations; and an analysis of AI-related risks, mitigations, and benefits. The keynote presentations and discussions also touched upon the intersection of the fundamental right to data protection with other rights; the geopolitical dimension of AI; and the latest developments and challenges in accountable AI development, deployment, and governance.

Day Two provided an opportunity for industry leaders to discuss key takeaways from the previous day; to benchmark and share their views on the latest developments in relevant legal, policy, and compliance issues, and to provide input on CIPL's strategy for the coming year.

Both days of the retreat were held under the Chatham House Rule. The conversations and networking opportunities generated a wide variety of insights. Key takeaways include:

1. The GDPR has had an overall positive impact, but has not yet realised its full potential.

The GDPR has had a profound impact on the level of awareness of data protection in the EU and globally. It has contributed to an enhanced corporate privacy mindset and responsibility within organisations and resulted in creating a baseline global privacy management standard. Also, it helped drive privacy and data management as a board-level issue.

However, **as evidenced in the latest CIPL Discussion Paper, "The GDPR's First Six Years," certain challenges remain**, such as the lack of consensus on risks and harmsthe risk-based approach of the GDPR has not been fully realised, overly conservative interpretations of key concepts and requirements by DPAs, and the continued complexities of international data flow requirements. Also, the GDPR has not quite fulfilled its potential and ambition, especially in harmonising national rules and interpretations of DPAs; reinforcing and incentivising organisational accountability; and promoting wider adoption of codes of conduct, certifications, and BCRs.

Finally, **the GDPR should remain technology-neutral and must be interpreted in that way to ensure its requirements are also future-proof**. This will be especially acute with transformative technologies, such as AI, that present distinct tensions between data protection principles and the way technology works. It will require organisations and DPAs to be thoughtful about the interpretation and implementation of data protection principles to enable responsible development and use of AI.

Moreover, given the limited resources of both DPAs and organisations and in light of the increasing legal and compliance obligations stemming from the GDPR and other digital regulations, **the focus should squarely lie on a risk-based approach to compliance, data privacy management programs, regulatory supervision and enforcement, and the priortisation of meaningful outcomes, especially those that mitigate high-risk, high-impact harms**.

While DPAs in Europe must work within the framework of the Charter and ECJ and national case law, there is a real need and a recognition, including amongst some of the DPAs, of **the importance of cooperation between regulators, both nationally and internationall**y. At the same time, DPAs should take steps in practice to **better consider that privacy is not an absolute right: it must be balanced with other fundamental rights and interests, as well as with existing and new digital and sectoral laws**. DPAs must think more broadly and consider the impact of data and data privacy regulation on the overall digital landscape and the society and economy. With the enactment of new digital laws (discussed below in Takeaway #3), the GDPR (and privacy in general) has become part of a larger digital framework.

2. The Importance of an outcomes-based and risk-based approach to regulation, oversight, and compliance.

An outcomes-based approach shifts the regulatory focus from policing check-the-

box compliance to achieving tangible, beneficial results for all stakeholders and society as a whole. By envisioning what success looks like and working backwards to devise strategies for advancing that vision, regulators and organisations can focus on long-term goals rather than simply ticking compliance boxes. This also means adopting the risk-based approach to all areas of regulatory action and enabling regulators "to be selective to be effective" and deliver the right outcomes for all. In this way, organisations are held accountable for the actual impact of their actions. This would lead to more effective regulation, allowing for innovation and adaptation in an ever-changing digital landscape while ensuring that desired outcomes are met.

Importantly, though, **an outcomes-based approach relies on identifying good outcomes for society and individuals, and balancing those outcomes with unacceptable and unlikely risks and harms. It is crucial for all stakeholders—privacy regulators, regulated entities, government, and individuals—to be actively engaged in the process and, in a cooperative way, to build consensus on the outcomes to be achieved**. The outcomes-based approach is also part of organisational accountability—as organisations build and implement their data protection management programs, they should do so in a risk-based way and focus on delivering change and outcomes in practice, including the culture change within the organisation. This will be even more important with the new transformative technologies.

During the retreat, CIPL opened a survey asking attendees to reflect on the most important outcomes of data protection regulation. While attendees provided diverse responses, "*Building a society where people can trust that they will not be harmed by misuse of their personal information*" was prominent among them. Also, the concept of fairness was a persistent thread throughout the discussion, demanding renewed focus and consideration, especially as it is a central theme of both data protection and other areas of digital regulation, such as AI.

3. The regulatory focus is moving beyond data protection.

In Europe, the digital regulatory landscape is shifting from a sole focus on data protection/privacy concerns towards a more holistic approach, following the new legislative pieces introduced by the EU Digital Strategy. In addition to privacy, these new laws regulate online safety, competition, content moderation, data sharing, and AI. This is also becoming a global trend, with many other countries considering a more holistic digital and data strategy approach to regulation.

This means that **DPAs will have to cooperate and coordinate with regulators in other disciplines to facilitate effective implementation and a consistent approach, especially where there is increasing overlap and sometimes even conflict between different regulatory disciplines. For organisations, this also means having a more holistic approach to digital and data regulation, internal compliance and management programs; and oversight of such programs , which cannot consider compliance in silos**. Regulators will expect a coordinated approach between privacy, safety, and competition teams within an organisation when it comes to compliance and regulatory response strategies.

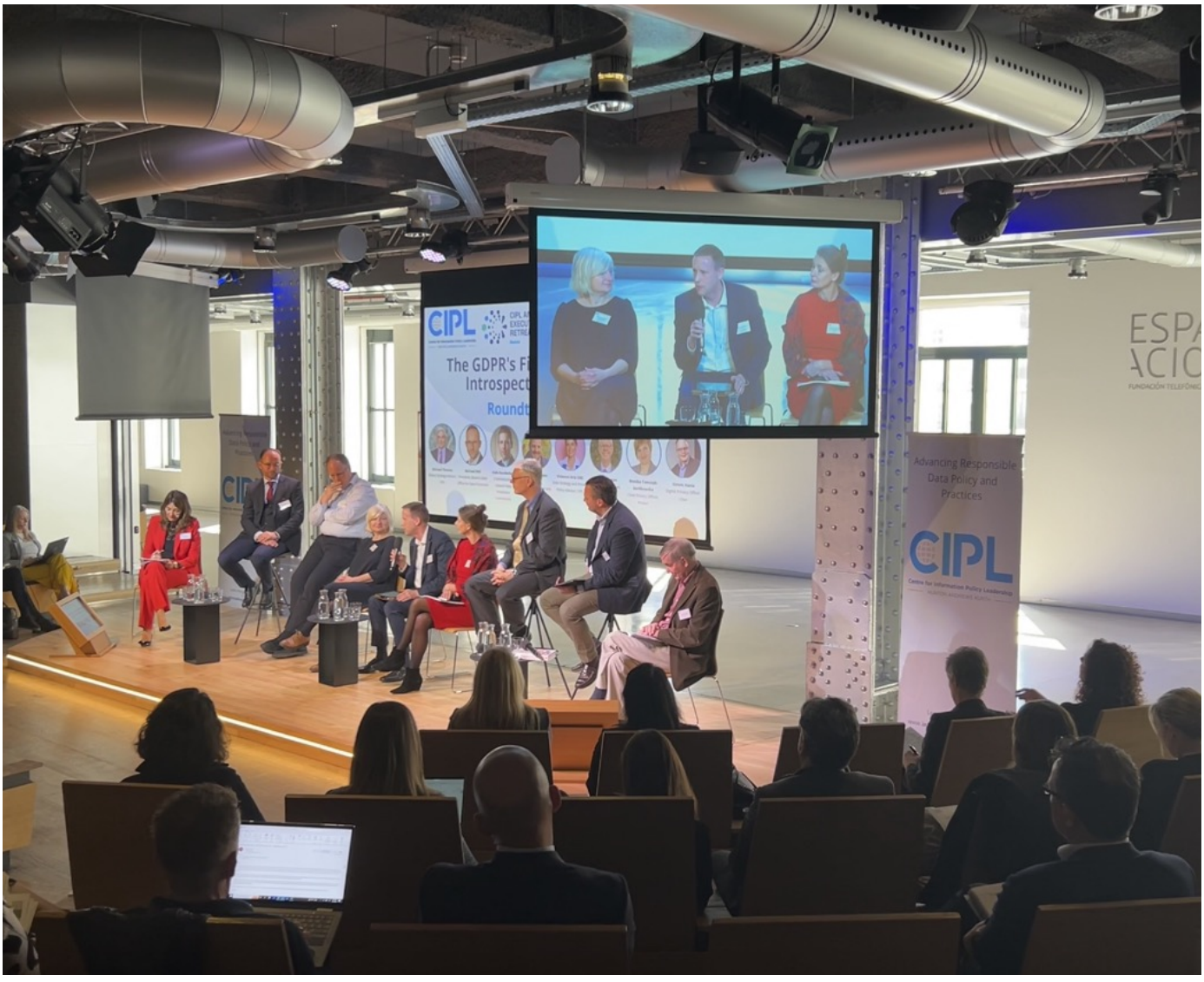
Overall, a collaborative approach and continued dialogue between all stakeholders in the new digital legislative frameworks, including organisations, will promote a shared understanding of the various requirements and obligations involved and will ensure more effective implementation.

4. Promote and encourage demonstrable and enforceable accountability under GDPR and other areas of digital regulation.

Organisational accountability serves as a key building block for effective data protection and corporate digital responsibility. Accountability ensures effective protection for individuals and their data, and it also enables digital trust and responsible use of data. There is a need to reinvigorate the focus on accountability, both by regulators and within organisations. In particular, how can regulators and organisations build a shared understanding of the expectations and elements of accountability and an effective and comprehensive privacy management program? **Throughout the retreat, many stressed that accountability is not just about compliance, but also about outcomes and behaviours. Both compliance and outcomes should be considered and delivered, yet the latter is perhaps even more important for the effective functioning of the GDPR and any regulation.**

Accountability of course extends beyond data protection and is central to all areas of data governance and digital compliance, including the responsible governance of AI. It fosters trust, transparency, and ethical practices whilst ensuring that organisations take responsibility for their actions and decisions. In particular, accountability enables organisations to consider fairness in data protection and in AI, for example, and provides them with a moral compass—a *North Star*—when navigating new legal and technological developments.

With the emergence of new digital laws in the EU, it is important for organisations to understand how accountability can be implemented consistently in the context of these new rules and across different legal disciplines, and how they can demonstrate their accountability to different regulators. Equally, it would be helpful for regulators to agree on the elements of accountability and how these can be demonstrated not only in data protection under the GDPR, but also across the other digital regulations, such as online safety, children's protection, AI, and competition.



5. The essential role of constructive and authentic engagement and open and trusted dialogue between regulators and regulated entities.

DPAs and organisations should maintain an open and trusted dialogue and authentic engagement. This is increasingly important in the times of ever-changing regulation, galloping technological advancement, and digital transformation of our societies. It is also essential given the trust deficit between industry and regulators and the general polarisation of our societies.

Organisations possess valuable insights regarding technological developments and the operationalisation of privacy principles. These insights can inform and help support the development of practical data protection frameworks. Organisations can share with regulators the challenges they face and the best practices they adopt, especially in the context of responsible AI governance and other transformative technologies, such as quantum and neurotechnology. Cooperation between organisations and regulators can also promote the development of codes of conduct, which have not been fully realised in the context of the GDPR. Finally, engagement would also advance shared understanding, interpretation, and consensus on the key outcomes, concepts, and requirements of the GDPR and other digital regulations.

Ultimately, ongoing engagement and knowledge-sharing between industry and regulators can collectively address emerging challenges and promote a regulatory environment that fosters innovation while safeguarding privacy and data protection rights.

6. Data protection's intersection with ESG/sustainability goals.

Data protection plays a key role in achieving ESG goals, particularly in the "S" (*social*) and "G" (*governance*) aspects. **Organisations can improve ESG ratings by building and implementing accountable data privacy management programs, with policies, controls, and privacy-protective measures such as data minimisation and retention policies, proper handling of data subject requests, implementation of privacy by design principles, increased transparency, and comprehensive training and awareness programs**. Good data governance promotes *social* goals by giving individuals greater control over their data, fostering transparency, and enhancing trust and brand value. It promotes *governance* goals by strengthening compliance, embedding risk management practices, and mitigating potential harms. Therefore, integrating robust data protection practices into organisational frameworks not only safeguards privacy but also contributes significantly to achieving broader ESG objectives.