

Takeaways from CIPL In Focus

Beyond Compliance: Data Governance as Business Enabler and Trust Builder

4 June 2025



Takeaways from CIPL In Focus

Beyond Compliance: Data Governance as Business Enabler and Trust Builder

4 June 2025

New York, New York

On June 4, 2025, the Centre for Information Policy Leadership (CIPL) hosted its first-ever “CIPL In Focus”—an immersive, full-day roundtable for senior-level professionals to examine in-depth the operational challenges related to a given issue and to share practical approaches for overcoming those challenges. The inaugural event was held at Hunton’s law office in New York City, on the 52nd floor of the MetLife Building in Midtown Manhattan.

The fast-moving, thought-provoking discussion focused on the future of privacy, data governance, and responsible innovation. CIPL’s white paper—[Leveraging Data Responsibly: Why Boards and the C-Suite Need to Embrace a Holistic Data Strategy](#)—served as the starting point for the conversation. Participants included partners from Hunton’s top-ranked global privacy and cybersecurity practice as well as chief privacy officers and other senior professionals from global businesses representing a wide range of sectors, including tech, financial, pharma, retail, hospitality, and entertainment.

To facilitate open dialogue, the event was held under the Chatham House Rule. The conversation looked beyond check-the-box compliance, addressing how to lead in an era of accelerating technological change, rising cyber threats, and shifting data privacy, cyber, and AI rules.

CIPL is pleased to share the following takeaways:

- **The role of the CPO and data leaders is expanding and changing quickly.** It is vital for privacy professionals to learn new skills and new technologies, and to bridge legal, technical, and business requirements in order to be effective. Be prepared to evolve into a risk manager and program manager, while maintaining a role as legal advisor.
- **Business metrics can be used to enhance value perception of the privacy office.** While operational metrics (such as the number of DSARs) can be helpful for evaluating the privacy team itself, the C-Suite and Board want to see business metrics, i.e., how have you contributed to the growth of the business? While quantification of achievements is valuable, qualitative descriptions of impact can also be valuable, especially when they are less readily quantifiable.
- **Professionals with a broad perspective are ideally suited to lead the data governance conversation.** Privacy is only one element when viewing data holistically. Organizations need to break down silos and view data with a multidisciplinary lens.

- **Understand what's coming next to remain relevant.** Look beyond privacy to spot trends and become more involved in the organization's data strategy. If you have a narrow remit, you will become obsolete. In addition to intersections with topics such as cybersecurity and management of non-personal data, AI accountability and AI literacy are prime areas to embrace.
- **Data and data monetization are now board-level issues.** With data as a revenue generator, establish clear guard rails for data sets and ensure that your organization has the appropriate rights and legal bases to use the data.
- **Data is also viewed as a strategic national asset,** as evidenced by the DOJ's Bulk Transfers Rule (90 FR 1636) and a rise in economic protectionism and digital sovereignty. Privacy professionals will need to understand and adjust their roles in light of this evolving nuance.
- **Privacy professionals should be business enablers who create "green paths" for innovation and business success.** Compliance itself is a business enabler. Organizations should understand and realize the benefits of compliance and how it builds trust. Consider building a framework for a "green path" that enables innovation and growth.
- **A risk-based approach to regulatory compliance is central to success.** With the growing complexity of global laws, it's no longer about chasing perfection, it's about building accountable programs grounded in strong, adaptable principles.
- **Articulating risk is key.** Framing risk in thematic terms can make it more understandable to the C-Suite. Reputational risk resonates with decision-makers, too. Emphasize the impact of risk to the bottom line. Be prepared to respond to the question: "What's in it for me?"
- **Companies and sectors have different risk profiles,** so be attuned to how you measure risk and how to evaluate your company's risk tolerance. For example, are you potentially facing a fine or will your business be banned?
- **Leverage others within your organization** to help spot and address risk. Create strong relationships, especially with those on the front line and those in engineering. Use internal channels of communication wisely. Ask questions.
- **Using AI agents to assist with privacy compliance may be helpful,** but assess your company's risk level before deploying AI tools. Agentic AI models still present many challenges.
- **Be the one who can bring the right people together.** In order to address risk properly, be able to identify the executives who "own" the different types of risk—financial, operational, reputational, legal, and technological—within your organization. Understand your company's org chart to identify key stakeholders.
- **To operationalize a holistic data strategy,** identify goals and develop a roadmap to navigate toward those goals. Go beyond giving advice; strive for something more tangible—something more akin to a deliverable.

- **Synthetic data has come a long way**; it has manifold ways to enable beneficial and valuable uses of data in a manner that respects privacy.
- **Cyber threats are more malicious than ever, from both criminal threat actors and nation states.** Attackers are employing increasingly sophisticated social engineering strategies. Training and tech literacy are essential, but even the best training won't stop every cyber-attack. Cybersecurity remains a key board-level concern, and organizations must focus on building practical plans to ensure smart, fast response strategies.

Next Steps

CIPL looks forward to continuing the discussion, with a particular focus on the evolving role of professionals in this space. If you would like to contribute to future discussions or inquire about future CIPL In Focus events, please [contact us](#).



The Centre for Information Policy Leadership (CIPL) is a global data and privacy policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.