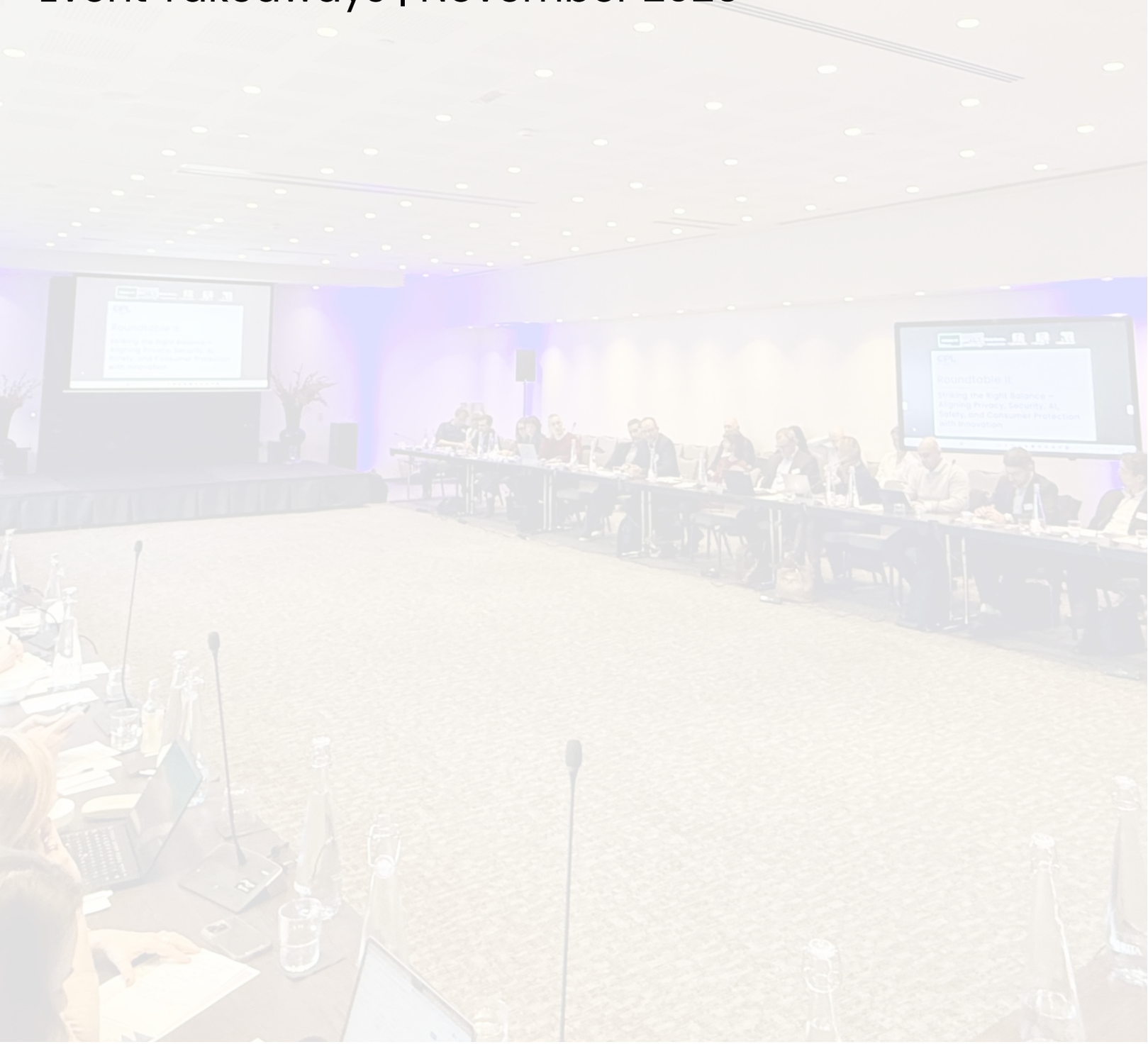
Centre for Information Policy Leadership
HUNTON

Key Takeaways from the CIPL Roundtable on Simplifying Europe's Digital Framework

Event Takeaways | November 2025



Key Takeaways from the CIPL Roundtable on Simplifying Europe's Digital Framework

At a moment of remarkable technological acceleration, Europe's increasingly complex digital regulations are at a critical turning point. The Centre for Information Policy Leadership (CIPL) convened a high-level roundtable in Brussels in November 2025, bringing together senior leaders from industry, data protection authorities, policymakers and academia to explore the key topics driving the discussions and chart ways forward.

The roundtable discussion examined a simplified, more coherent digital rulebook fit for the digital age, capable of fostering innovation and supporting European competitiveness. The takeaways below reflect CIPL's considerations emerging from the roundtable.

1. The Imperative for Simplification: A Digital Rulebook at a Crossroads

Europe's digital rulebook is at a critical inflexion point. The proliferation of intersecting and partly overlapping laws, from the GDPR to the AI Act, Digital Services Act, Digital Markets Act, Data Act, and cybersecurity legislation, creates legal uncertainty, imposes unsustainable compliance burdens, and ultimately threatens European businesses' ability to innovate and compete at scale.

This calls for an urgent shift toward "smarter" regulation. This does not require "deregulation" but can be achieved through strategic changes to the current rulebook, coupled with evolving interpretations of the rules and a shift in the mindset of regulators, policymakers, and lawmakers.

Key Tensions

The discussions highlighted several challenges stemming from the current digital framework:

Regulatory Overlap and Fatigue

Organisations described navigating a dense web of interconnected yet distinct laws. This complexity does not merely create difficulty but generates material implementation challenges for legal, engineering, and product teams tasked with operationalising a fragmented set of requirements into coherent business practices. This is especially true for smaller organisations with fewer resources. Instead of enabling structured compliance, overlapping and sometimes inconsistent obligations complicate translation into technical systems, governance processes, and product design. Participants expressed concern that this sustained implementation strain risks normalising workaround-driven solutions and reactive compliance behaviours.

Fragmented Interpretation and Enforcement

Difficulties equally persist due to inconsistent interpretation and enforcement of digital rules across the EU's Member States, creating an unpredictable environment for businesses operating across the Digital Single Market. Rather than facilitating harmonised compliance across jurisdictions - a core objective of the single market- this fragmentation risks producing divergent interpretations and uneven implementation, thereby reintroducing the very barriers the single market seeks to remove.

Disproportionate Compliance Burdens

Operational costs of compliance have been increasing significantly with every new piece to the legislative puzzle. For example, organisations report that the real-world external audit costs may be up to 500% higher than initial estimates by lawmakers. Both SMEs and large organisations operating in the EU report the disproportionate impact of the compliance burdens.

Intersection of Fundamental Rights and Proliferating Impact Assessments

A structural challenge lies in the limited integration of intersecting fundamental rights within the current digital regulatory framework. Organisations are required to give effect simultaneously to obligations relating to privacy, online safety, child protection, cybersecurity, fraud prevention, competition, data portability, and consumer transparency. While these objectives are individually well established, their interaction often generates operational trade-offs. Yet the framework has largely developed in legislative silos, without a sufficiently clear methodology for reconciling competing rights and obligations in practice. Teams frequently conduct multiple risk assessments for the same product or feature without sufficient guidance on redundancies.

---

2. The 'Digital Omnibus': First Impressions

The European Commission's draft "Digital Omnibus" proposal anchored a discussion on how simplification could be achieved in practice:

a) Stakeholders welcomed the Digital Omnibus as a constructive first step and would like to see further thoughtful consideration and evolution of the existing rules and interpretations.

b) The GDPR should not be reopened comprehensively. Instead, targeted clarifications are needed to address well-documented interpretive and operational challenges.

c) Targeted and precise legislative changes can enable a broader legal basis for processing of sensitive data for AI training and product development that depends on the use of sensitive data (health apps, safety features, etc.).

Against this backdrop, participants identified several areas where the proposal stimulated both convergent and divergent viewpoints:

- **Legitimate Interest for AI Development:** Establishing legitimate interest as a clear and usable legal basis for certain AI development activities is essential to enable innovation while preserving accountability, particularly where multiple fundamental rights need to be balanced and achieved simultaneously, e.g., public safety, fraud prevention, and cybersecurity. Legitimate interest, when properly applied, embeds risk-benefit analysis, safeguards fundamental rights, and ensures organisational responsibility more effectively than consent, especially in complex, data-intensive contexts.[1]

- **The Definition of 'Personal Data':** The interpretation of "personal data" has progressively broadened in practice, particularly with respect to pseudonymised and indirectly identifiable data. While the GDPR intentionally adopts a broad definition, challenges arise when this breadth is not accompanied by sufficiently risk-based and context-specific application. Greater differentiation in the regulatory treatment of fully anonymised data, pseudonymised data, and data directly linked to identified individuals could enhance legal certainty and proportionality. A more nuanced approach, consistent with the GDPR's architecture and evolving CJEU jurisprudence, would preserve strong protection while better reflecting varying levels of risk.

- **Browser-Level Consent and Opt-Outs:** Proposals relying on browser-level consent or objection mechanisms raise questions of feasibility, governance, and enforceability. Without clear design standards and accountability mechanisms, such approaches risk creating new layers of complexity without delivering meaningful transparency or user control, while also undermining existing service models.

3. The Necessary Trade-Off: Balancing Privacy Against Physical Safety and Public Good

A central challenge in simplifying Europe's digital framework lies in reconciling data protection with other fundamental rights and societal objectives, including physical safety, public health, and technological progress. Absolute interpretations of privacy obligations can, in certain contexts, undermine broader public interests. The roundtable explored several real-world examples where these goals come into direct tension and illustrate the difficult trade-offs that policymakers, regulators, and businesses must navigate.

	Innovation/Safety Goal	Privacy Challenge/Tension
Physical Safety	Developing innovative safety features, such as optional in-trip audio recording in rideshare services, that could deter and document interpersonal conflict.	Navigating strict privacy interpretations impedes innovations of safety features that provide clear consumer benefits.

[1] Please see CIPL Paper: Legitimate Interests for Data in AI Training - The DPO Perspective, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_legitimate_interests_for_data_ai_training_dpo_perspective_dec25.pdf.

	Innovation/Safety Goal	Privacy Challenge/Tension
Automotive Safey	Collecting real-world driving data to improve Advanced Driver-Assist Systems (ADAS) is critical for training models to handle rare but dangerous traffic scenarios and prevent accidents.	Overcoming the limitations of consent as a practical legal basis can result in the loss of 60-80% of necessary life-saving data.
Health & Research	Using personal and even sensitive health data remains crucial for R&D, particularly in fields like preventative medicine and addressing historical gaps in women's health diagnostics.	Balancing data access for R&D with stringent, sensitive data rules can slow or block vital innovation.
Fraud Prevention & Financial Integrity	Deploying AI-driven monitoring systems to detect fraud, identity theft and financial crime.	Balancing continuous monitoring and data aggregation is necessary to detect sophisticated fraud patterns with proportionality, transparency and purpose limitation requirements.
Digital Identity & Biometrics	Using biometric verification to secure digital identity and prevent impersonation across online services.	Ensuring enhanced safeguards, lawful bases and risk-based limitations for biometric data processing, while recognising the security benefits of strong identity assurance mechanisms.
Cybersecurity & Threat Detection	Conducting network traffic analysis, anomaly detection, and log retention is essential to prevent cyberattacks and protect critical infrastructure.	Reconciling broader monitoring and data retention practices required for effective threat detection with data minimisation and storage limitation principles.
Online Safety & Platform Compliance	Implementing proactive monitoring, content moderation and systemic risk mitigation tools to comply with DSA obligations.	Ensuring monitoring mechanisms respect privacy, avoiding disproportionate surveillance, and maintaining appropriate safeguards while meeting the breadth of regulatory expectations for systemic risk management.

These cases reinforce the need for a context-specific, risk-based application of data protection law, shifting the focus from formalistic compliance to real-world outcomes and harm prevention.

4. The Path Forward: From Legal Theory to Operational Reality

Simplification must extend beyond legislative text to the practical operationalisation of compliance. Complex legal obligations cannot deliver effective protection if they cannot be translated into engineering, product design, and governance processes.

CIPL identifies four operational priorities

1. Promoting holistic internal governance. As a result of the challenges posed by fragmented compliance, the trend towards a consolidated, intra-organisational response has emerged. Entities are observed moving toward integrating internal governance teams, functions, and controls such as risk assessments, transparency, training and awareness. One example provided is a "Trusted Technology Group" that unites traditionally siloed functions, including privacy, accessibility, digital safety, human rights, and responsible AI. This holistic structure ensures a consistent and coherent approach to trust, allowing the organisation to manage competing obligations from a unified perspective rather than through conflicting workstreams. Other examples are the creation of unified and integrated review and risk assessment processes that encompass privacy, online safety, children's best interests, and responsible AI considerations.

2. Developing a 'Standardisation Layer' to solve the operational crisis of legal teams being unable to give engineers clear answers. This layer acts as a translator, ingesting fragmented legal obligations from various regulations and converting them into a unified set of technical standards to ensure engineering teams are part of the process. For example, multiple rules on user control could become a single "customer choice" standard for engineers, dramatically simplifying implementation.

3. Shifting to Outcomes-Based Regulation There was a strong consensus on the need to support an outcomes-based regulatory model. This approach would see regulators define the high-level objectives (the "what") while empowering organisations to determine the most effective, risk-based methods for achieving them (the "how"). This fosters innovation in compliance and allows businesses to embed protections in a way that is tailored to their specific technologies, rather than following a one-size-fits-all prescriptive set of rules. Outcomes-based regulation strengthens organisational accountability and pushes organisations to implement best practices, controls, processes and tools to achieve desired outcomes in a more flexible and scalable manner, appropriate to the risk, size and complexity of their operations and offerings.

4. Encouraging technical solutions for compliance challenges and accountable programs. Organisations reported the need to invest in technical solutions to address compliance challenges, including the development and use of Privacy-Preserving Technologies, automation of compliance processes, and the use of technologies such as AI to aid compliance. Investments in PPTs and the automation of accountability programs and measures must be further encouraged and explored by all. Organisations would like to see regulators proactively incentivise and support these initiatives more and provide legal clarity for when they are "good enough" to ensure appropriate levels of compliance.

5. Conclusion: A New Blueprint for Digital Governance

A meaningful simplification requires a shift in regulatory mindset, not merely technical amendments. Europe's digital future depends on a governance framework that is agile, risk-based, and operationally grounded, capable of evolving alongside emerging technologies.

The discussion revealed a number of ideas, and CIPL identifies here three priorities for this new blueprint:

1. Adopt Agile and Risk-Based Regulation and Regulatory Action: Policymakers must embed risk-based principles at the core of new legislation, focusing resources where the potential for harm is greatest. Equally, regulators must act in a risk-based way, in order to be most effective and prioritise resources in high-risk areas. Regulators should actively support innovation through mechanisms like regulatory sandboxes and ensure their frameworks can adapt to emerging technologies, safeguarding Europe's competitive edge.

2. Encourage Integrated Accountability: Regulators and lawmakers should encourage demonstrable accountability and understanding that it delivers the most effective outcomes for all. Furthermore, regulators should enable integrated organisational accountability, allowing companies to manage privacy, safety, and ethical risks holistically rather than through siloed compliance functions.

3. Shared goals and sincere constructive dialogue: Foster genuine collaboration among policymakers, regulators, industry, and civil society to ensure Europe's digital framework both protects fundamental rights and enables innovation while supporting global competitiveness. In today's interconnected digital landscape, all stakeholders face common challenges and opportunities. Sincere, transparent, and constructive engagement—underpinned by mechanisms for ongoing dialogue and information exchange—is essential to align efforts, build trust, and achieve shared objectives.