Centre for Information Policy Leadership
HUNTON

Innovation, AI and Data Protection: Smart Regulation in a Changing World

Event Takeaways | 1 April 2025

Innovation, AI and Data Protection: Smart Regulation in a Changing World

London, 1 April 2025

Event Takeaways

The Centre for Information Policy Leadership (CIPL)[1] has long advocated for and provided thought leadership on risk-based organisational accountability and proportionate and outcomes-based regulatory frameworks in data protection and broader digital and data policy.[2]

Enabling responsible innovation to advance economic growth has become central to the global discussions on privacy and digital policy. As the digital landscape rapidly evolves, policymakers worldwide are exploring pro-innovation approaches to regulate emerging technologies effectively without stifling innovation. For example, the EU has initiated a simplification agenda aimed at streamlining its complex digital law and policy frameworks.

On 1 April 2025, CIPL held a roundtable on 'Smart Regulation in a Changing World' to discuss shared challenges and potential solutions to support more agile, effective regulation that can facilitate innovation.

The discussion, held under the Chatham House Rule, included government officials, regulators, and industry experts discussing their roles in encouraging smart, risk-based, and evidence-based regulatory approaches. Below, we share the key themes, insights, and recommendations developed during the discussion.

Context

Data Protection as an Enabler of Growth

- The responsible use of data is a business enabler and a driver of economic growth.[3]

- Data governance laws enable trust by upholding fundamental rights and facilitating the responsible use of data.

- In that context, data protection authorities (DPAs) can play a crucial role in fostering responsible economic growth, safeguarding individuals, and facilitating compliance. DPAs should act as stewards of the data economy and regulate in a balanced and contextual manner, ensuring the protection of fundamental rights while allowing technology to thrive. As data protection is horizontal and intersects other disciplines such as competition, cybersecurity, consumer protection or online safety, DPAs should cooperate with their regulatory counterparts to foster common understanding and mutual learning.

Data Protection as an Enabler of Growth

- Effective, smart regulation encourages responsible economic growth, protects individuals from real harm, and increases user trust in organisations' data processing. It aims to increase regulatory certainty for organisations,

promote accountability, and allow sufficient room for organisations to tailor compliance to their products, services, and cultures through a principle and risk-based approach.

- At the same time, the behaviour of regulators and a consistent and evidence-based interpretation of laws are just as important as the laws themselves.

- A lack of uniform interpretation or common understanding of the GDPR across member states persists. While some differences are due to differing national legal systems, there is still room for better alignment on the fundamental principles of the GDPR. One of the key remaining challenges for DPAs is coordinating and bridging the differences through the relevant coordination bodies, such as the EDPB.[4]

- There is an increasing demand for enhanced cooperation not just amongst DPAs, but across sectors and digital regulators in order to ensure a harmonised approach where competencIes overlap. Initiatives aimed at supporting effective cross-regulatory cooperation, similar to the UK DRCF, are developing in Ireland, the Netherlands, Germany and internationally, but there should be a stronger push for more.

- Similarly, organisations must create streamlined internal approaches with a consistent, accountable approach to data compliance.

- The ongoing debate around simplification of regulatory frameworks to enable and encourage innovation does not take away from the importance of regulation or robust oversight. It supports the need for regulation that is adaptive to governing an increasingly complex and digital environment.

Key Considerations for Better Outcomes

1. Evolving Mindsets and Legal Interpretation

While the GDPR is intended to be principle-based and technology-neutral, these features must be actively enabled through the way the law is interpreted and applied. Legal interpretation should not be static but dynamic, risk-based, and rooted in our digital reality to ensure the GDPR remains future-proof and relevant in the face of rapid technological change.

Overly narrow readings of the law can restrict legitimate uses of data, and regulators should consider how the law might accommodate such uses with appropriate safeguards rather than preclude them entirely. This requires a deep understanding of the existing technology, business models, as well as societal expectations.

2. Clarifying Legal Uncertainty

Legal uncertainty, ambiguity, or rigidity can create barriers to responsible innovation, and innovators welcome legal certainty and regulatory guidance. At the same time, efforts towards the simplification of the complex regulatory framework are necessary, but a focus on just reporting burdens for SMEs may not go far enough. More fundamental clarifications are needed to address issues arising from new technologies and evolving societal expectations.

The reforms to the UK's data protection framework under the Data (Use and Access) Bill can provide examples of targeted legislative updates in support of innovation through simplifying compliance mechanisms, such as clarifying the use of legitimate interests and refining the approach to automated decision-making.

3. Promoting Innovation-Positive Regulatory Culture

Ongoing efforts by regulators to engage constructively with industry and promote innovation through mechanisms are welcome and necessary. Innovative regulatory tools like sandboxes are effective platforms for dialogue, testing novel use cases, and co-creating compliance strategies in a safe and supervised environment. The sandbox provisions under the EU Artificial Intelligence Act (EU AIA) provide a welcome step and a signal in the right direction.

Robust enforcement remains a crucial backstop for the protection of fundamental rights, but it must be applied proportionately and constructively. More efforts should be made to systematically integrate innovation-friendly considerations into the regulatory culture, including the development of incentive frameworks and the broader use of innovative agile regulatory tools.

Regulators should consider outcome-based enforcement strategies and recognise and reward organisations demonstrating maturity in their privacy practices instead of pursuing a punitive or rigid approach to enforcement. More nuanced enforcement models take into account organisational efforts, such as early engagement with regulators or the deployment of privacy-enhancing technologies (PETs), and reflect these efforts in regulatory decisions.

In all efforts, the public also needs to be brought on the journey, by organisations, regulators and policy makers alike.

4. Cross-Sector and Cross-Border Collaboration

Increased collaboration across regulatory domains—such as between data protection, AI, consumer protection, and competition authorities—as well as between jurisdictions, is essential to ensure coherent governance of complex technologies and to minimise regulatory fragmentation, and increase legal certainty for organisations.

Equally, organisations must align their governance practices internally and be prepared for overlapping regulatory requirements.

5. Formalising the Risk-Based Approach

A risk-based approach provides much-needed flexibility and focus in data protection compliance. It allows regulators and organisations alike to allocate resources proportionately, concentrating on high-risk activities and adopting lighter-touch measures for low-risk cases.

6. Elevating Accountability as a Governance Tool

Accountability is a cornerstone of modern data governance. Organisations must be able to demonstrate, with evidence, that their data practices are thoughtful, proportionate, and rights-respecting. This includes being able to justify data processing decisions and engage transparently with regulators.

DPAs should support and incentivise advanced accountability frameworks, recognising those organisations that go beyond compliance minimums in their privacy programmes.

7. Leveraging Existing GDPR Mechanisms

Finally, the discussion noted that some of the GDPR's existing tools, such as codes of conduct, remain underutilised. These mechanisms could offer valuable sector-specific guidance and foster collective compliance, particularly in sensitive areas like health data. Regulators should take a more active role in initiating and shaping these instruments in cooperation with industry.

Key Recommendations

For Data Protection Authorities (DPAs)

- **Adopt a forward-looking, risk-based interpretation of the GDPR** to enable innovation while safeguarding rights.
- **Clarify key legal provisions** to address uncertainties and ensure consistency across sectors and use cases.
- **Promote constructive regulatory engagement**, including wider use of sandboxes and other innovative regulatory tools.
- **Balance enforcement with encouragement**, using incentives and proportionate responses to support good-faith compliance.
- **Coordinate across sectors and jurisdictions** to ensure consistency, reduce fragmentation, and support cross-border innovation.
- **Codify and operationalise the risk-based approach**, providing clear frameworks for its application.
- **Support and reward accountability**, especially when organisations adopt proactive privacy practices.
- **Activate underused GDPR mechanisms**, such as codes of conduct, to provide practical, context-specific compliance models.

For Organisations

- **Adopt mature accountability frameworks**, with demonstrable and proactive privacy governance that can be leveraged for other compliance areas such as AI.

- **Engage early and openly with regulators**, especially when deploying novel technologies or entering sandboxes.

- **Participate in or help shape codes of conduct** relevant to their sectors.

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.

Endnotes

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data 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.

[2] For more information on CIPL's accountability framework see CIPL paper 'The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society' and 'Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability'. For more information on outcomes based regulatory frameworks see CIPL paper 'Getting the Best Outcomes: Pathways for Data Protection and Privacy Authorities'.

[3] See CIPL paper 'Cisco-CIPL Report on Business Benefits of Investing in Data Privacy Management Programs'.

[4] See CIPL report on 'The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement'.