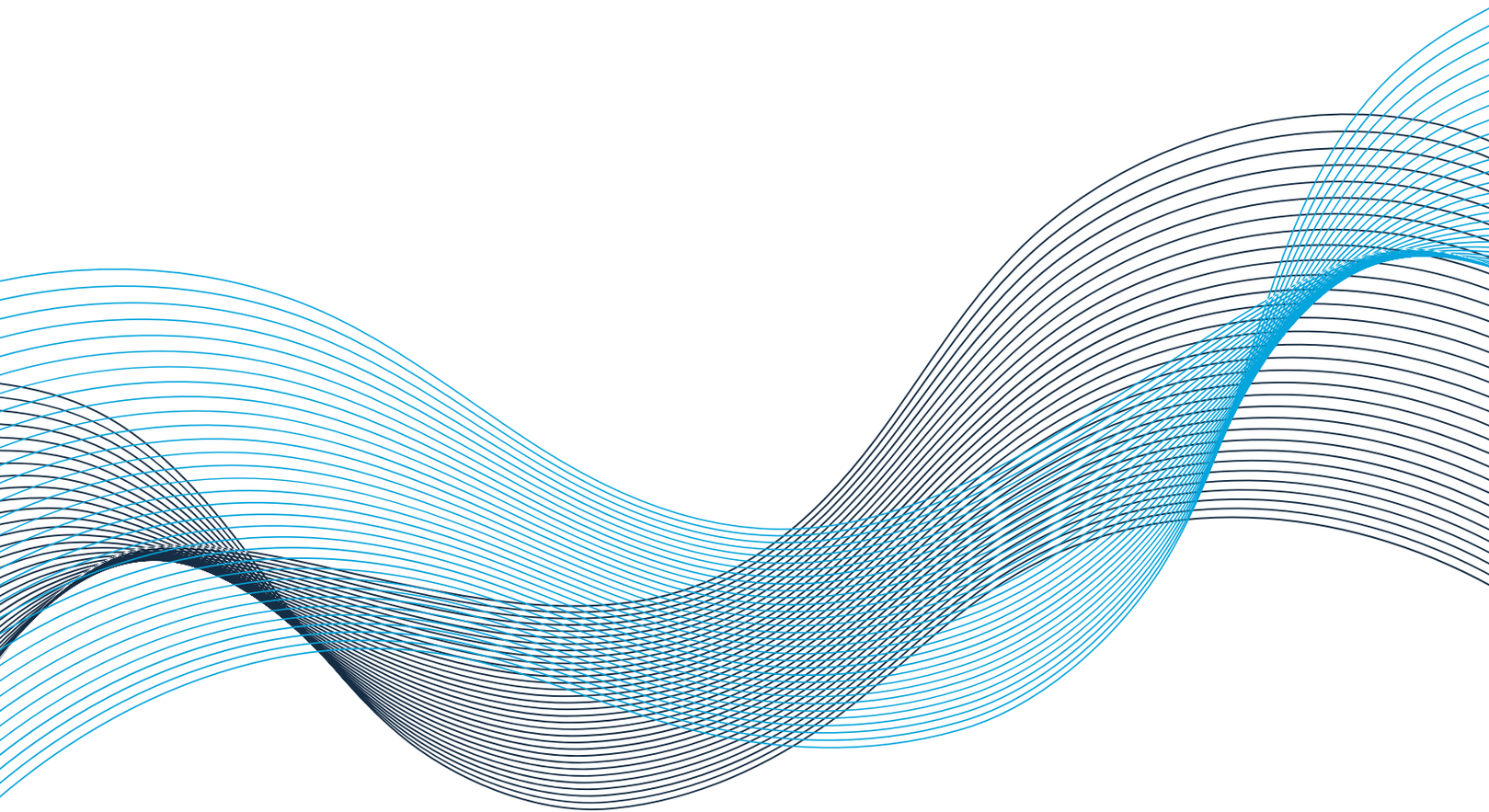
Centre for Information Policy Leadership
HUNTON

# Inaugural CIPL EU AI Act Forum

## Setting the Direction for Implementation

### Event Takeaways

18 November 2024
In Brussels



# Inaugural CIPL EU AI Act Forum: Setting the Direction for Implementation

Brussels, 18 November 2018

EVENT TAKEAWAYS

The Centre for Information Policy Leadership (CIPL) has advocated for and provided thought leadership on organisational accountability in data protection and broader digital and data policy for more than 20 years. Since 2018, CIPL has also been at the forefront of addressing questions of accountability in artificial intelligence (AI) and the intersection of AI and data protection issues.1

The EU AI Act will have a substantial impact on organisations' developing, deploying and putting AI systems on the market in the European Union, and the experiences with its implementation, compliance and enforcement may impact the direction of other emerging regulatory regimes globally. In 2024, CIPL, therefore, launched its EU AI Act Implementation Project focused on key questions raised by the EU AI Act, posing operational and compliance challenges and exploring best practices and risk-based, forward-thinking practical solutions. The project will be a forum for engagement with new and existing regulators and relevant experts from the academic, technology, research and business communities.

On 18 November 2024, CIPL held its Inaugural Forum for this project, which convened key stakeholders to discuss the implementation of the AI Act under Chatham House Rules. Prof. Dr Martin Ebers opened the Forum with a keynote on the risk-based approach in the AI Act and set the stage for the roundtable discussion with leaders in AI and data protection. Below are the thematic observations and insights from the forum.

## Join CIPL's EU AI Act Project

CIPL's EU AI Act Implementation Project is designed to ensure that organisations are not only compliant with the Act, but can excel in the emerging regulatory environment.

Through close engagement with leading experts from academic, the project will address key questions raised by the Act, explore best practices and develop risk-based and forward-thinking practical solutions.

**The project:**

- Advances risk-based, constructive and forward-thinking interpretations of key AI Act obligations;
- Furthers understanding of regulators' priorities and objectives;
- Explores best practices and challenges in implementing key AI Act requirements.

Scan to register your interest

## The Transformative Power of AI Requires Trust

We are witnessing a pivotal moment in technological advancement driven by artificial intelligence. The AI revolution is in its nascent stages, with expectations of significant further developments in multimodal AI, enhanced search capabilities, explainable AI, and autonomous agents capable of performing complex tasks. The challenge lies in integrating accountability, regulation, and digital trust into these rapidly evolving technologies while anticipating future innovations.

While AI presents immense potential benefits in areas such as healthcare, education, and climate change mitigation, it can also pose risks, including concerns around national security, data privacy, accuracy, and discrimination. The critical role of data as the fuel for AI innovation highlights the need for accountable data use practices.

Building digital trust is paramount. This involves fostering an approach that is inclusive of the benefits of AI and data use and engages in a dialogue that explores the responsible use of AI.

Privacy professionals play a crucial role in this conversation, serving as leaders who can bridge technical, legal, and ethical considerations to foster trust and accountability in AI deployment.

## The EU's Position on AI and the Regulatory Approach

The European Union was the first to legislate a comprehensive AI law and is actively striving to enhance its position in the global AI landscape. However, there is a growing concern that a densely regulated tech sector, in combination with lagging investment and a fragmented market, might ultimately have a negative effect on AI development in Europe and the competitiveness of European organisations.2

Considering this context, there is a need to carefully balance innovation with safety and fundamental rights. This involves adopting smart, outcome-based regulation that fosters collaboration between regulators, companies, and other stakeholders and a regulatory approach based on demonstrable risk, taking likelihood and severity into consideration.

## The EU's Risk-Based Approach to AI Regulation

The EU AI Act was developed as a risk-based product safety legislation. The emergence of general-purpose AI models during the legislative process made apparent the challenges for a future-proof legislative framework. To address this, the AI Act includes provisions specific to general-purpose AI.

## A Number of Challenges Remain:

### Regulating Fundamental Rights

- The AI Act's approach may not adequately address the nature of risks to fundamental rights, since those risks are difficult to quantify.

### Lack of Risk-Benefit Analysis

- The Act focuses predominantly on risks without sufficiently considering the benefits of AI, limiting truly informed decision-making.

### Predefined Risk Categories

- The use of predefined, closed risk categories may lead to over-regulation of some AI systems and under-regulation of others, especially as technology continues to evolve.

### Overly Broad AI Definition

- The broad definition of AI in the Act could encompass a wide range of software systems, including those with minimal risks, leading to potential over-regulation.

### Horizontal Approach and Overlaps

- The AI Act's horizontal approach leads to overlaps with existing EU laws like the GDPR, causing inconsistencies and increased compliance burdens.

### Enforcement Challenges

- Reliance on Member States for enforcement may result in fragmented oversight and a lack of coordination among regulatory authorities.

---

## Recommendations for Implementing the AI Act

### Guidelines and Delegated Acts

- The European Commission should issue clear guidelines and utilise delegated and implementing acts to provide specificity and clarity on key aspects of the AI Act.

- Refining the AI definition to distinguish between systems based on their level of autonomy, adaptiveness, and associated risks.

### Harmonised Standards

- Development and adoption of harmonised industry standards can aid in demonstrating compliance and ensure consistency across sectors.

### Consolidation of EU Digital Laws

- Streamlining and consolidating overlapping regulations can reduce complexity, eliminate incoherence, increase legal certainty, and lower compliance costs.

### Risk-Benefit Analysis and Empirical Evidence

- The Commission should conduct thorough risk-benefit analyses and base risk categories on empirical evidence, allowing for adjustments as technology and societal impacts evolve.

To address these challenges and move towards a more risk-based approach application of the EU AI Act, the Forum discussed several considerations.

## Insights from Roundtable Discussions

Experts participating in the Forum highlighted the importance of leveraging lessons from the GDPR and data protection in shaping AI regulation. Below are key insights and best practice recommendations that emerged during the Forum.

### 1. Evolving Organisational Governance - The Current State of Play

- Organisations are developing governance approaches to align their operations with the AI Act, integrating compliance into existing governance frameworks; many organizations have moved beyond a siloed approach to a more integrated strategy that layers AI requirements on top of existing compliance and accountability frameworks like the GDPR.

- The EU AI Act is seen as a product safety regulation, requiring involvement from product experts alongside privacy and legal professionals.

- The question of ownership of AI governance is critical. Some organisations set up separate AI teams with strong executive sponsorship. In some organisations, AI governance is added to the responsibilities of the privacy team or legal teams or may be staffed by the safety or engineering teams.

- A key challenge lies in keeping AI inventories up to date. To address this, organisations are increasingly looking to technology to manage AI effectively. Some, for example, are developing automated systems that integrate with various development and deployment platforms or creating platforms with embedded safeguards to support responsible AI use and creating centralized and automated repositories for AI projects and risk assessments.

- Organisations are continuously adapting and updating their governance frameworks to address new issues and risks, including those raised by generative AI.

## 2. Risk-Based Approach

- A risk-based approach is essential for effective AI governance, ensuring that regulations address both high-risk systems and innovation. Flexibility in implementation is vital to accommodate diverse use cases and industries. Assessing risk must take into consideration the severity and likelihood of the risk, as well as the opportunity costs of not progressing with an AI deployment in light of the societal benefits of the AI application at issue.

- The forum participants emphasized that it is not enough to embed elements of a risk-based approach into the law, but it should also extend to enforcement and regulatory dialogue.

- Regulators should focus on proactive compliance and setting organisations up for success, reserving strict enforcement for edge cases.

- Tools such as practical guidance OR codes of conduct are needed to set out practical guidance for risk assessments and other compliance obligations.

## 3. Regulatory Aspects

- Laws and regulations should facilitate lawful mechanisms for the use of personal data in model training to enable the beneficial development and use of AI.

- There is an ongoing discussion on how to reconcile data protection principles and the practicalities of AI technologies, particularly around the use of personal data for training AI models.

- Lawmakers and regulators should recognise the inherently broad purpose of training a general-purpose genAI model. In this regard, the use of personal data for training of general-purpose AI models should be recognised as a legitimate and permissible purpose, so long as accountability measures are implemented and the legitimate interest balancing test is met.

- There is a need to address issues regarding the classification of AI products and systems, particularly when they do not easily fall into existing categories.

- Laws should enable the processing and retention of sensitive personal data for AI model training to avoid bias or discrimination.

- Regulators should avoid unduly restrictive interpretations regarding the use of personal data in AI model training. It is important to keep in mind that different data privacy rules apply in different phases of the AI lifecycle.

- Organisations should be able to rely on the “legitimate interests” legal basis for processing publicly available data and first-party data for genAI model training, provided that processing meets the legitimate interest balancing test and appropriate mitigations are in place.

- Organisations must consider the regional weight of regulations. Introducing products in the EU sometimes creates longer timelines and launch uncertainties, making it difficult to prioritise Europe.

- The concept of "reasonable expectations" of data subjects is crucial in AI discussions, as those expectations will change over time.

## 4. Collaboration and Harmonisation

- The AI Act's success hinges on refining its implementation to address practical challenges and regulatory overlaps.
- Collaboration and dialogue between regulators, companies, and stakeholders is essential to align AI regulation with technological realities, ensuring innovation thrives alongside the protection of fundamental rights.
- Harmonisation of AI across jurisdictions' regulations remains a priority to ensure innovation is possible across borders. Engagement at the OECD, UN, and G7 levels to ensure a level of interoperability remains of high importance.
- It is important to develop efficient, multilateral cross-border transfer mechanisms (e.g. Global Cross-Border Privacy Rules (CBPR)) to enable access to globally-sourced data that underpins effective AI development and use.

## 5. Emerging Best Practices

### AI Governance

- Organisations should invest in comprehensive, risk-based AI and data privacy programs, continually improving and evolving their controls and best practices. A key challenge lies in balancing the need for detailed compliance with the practicality of implementation across diverse global operations, particularly in countries that have not have laws similar to the AI Act or the GDPR.
- AI governance requires a cross-functional approach involving legal, ethics, HR, and technical expertise, among others.
- Governance is not a one-time implementation but an iterative process.
- Organisations should consider how to build AI governance into the product or platforms to ensure compliance by design rather than relying solely on policy and training.
- Organisations must be transparent about the limitations and risks of AI systems, not just their benefits.
- Risk assessments must be holistic, addressing not only data privacy but also broader issues like fairness, bias, security, and fundamental rights.
- Implementing AI regulations needs to take regional variations and priorities into account and be commensurate with company culture.

### Data Protection

- Accountability is a key concept in both the GDPR and the AI Act, and lessons learned from the GDPR can be applied to AI compliance.
- Data protection principles such as fairness, collection limitation, purpose specification, transparency and accountability are crucial in the responsible development of AI systems.
- Data minimisation should be understood in the context of AI to allow for the collection of appropriate amounts of data for high-quality models and user experience.

- Developers should explore privacy-enhancing technologies (PETs) such as synthetic data and differential privacy to reduce risks associated with the use of personal data.

- Fairness should be interpreted to facilitate personal data processing in genAI model development to train accurate and accessible models that do not unjustly discriminate.

- Data minimisation should be understood as limiting the amount of personal data to what is necessary for a high-quality model, not using less data than required.

- Organisations should implement controls at the output stage to prevent users from creating detailed profiles, retrieving sensitive information, or generating likenesses without consent.

    - Transparency is essential for building trust and credibility in developing and deploying AI technologies.

    - Organisations should be transparent about their AI practices with both internal and external stakeholders.

    - Organisations should provide clear explanations of how and why user-submitted personal data is used to operate applications and whether user data will be used to train the model.

    - The level of transparency should be balanced with the need to protect intellectual property rights, copyright, confidential information, and data security, as well as potential benefits that may outweigh individual rights.

    - Risk assessments should be required to help organisations properly weigh these considerations.

- Transparency should be implemented with a tiered or layered approach that balances the need for disclosure with the protection of intellectual property.

## AI Literacy and Training

- The scope of Article 4 of the EU AI Act extends beyond high-risk AI systems and will, therefore, apply more broadly in the context of AI systems. AI literacy is a strategic imperative for organisations that go beyond mere compliance. It is crucial for fostering a culture of responsible AI development and deployment and is also key to addressing any scepticism and fear surrounding AI in the workforce.

- Continuous investment in AI literacy programs is essential to empower employees, ensure their understanding of the risks and responsibilities associated with AI systems, and give them the necessary competence to address them in their respective areas of responsibility. Organisations should invest in tools and resources so that employees stay updated on AI developments and regulatory changes (where relevant) in the context of AI.

- AI literacy initiatives should be tailored to specific use cases in a department or business unit, combining general training with role-based programs and incorporating diverse learning methods, such as e-learning, in-person workshops, and peer-led circles.

- Companies should consider their broader responsibility in promoting AI literacy among affected persons beyond their workforce.

## Endnotes

1 - Please see, CIPL AI First Report - Artificial Intelligence and Data Protection in Tension, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf;CIPL AI Second Report - Hard Issues and Practical Solutions, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf; CIPL White Paper - Ten Recommendations for Global AI Regulation, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ten_recommendations_global_ai_regulation_oct2023.pdf; CIPL AI Third Report - Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf; CIPL White Paper Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf.

2 - European Commission, “The future of European competitiveness: Report by Mario Draghi”, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en