The AI Act: The EU's Bid to Set the Global Standard for AI Regulation

March 13, 2024

Rosa Barcelo | Romain Perray | Lorraine Maisnier-Boché | Simon Mortier

SUMMARY

In a groundbreaking move, the European Union has launched its bid to set the new comprehensive standard for the regulation of artificial intelligence (AI) with the European Parliament passing the EU AI Act on March 13, 2024. This pioneering legislation, set to come into effect in the coming years, ushers in a new era in AI regulation and stands as a testament to the EU's commitment to ensuring a subtle balance between safe, ethical, and innovative use of AI.

In this article we will first explore the **eleven key aspects of the EU AI Act**, offering an in-depth look at its broad scope and essential requirements, including its interplay with the EU General Data Protection Regulation (GDPR), and how businesses can leverage their existing GDPR compliance programs to meet the EU AI Act's requirements.

We will then dive into **five key takeaways** focusing on the key points and actionable steps you can take to navigate the evolving landscape of AI regulation and the EU AI Act in particular.

IN DEPTH

Eleven Key Aspects of the EU AI Act

The EU AI Act introduces several pivotal provisions that will significantly impact the regulatory framework of AI. Most significantly these include:

1. **Broad Scope and Specific Exclusions**: The EU AI Act is intended as a horizontal regulation and provides a comprehensive definition of AI systems, applicable to a wide array of applications in sectors such as healthcare, finance, public administration, and consumer technologies. Drawing from the OECD's definition, the Act describes an AI system as "*a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*". As inclusive as the GDPR in order to ensure the highest level of protection possible, this definition aims to encompass the diversity in AI systems' levels of autonomy and adaptability after their initial deployment.

At the same time, the Act makes it clear that it does not apply to areas outside the scope of EU law, including national security and defense, and excludes AI models and systems used solely for research, innovation, or for non-professional purposes.

2. **Extraterritorial Effect**: The AI Act will apply not only within the EU but also to entities outside its borders. This includes non-EU providers placing AI systems or models on the EU market, those putting AI systems into service within the EU, and cases where the output of an AI system located outside the EU is used within its borders. In this respect, the AI Act aligns with both GDPR and the other acts included in the new EU digital package that it belongs to, although with quite a special angle notably as the only one directly governing technologies in contrast with the others which merely focus on data usage.

3. **Risk-Based Approach**: The Act employs a structured, risk-based approach to AI regulation, organizing AI systems into four categories based on their potential risk levels: Prohibited AI, High-Risk AI, Limited Risk AI, and Minimal Risk AI. This system ensures that stricter regulatory measures are applied to AI applications with higher potential risks, particularly those used in critical areas such as healthcare or infrastructure. Conversely, AI systems with minimal risk are subject to less rigorous requirements. This tiered model is designed to balance the necessity of safeguarding user safety and privacy rights with the goal of fostering innovation in lower-risk AI technologies.

4. **Prohibited AI and Law Enforcement Exemptions**: The EU AI Act sets clear boundaries by prohibiting certain AI applications that pose risks to privacy, ethics, and fundamental rights. Again following the GDPR quite closely these include:

- **Subliminal Techniques**: The use of manipulative or deceptive techniques that significantly distort behavior and impair informed decision-making.
- **Exploiting Vulnerabilities**: AI systems that exploit vulnerabilities related to age, disability, or socio-economic circumstances.
- **Biometric Categorization**: Systems inferring sensitive attributes from biometric data, such as racial or ethnic origin, political opinions, religious beliefs, or sexual orientation.
- **Social Scoring**: Evaluation or classification of individuals based on social behavior or personal characteristics, leading to detrimental treatment of individuals.
- **Predictive Policing**: Assessing the risk of an individual committing criminal offenses based solely on profiling or personality traits.
- **Facial Recognition Databases**: Compiling databases through untargeted scraping of facial images from the internet or CCTV footage.
- **Emotion Inference**: Inferring emotions in workplaces or educational institutions, except for AI systems used for medical or safety reasons.

In the context of law enforcement, the Act generally restricts the use of real-time biometric identification in public spaces, allowing it only under limited, pre-authorized circumstances.

5. **High-Risk AI Systems and Key Requirements**: The EU AI Act identifies high-risk AI systems as those critical to sectors such as healthcare, transportation, HR management, education, essential public services, and systems influencing democratic processes. It categorizes these into two main groups:

- **Annex II Systems**: AI systems acting as safety components of products or as standalone products, which are subject to EU laws already requiring a conformity assessment. These are typically associated with high-risk and regulated products (medical devices, machinery, protective equipment, etc.).
- **Annex III Systems**: AI systems designed for specific purposes such as biometrics (excluding banned types), critical infrastructure, educational and vocational training tools, employment and workers' management systems, essential services access (including credit scoring and insurance pricing), law enforcement, migration and border control, and the administration of justice and democratic processes.

The Act mandates comprehensive obligations for providers and deployers of these systems, covering governance measures and technical interventions necessary from the design stage through the entire lifecycle. This includes ensuring CE marking, transparency, accountability, technical documentation, data governance, human oversight, and maintaining accuracy, robustness, and cybersecurity. Providers of these systems will have to report serious incidents to market surveillance authorities.

Despite recent efforts to refine the scope and introduce exemptions for certain AI systems, ambiguities in classification remain. To address this, companies are advised to maintain high governance standards for all AI systems in use. The EU Commission will provide further classification guidelines within 18 months of the Act's entry into force, aiming for clarity and consistency in high-risk AI system regulation.

Interestingly, the AI Act also allows, where strictly necessary and under additional conditions, the processing of special categories of personal data, such as ethnicity, for the purpose of ensuring bias detection and correction in relation to high-risk AI systems. As feeding such systems, this processing will also remain subject to the GDPR, under which it will be allowed for purposes of substantial public interest within the meaning of Article 9(2)(g).

6. **Limited/Minimal Risk AI**: Under the EU AI Act, AI systems categorized at the lower risk level are subject to specific transparency and identification requirements. This primarily targets AI technologies that engage directly with users, mandating that any synthetic content produced—be it audio, visual, or textual—must be clearly labeled in a way that machines can recognize as artificially created or altered. Providers are responsible for the efficacy, compatibility, and dependability of these labeling mechanisms. Additionally, the Act imposes obligations on AI functionalities like emotion detection, biometric sorting, AI-generated content, deep fakes, or the alteration of

significant textual content to ensure they are transparently marked and made detectable to uphold transparency and prevent misinformation. Regarding Generative AI applications specifically, individuals must be clearly informed when they are interacting with such as chatbots and content generation tools. For AI systems deemed to pose minimal risk, the Act envisages the adoption of voluntary best practices through future codes of conduct.

7. **General Purpose AI**: The EU AI Act introduces specific requirements for General Purpose AI (GPAI) Models, generally known as Foundation Models, which are defined as those "*capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications*". GPAI was not expressly considered in the initial draft AI Act, while the risk-based approach based on the AI intended purposes and applications created the risk of leaving underlying foundation models uncovered. GPAI became a bone of contention, discussed until the last stages of negotiation of the Act, because of the specific risks it presents for users' fundamental rights and safety. The Act thus focuses on GPAI transparency and accountability. All GPAI models, such as those used for broad applications, are required to provide extensive technical documentation, summaries of training data, and adhere to copyright and intellectual property safeguards. Models released under open-source license are considered as already insuring high levels of transparency and benefit from exemptions. For high-impact GPAI models, i.e., that pose systemic risks, the Act mandates additional stringent requirements, including thorough model evaluations, comprehensive risk assessments, adversarial testing, and incident reporting.

8. **Innovation-Friendly Ecosystem**: To nurture innovation, the Act introduces measures such as regulatory sandboxes and provisions for real-world testing. These initiatives intend to benefit SMEs and startups, offering them the flexibility to experiment and refine their AI systems within a controlled environment before wider deployment. This approach recognizes the dynamic nature of AI development and seeks to provide a supportive ecosystem for emerging AI innovations.

9. **The interplay between the EU AI Act and the GDPR**: AI systems that process personal data will be subject to both the GDPR and the EU AI Act (and respective fines in case of violations). Both acts lay down some requirements that have strong commonalities. A key question is whether it is possible to leverage compliance efforts, and if so, how. For instance, under the GDPR, data controllers are required to carry out a data protection impact assessment (DPIA) in certain circumstances, whereas under the EU AI Act, providers/users of high-risk AI systems have to carry out DPIAs, which, among others, need to consider privacy risks. In line with the effective explainability and transparency principles – which are the cornerstones of trustworthy AI systems – the EU AI Act imposes requirements to inform individuals when they interact with AI systems (e.g., chatbots and content generation tools).

10. **Penalties and Enforcement**: The EU AI Act establishes a comprehensive framework for penalties and enforcement. Fines for violations are scaled, with up to 7% of global annual turnover or EUR 35 million for prohibited AI violations, up to 3% for other breaches, and up to 1.5% or EUR 7.5 million for supplying incorrect

information, including specific caps for SMEs and startups. Enforcement will be coordinated through a newly established central 'AI Office' and 'AI Board' at the EU level, complemented by market surveillance authorities in each EU country, ensuring a balanced and effective application of the Act across all member states.

11. **Entry into force**: The AI Act will start applying gradually: prohibited AI will be banned six months from the Act entering into force, while the Act will start applying to GPAI one year after entry into force; two years for high-risk AI systems of Annex III and three years for high-risk AI systems already covered by other EU regulations mandating a third-party conformity assessment.

Five Takeaways on the EU AI Act

The above compilation of key aspects is intended to serve as a useful starting point to inform proactive steps legal and compliance managers as well as DPOs can take to position their companies and their teams for success. Below, we are sharing five key takeaways for businesses to prepare for the rapidly evolving risks and challenges posed by AI:

1. **Comprehensive Impact Assessment and Compliance Evaluation**: Businesses should conduct a thorough assessment to understand how the AI Act will affect their operations. This evaluation should cover not just mapping and identifying high-risk AI systems but also the wider range of entities involved in AI deployment, distribution, or usage. It's important to review existing governance frameworks to ensure they align with the Act's requirements. Additionally, organizations should proactively examine how the AI Act might impact their daily operations and specifically, systems already covered by other EU mandatory conformity assessments (medical devices, machinery, protective equipment, etc). This requires gaining a comprehensive understanding of the legal, technological, and ethical aspects of AI to facilitate responsible integration and usage within the organization.

2. **Developing a Robust AI Governance Program**: It's essential for organizations to develop an AI governance program that integrates the AI Act's requirements with broader business strategies and objectives. This program should cover risk management, privacy, ethics, data governance, intellectual property, safety, and security, among others, and adapt existing policies and procedures to meet the new standards. Any types of organizations, more specifically businesses in tech- and data-driven industries, should assess how to leverage their existing GDPR compliance programs to also meet most, if not all, of the AI Act's requirements. The role of the board in overseeing AI use within the organization is also a critical consideration.

3. **Global Coordination and Voluntary Initiatives**: Businesses, above all, should pay close attention to international efforts to harmonize AI regulations, including the EU's collaborations with global bodies and initiatives. In this regard, the EU Commission has initiated an 'AI Pact', encouraging organizations to anticipate the AI Act by voluntarily sharing their internal guidelines, processes and concrete actions carried out to address the AI Act

requirements, and by testing their solutions within the community. Participating in such voluntary commitments to implement the AI Act's requirements ahead of deadlines can position organizations as leaders in ethical AI use and governance.

4. **Proactive Adaptation and Compliance Strategy**: With the regulatory landscape rapidly evolving, businesses need to be agile, ready to update their AI strategies and compliance programs as new guidelines and requirements emerge. Starting early on this adaptation process will help mitigate risks and liabilities and ensure compliance. Keeping an eye on regulatory developments in the EU (including the AI Act delegated / implementing acts and guidance), the UK, the US, and other regions further along in AI regulation is vital for a comprehensive compliance effort.

5. **Engagement and Transparency**: Collaboration with regulators, transparent communication, and fostering global harmonization are critical for successful AI governance. Businesses should also consider public engagement and transparency in their AI operations as part of their compliance and risk management strategies. This includes clear communication about AI's role and impact within the organization and ensuring that AI technologies are deployed in a way that is ethical, responsible, and aligned with societal values. On a more operational standpoint, it would also make a lot of sense to combine as much as possible information to individuals respectively required under GDPR and the EU AI Act.

GET IN TOUCH

Rosa Barcelo
View Profile

Romain Perray
View Profile

Lorraine Maisnier-Boché
View Profile

Simon Mortier
View Profile

This may be considered attorney advertising. Prior results do not guarantee a similar outcome.