KPMG

EU Artificial Intelligence Act

Ten essential EU AI Act questions businesses need to know

kpmg.ie

EU Artificial Intelligence Act

The world has seen a paradigm shift in the speed in the development of Artificial Intelligence (AI) over the past eighteen months. While these tools and capabilities provide significant opportunity to completely revolutionise businesses and their products and services, there is also a fear of the unknown and potential consequences this technology brings.

A critical component on managing the potential risks associated with AI is appropriate regulation. The European Union (EU) is taking a proactive approach to governing AI technologies to ensure they align with fundamental rights, privacy, and safety standards.

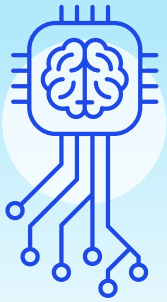
On the evening of Friday 8 December, following what has been described as 'marathon' talks, the Council presidency and the European Parliament's negotiators reached a provisional agreement on the proposal on harmonised rules on AI. In January 2024, an unofficial updated EU AI Act draft text was issued which outlines further the proposed legislation. Until now, there has been strong disagreement between the EU's legislative bodies on what the Artificial Intelligence Act **("EU AI Act")** should look like. If formally passed into law, the highly anticipated EU AI Act will set a global standard in the regulation of AI, a model on the basis of which other jurisdictions may seek to mould their own national rules. While the legislation still needs to be formally passed by each legislative body, businesses that operate in Europe now have a much clearer picture of what their compliance obligations will be once the EU AI Act enters into force. It is expected that the EU AI Act will be formally passed into law in early 2024. This paper answers the 10 essential EU Act questions business need to know.

1 What is the EU AI Act?

The EU AI Act is a proposed regulation by the EU to establish uniform rules for using AI. It aims to ensure that AI systems deployed in the EU are safe, respect fundamental rights and EU values, and encourage the development of a single market for AI applications. The Act follows a risk-based approach requiring AI systems to be classified and assessed based on risk level and imposing corresponding requirements.

What defines AI?

An AI system is 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 content, predictions, recommendations, or decisions that can influence physical or virtual environments.



2 Who should take note of the EU AI Act?

- **AI system providers:** Organisations and individuals who develop or create AI systems, including software developers and technology firms.
- **AI system deployers:** Organisations who deploy and use AI systems in their operations, irrespective of the sector or industry.
- **Public authorities:** Government bodies and agencies that deploy AI systems for public services, law enforcement or administrative purposes.
- **Regulators and supervisory bodies:** Authorities responsible for monitoring and ensuring compliance with the AI Act, including data protection agencies.
- **Consumers and the general public:** Indirectly affected, as the Act aims to safeguard their rights and safety in relation to AI use.
- **Global impact:** This new law will apply to non-EU organisations offering AI services in the EU market or to EU citizens, reinforcing global standards.

3 What significant impact will the EU AI Act have on organisations?

Organisations will need to reinforce certain activities or create new functions to comply with this upcoming regulation. Below are the most impactful expected changes:

- **Compliance with risk-based regulations:** Adhering to the varying levels of regulations based on the risk classification of AI systems.
- **Ensuring data governance:** Managing data sources and AI systems consistently across the organisation.
- **Respecting privacy and fundamental rights of individuals:** Ensuring AI systems have clearly defined purposes and adequate safeguards in place to protect the rights and freedoms of individuals. High-risk AI systems require a fundamental rights impact assessment before deployment.
- **Maintaining transparency:** Ensuring AI systems are designed in a way that makes them understandable and their decisions should be explainable.
- **Balancing innovation with ethical considerations:** Innovating while respecting ethical guidelines, avoiding bias and ensuring fairness.
- **Maintaining a risk management system:** Assessing and managing risks associated with AI deployments, including potential biases and ethical concerns.
- **Keeping up with rapid technological changes:** Staying updated on the latest AI developments and regulatory changes.

4 What constitutes a high-risk AI system?

- High-risk AI systems are those that pose significant risks to health, safety or fundamental rights and freedoms.
- They include AI systems used in **critical infrastructures, education, employment, essential private and public services, law enforcement, migration and administration of justice**.
- High-risk AI systems require strict compliance with mandatory requirements before being placed on the market or put into service.

5 What are the requirements for AI systems classified as high-risk?

- **Adequate risk assessment and mitigation:** Providers must conduct thorough risk assessments including fundamental rights impact assessments and implement adequate risk mitigation measures.
- **High data quality standards:** Ensuring the accuracy, reliability and relevance of data used by the AI systems.
- **Detailed documentation and record-keeping:** Maintaining extensive documentation about the AI system's development, capabilities and compliance.
- **Transparency and provision of information:** Providing clear information about the AI system's capabilities, limitations and intended use.

6 What are the requirements for AI systems classified as having limited or minimal risk?

Any AI systems that are not prohibited including those not classified as high-risk have requirements too.

- **Basic compliance with safety and rights:** Ensuring the AI system does not pose a risk to safety or fundamental rights.
- **Transparency obligations:** Users should be informed when they are interacting with an AI system, particularly in cases of content generation or manipulation.
- **Data governance:** Ensuring proper handling and protection of data used by the AI system.

7 Which AI systems fall under the classification of having unacceptable risk?

- **Practices contradicting union values:** AI systems that deploy subliminal techniques or exploit vulnerabilities of specific groups to materially distort a person's behaviour in a manner causing physical or psychological harm.
- **Social scoring by public authorities:** Systems that enable social scoring by public authorities, leading to discrimination or unfavourable treatment.
- **Real-time biometric identification:** Use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, with certain exceptions.

8 How should companies organisations prepare in the short-term?

As the agreed text awaits formal adoption by both Parliament and Council to become EU law, organisations can proactively begin preparing for compliance with the EU AI Act. Here's a list of the most significant changes that can be initiated in advance:

- **Inventory and classify current AI landscape:** Review existing AI systems and use cases and categorize them to identify high-risk systems that require compliance to the EU AI Act. Leveraging an automated detection / identification solution, automating intake questionnaires or implementing a workflow platform, for instance, can aid in accelerating the discovery, inventory and classification activities required to support and map compliance obligations.
- **Implement (or improve) AI governance framework:** Implement standards and best practices for AI system development, deployment and maintenance in alignment with the EU AI Act's requirements, other emerging regulatory standards and ensure scalability. Here again, leveraging an automated solution to manage various aspects of compliance mapping, obligations tracking, and workflow management can aid in supporting and scaling various governance activities.

- **Conduct gap analysis:** Conduct a thorough gap analysis to identify areas of non-compliance and develop an immediate action plan to address these gaps. This analysis could be expedited using an automated or rapid AI assessment approach against established governance framework or EU AI Act compliance obligations.
- **Automate system management and evaluation:** Optimize, automate and streamline AI system management processes, ensuring models are transparent, explainable and trustworthy. Leverage automation to extract and map technical metrics and data from AI system and application metadata to your governance framework, enabling automated compliance and management processes.
- **Prioritize and manage AI risks adequately:** Understand the risks that AI systems pose internally to your organisation and externally to your stakeholders and ecosystem. Review and, if necessary, update data handling practices to ensure they comply with applicable laws, regulations, and industry good practice, in particular GDPR and other data privacy aspects of the EU AI Act. Leveraging automated threat detection, analysis and intelligence solutions can drastically reduce level of effort required to support testing and technical documentation requirements outlined in the EU AI Act.
- **Documentation and record-keeping:** Establish documentation repository and management system to ensure appropriate documentation processes are in place to ensure AI systems are well-documented and in compliance with the EU AI Act.
- **Train employees on AI ethics and compliance:** Educate your workforce on the legal and ethical implications of AI applications, ensuring they are prepared to handle new responsibilities and compliance tasks.
- **Stakeholder communication:** Communicate with all stakeholders, including customers and partners, about how your company is addressing the EU AI Act requirements as well as outline expectations and requirements for each stakeholder group in managing ongoing compliance.

9 What are mid- to long-term strategies business need to adopt?

- **Strategic alignment with regulatory changes:** In the medium term, align business strategies with the evolving regulatory landscape of AI, anticipating future amendments to the EU AI Act.
- **Long-term investment in AI ethics and governance:** Establish a dedicated team or department for AI ethics and governance to continuously monitor and guide AI practices in line with regulatory requirements.
- **Ongoing AI literacy and training programs:** Develop long-term training programs to enhance AI literacy across the organisation, fostering a culture of ethical AI use and compliance.
- **Sustainable data management practices:** Implement and maintain robust data governance frameworks that ensure long-term data quality, security and privacy — adapting to future technological and regulatory changes.
- **Regular AI system audits and updates:** Conduct periodic reviews and updates of AI systems to ensure ongoing compliance and to integrate advancements in AI transparency and explainability.
- **Active engagement in policy discussions:** In the long term, participate in industry discussions and policy-making processes related to AI regulation to influence and stay ahead of future regulatory trends.
- **Innovation within ethical boundaries:** Foster an environment of innovation that respects ethical boundaries and regulatory requirements, balancing technological advancement with social responsibility.
- **Building consumer trust through transparency:** Prioritize transparency in AI operations to build and maintain public trust, ensuring long-term viability and acceptance of AI solutions.
- **Trusted AI and Security by design:** Adapt the building of AI systems to include Trusted AI and AI Security in the design phase.

These mid- and long-term considerations are critical for ensuring that organisations not only comply with current regulations but are also well-prepared for future developments in the AI regulatory landscape.

10 Which senior roles are most affected?

- **Chief Executive Officer (CEO):** Responsible for overall compliance and steering the company's strategic response to the EU AI Act.
- **Chief Technology Officer (CTO) or Chief Information Officer (CIO):** Oversee the development and deployment of AI technologies, ensuring they align with regulatory requirements.
- **Chief Data Officer (CDO):** Manage data governance, quality and ethical use of data in AI systems.
- **Chief Compliance Officer (CCO) or Legal Counsel:** Ensure that AI applications and business practices adhere to the EU AI Act and other relevant laws.
- **Chief Financial Officer (CFO):** Oversee financial implications, investment in compliance infrastructure and potential risks associated with non-compliance.
- **Human Resources Manager:** Address the impact of AI systems on employee management and training, ensuring AI literacy among staff.
- **Chief Information Security Officer (CISO):** Handle cybersecurity and data protection aspects of AI systems to ensure data integrity and prevent any unauthorized use.
- **Chief Privacy Officer (CPO) or Data Protection Officer (DPO):** Ensure that AI systems adhere to the privacy principles, are explainable and transparent, and have safeguards in place to preserve the fundamental rights and freedoms of individuals.

These roles play a crucial part in adjusting business operations, refining technology strategies and aligning organisational policies to comply with the EU AI Act. While some organisations have already appointed a Chief AI Officer, we foresee the emergence of a new senior role: the Chief AI Risk Officer.

What next?

As cited above, the EU AI Act will likely be passed into law early in 2024, however businesses will have some time to prepare before it begins to apply. Nevertheless, with respect to transactions happening today involving businesses that use AI, scrutiny should be cast over any target companies which could use unacceptable or high-risk AI, including ensuring a consideration of how that AI can be made compliant with the EU AI Act (and what impact that may have on the business and its operational performance). Preparing an AI road map and running an AI compliance review (as outlined in pt. 8 above) today will also hold businesses in good stead for when the EU AI Act comes into force.

Footnote: Please note that the EU AI Act's final text is not yet available and could be subject to change. This analysis is based on the 2021 draft proposal, updated in subsequent years and supplemented by the agreement reached on December 8th, 2023.

Get in touch

If you have any queries about meeting required AI regulation, please contact our Consulting team below. We'd be delighted to hear from you.

Gillian Kelly
Partner – Head of Consulting
KPMG in Ireland

t: +353 1 410 1120
e: gillian.kelly@kpmg.ie

Sean Redmond
Director – Risk Consulting
KPMG in Ireland

t: +353 87 050 4838
e: sean.redmond@kpmg.ie

Dani Michaux
Partner – Cyber Security
KPMG in Ireland

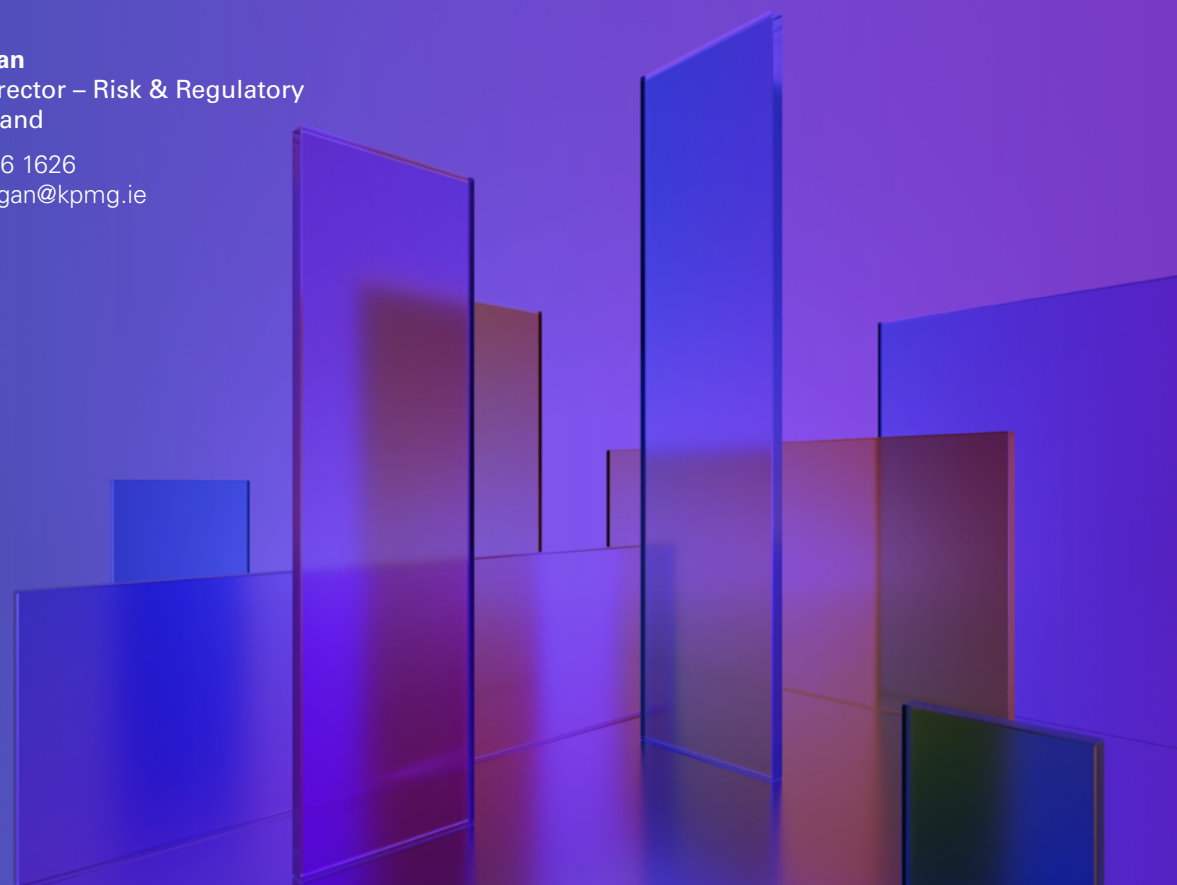
t: +353 1 700 4769
e: dani.michaux@kpmg.ie

Jackie Hennessy
Partner – Technology
KPMG in Ireland

t: +353 1 700 4171
e: jackie.hennessy@kpmg.ie

Emma Coogan
Associate Director – Risk & Regulatory
KPMG in Ireland

t: +353 87 216 1626
e: emma.coogan@kpmg.ie



kpmg.ie

Produced by: KPMG's Creative Services. **Publication Date:** January 2023. (10036)