Decoding the EU AI Act

What the new Act means—and how you can respond

How will the European Union's Artificial Intelligence (AI) Act impact your business?

Generative AI is a game-changing technology that is already delivering new value streams and transforming business models. But in The KPMG 2023 Generative AI Survey, business leaders cited concerns about the regulatory landscape as the top barrier to AI adoption at their organizations. That makes understanding the European Union's recently proposed Artificial Intelligence (AI) Act important for more than just compliance reasons—it's essential for businesses to continue innovating and remaining competitive in their industries today.

Concerns about the regulatory landscape are the #1 barrier to AI adoption

2023 KPMG Generative AI Survey Report

The proposed EU AI Act will reshape the market landscape for AI, just as the EU's General Data Protection Regulation (GDPR) did for data privacy in the last decade.

Though it won't be ratified until early 2024, the EU AI Act will instantly have wide-ranging impacts on any business that operates in the EU and offers AI products, services, or systems that can be used within the EU. The Act provides a robust regulatory framework for AI applications to ensure user and provider compliance. It also defines AI and categorizes AI systems by risk level while outlining requirements for safe and responsible use.

In this guide, we'll break down what the Act covers and the important definitions, provisions, and protections it establishes. Then we'll explore what your business can do now to proactively prepare, and how you can use the KPMG Trusted AI framework to help ensure responsible AI deployment and compliance.

01 What happened

02 What's in the Act

03 What's coming next

04 What you can do now

01 What happened

The European Commission proposed the Artificial Intelligence (AI) Act in April 2021. As of December 2023, the European Parliament has reached a provisional agreement to make the Act law.

In the same way the GDPR is enforced, the European Commission understands that foreign entities selling on the European markets must be regulated in a similar fashion to the member states. Just as GDPR shaped global data privacy regulation, the AI Act is poised to set a new standard for AI regulation worldwide.

Who will be affected?

Applicable parties for this regulation include:

- Any provider placing an AI product or service within the EU
- Users of the AI products and services within the EU
- Any provider or user of an AI system where the output produced by the system can or is intended to be used within the EU

The regulation does not apply to:

- AI systems developed or used exclusively for military purposes
- AI systems used by public authorities or international organizations in non-Union countries when used for law enforcement or judicial cooperation with the EU under a framework of international agreement

Which senior roles will be most affected?

Executives who manage compliance, data governance, and the development and deployment of AI technologies will see their roles and responsibilities impacted by the EU AI Act.

Chief executive officer (CEO) ↔ **Chief technology officer (CTO)** ↔ **Chief information officer (CIO)** ↔ **Chief data officer (CDO)** ↔ **Chief ethics and compliance officer (CECO)** ↔ **Chief financial officer (CFO)** ↔ **Chief AI officer (CAO)** ↔ **Chief information security officer (CISO)** ↔ **Chief risk officer (CRO)**

02

What's in the Act

The draft EU AI Act is a complex 108-page document with multiple subsections. Some of the more important provisions in the Act include:

1. Defining artificial intelligence
2. Proposing consumer protections for the users of AI products
3. Creating an AI risk framework that includes requirements for high-risk systems
4. Establishing transparency rules for AI systems

1. How the EU defines AI

The European Commission's proposed Harmonized Rules on Artificial Intelligence (the EU AI Act) defines artificial intelligence as:

- Machine learning approaches, including supervised, unsupervised, and reinforcement learning, using a wide variety of methods including deep learning
- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, and expert systems
- Statistical approaches, Bayesian estimation, and search and optimization methods

2. Consumer protections

The EU AI Act proposes product safety regulations in the same vein as the US Food and Drug Administration (FDA) issued Food Code, which contains recommendations on the safe handling and storage of food for American consumers. Similarly, the regulation ensures that EU citizens are safe from intentional or unintentional harm caused by AI products and services.

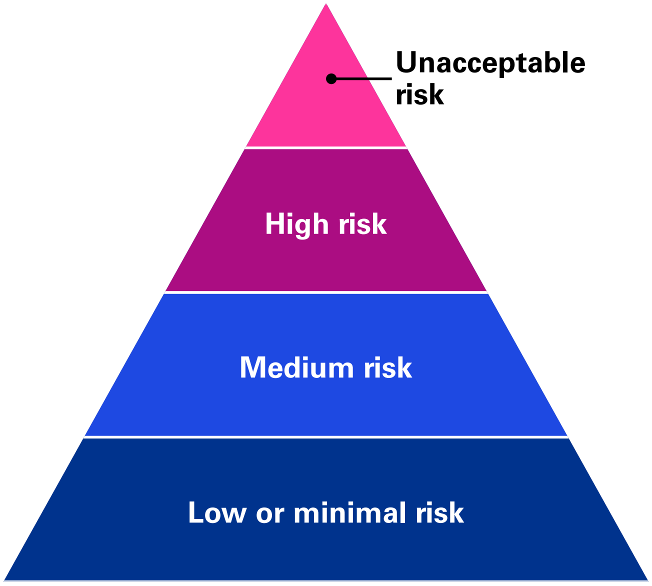
> “
>
> **For the purpose of this Regulation, the following definitions apply:**
>
> **‘artificial intelligence system’ (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.”[1]**
>
> European Commission AI Act, 2023, Article 3

[1] Earlier definitions were aimed at the approaches used to develop the system, but will likely not be included in the final version of AI Act.

3. AI risk levels and requirements

The EU AI Act creates a framework for understanding the risk associated with AI.

AI products and services will fall into one of four risk categories depending on the data that they capture and the decisions or actions that are made with that data.



Unacceptable risk

Prohibited

AI systems that are deemed to have unacceptable risk violate the fundamental rights of the consumer and are prohibited.

Examples include:

- *Social scoring*
- *Manipulation through subliminal techniques*
- *Exploitative practices*
- *Real-time biometric identification systems*

High risk

Permitted but subject to AI compliance requirements

High-risk AI systems create an elevated risk to the health and safety or rights of the consumer. Such systems are permitted on the EU market subject to compliance with certain mandatory requirements and a conformity assessment. There are two categories of high-risk systems:

- AI systems used as safety components of products that are subject to conformity assessments
- Stand-alone AI systems with listed fundamental rights implications

Examples of high-risk systems include:

- *Biometric identification and classification*
- *Management and operation of critical infrastructure*
- *Educational institution selections*
- *Employment selections (recruiting)*
- *Government benefits and immigration status*
- *Law enforcement and judicial processes*

All high-risk AI systems must comply with requirements regarding:

✓ **Risk management systems**

✓ **Data governance**

✓ **Technical documentation**

✓ **Recordkeeping**

✓ **Transparency**

✓ **Human oversight**

✓ **Accuracy, robustness, and cybersecurity**

Medium risk

Permitted but subject to AI transparency requirements

AI systems that require transparency requirements are not mutually exclusive with either high- or low-risk AI systems.

The four transparency requirements are:

1. *AI systems that aim to interact with people must be designed and developed in a way that makes it obvious that it is an AI system.*
2. *Users of an emotion recognition system or a biometric categorization system must inform anyone they plan to use it on.*
3. *Deepfake content must always be disclosed.*
4. *Requirements 1, 2, and 3 do not impact the requirements defined for high-risk systems.*

Low or Minimal risk

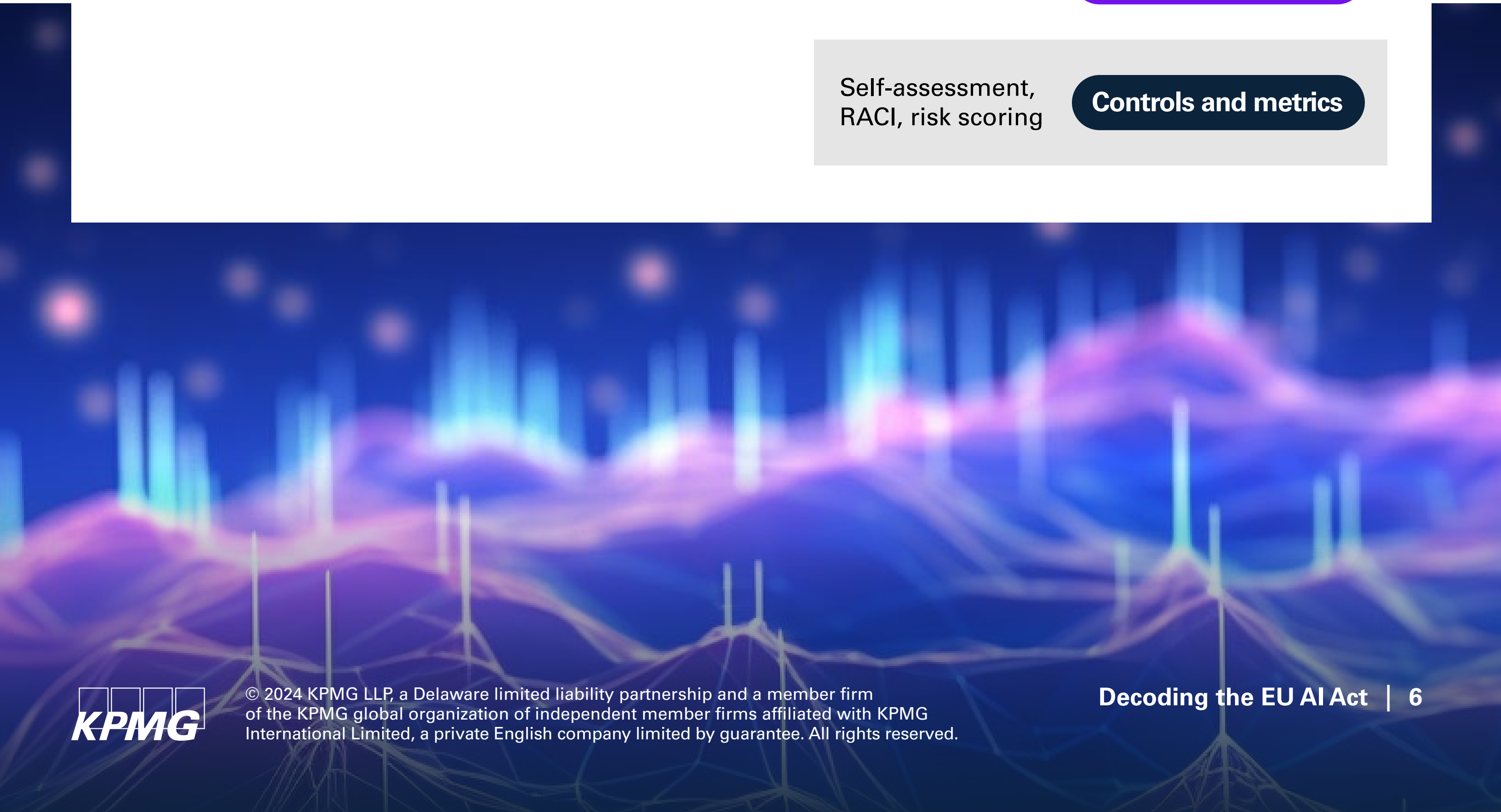
Permitted without restriction

Though low-risk systems are permitted without restriction, organizations should continue to monitor their AI systems periodically for changes and enhancements particularly when adding functionality aimed to interact with human emotions or characteristics through automated means.

4. Trusted AI governance

Implementing an AI risk management system is not a one-size-fits-all exercise. Existing models or frameworks that were built for traditional risks might not—and probably do not—apply to all the generative AI risks facing your organization. Everything up to and including principles and policies may need to be updated, and appropriate governance support will be required.

Core guiding AI principles	**AI principles**
Policies governing AI principles	**Policy**
Representative standards defined based on frameworks such as NIST, OECD, SR11-7, ISO (42001), and ENISA	**Standards**
AI Best Practices Guide	**Process**
Self-assessment, RACI, risk scoring	**Controls and metrics**



03

What's coming next

The EU AI Act is expected to be finalized in 2024. Afterwards, organizations will have a 24-month transition before it becomes fully enforced.

In the meantime, the European Commission will continue to hammer out the means of governance and enforcement while refining its approach to balancing innovation with consumer safety.

April 2021

The Commission submitted proposal for regulation of artificial intelligence.

June 2023

European lawmakers agreed on stricter amendments.

Dec. 2023

The Council presidency and European Parliament reached a provisional agreement to finalize the proposed rules.

1st semester 2024

The Act is expected to be ratified prior to the 2024 European Parliament elections.

2025 and beyond

Enactment will be followed by a 24-month transition period. Prohibitions will apply after 6 months; rules on General Purpose AI will apply after 12 months; and the Act will be fully enforceable at the end of the transition period.

Establishing governing bodies

The European Commission has proposed a structure for the enforcement of AI provider requirements with the establishment of an Artificial Intelligence Board and Expert Group. Both parties sit at the EU level and are responsible for:

- Contributing to effective collaboration with national supervisory authorities
- Providing recommendations for best practices
- Ensuring consistent application of the regulation

> "This is a historical achievement and a huge milestone towards the future! Today's agreement effectively addresses a global challenge in a fast-evolving technological environment on a key area for the future of our societies and economies. And in this endeavor, we managed to keep an extremely delicate balance: boosting innovation and uptake of artificial intelligence across Europe whilst fully respecting the fundamental rights of our citizens."[2]
>
> **Carme Artigas**
> Spanish secretary of state for
> digitalization and artificial intelligence

Each member state will be expected to create a National Component Authority that will ensure the implementation of the regulation and safeguard the objectivity and impartiality of their activities.

The chair of the Special Committee on Artificial Intelligence in the Digital Age (AIDA) has stated that the Committee, as well as members of the Commission, would prefer to revise this section to allow for the EU to govern the implementation of the proposed regulation without the need for national competent authorities. Their belief is that having to comply with authorities in each member state may cause issues during go-to-market and stifle smaller or younger companies.

[2] Source: Council of the EU, "Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world" (December 2023).

04 What you can do now

Many aspects of the EU AI Act will be challenging for organizations to implement and address, especially in terms of technical documentation for the testing, transparency, and explanation of AI applications.

Adding to this challenge is that every AI application comes with its own business processes, impact, and risks. Though there is no silver bullet for compliance, every business can kick-start its journey to EU AI Act compliance by taking these immediate steps:

1. **Inventory and classify the current AI landscape:** Review existing AI applications and categorize them to identify high-risk applications that require compliance with 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.

2. **Implement (or reimagine) the AI strategy & governance framework:** Implement standards and best practices for AI model development, deployment, and maintenance in alignment with the EU AI Act's requirements and other emerging regulatory standards, and ensure scalability. 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.

3. **Conduct a gap analysis:** Conduct a thorough gap analysis to identify areas of noncompliance 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.

At KPMG, we can help you streamline your compliance journey and successfully adapt to the challenges presented by the provisional EU AI Act. Our team can operationalize and scale your AI governance, management, and monitoring programs, while sharing learnings from prior engagements and our own AI automation journey to improve processes and policies.

4. **Automate model management and evaluation:** Optimize, automate, and streamline AI model management processes, ensuring models are transparent, explainable, and trustworthy. Leverage automation to extract and map technical metrics and data from AI model and application metadata to your governance framework, enabling automated compliance and management processes.

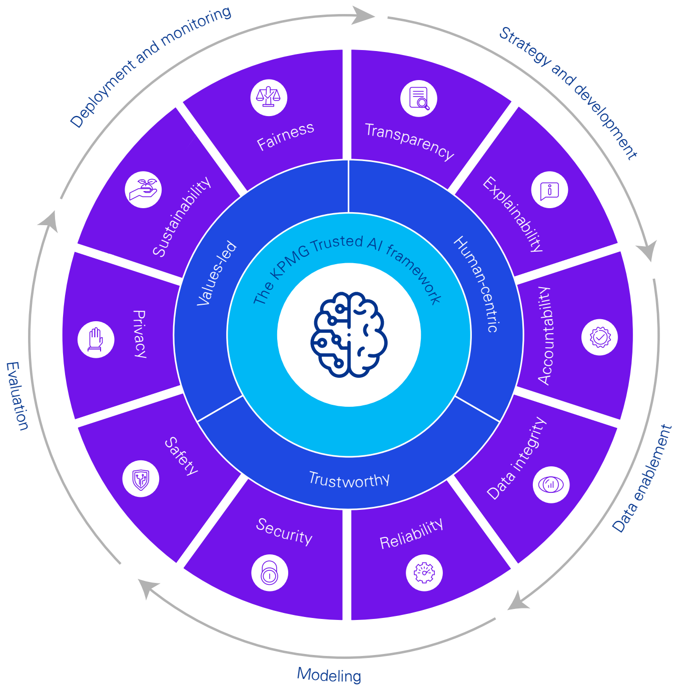
5. **Review data privacy and security:** Review and, if necessary, update data handling practices to ensure they comply with GDPR and other data privacy aspects of the EU AI Act. Leveraging automated threat detection, analysis, and intelligence solutions can drastically reduce the level of effort required to support testing and technical documentation requirements outlined in the EU AI Act.

6. **Maintain an AI inventory** and management tool to ensure AI systems are easily traceable and continuously monitored.

7. **Train your employees** on AI ethics and compliance.

8. **Communicate with all stakeholders**, including customers and partners, about how your company is addressing the EU AI Act requirements.

The need for Trusted AI



The KPMG Trusted AI framework

The EU's goal for this legislation is to ensure that AI systems are "safe, transparent, traceable, non-discriminatory and environmentally friendly."[3] Those priorities are shared by the KPMG Trusted AI framework. This ten-pillar guide is KPMG's strategic framework to help design, build, deploy, and use AI solutions in a responsible and ethical manner while also accelerating value.

Through our Trusted AI framework, we assist clients in strategically integrating responsible AI practices, from initial assessments and benchmarking to designing AI governance processes that will align with the provisions of the EU AI Act.

The journey to compliance with the EU AI Act is just beginning. With KPMG, you have an adviser who understands the complex regulatory landscape surrounding this legislation—and who is dedicated to empowering your business to help harness the innovation of AI technologies in a compliant and trusted manner.

[3] Source: European Parliament, "EU AI Act: first regulation on artificial intelligence" (December 2023).

Contact our team to start preparing for compliance with the EU AI Act, and learn how to leverage our Trusted AI framework to foster innovation while mitigating risk.

Contacts

Steve Chase
AI and Digital Innovation Vice Chair
KPMG LLP

Laurent Gobbi
Global Trusted AI Leader
KPMG LLP

Bryan McGowan
US Trusted AI Leader
KPMG LLP

Authors

Brian Consolvo
Technology Risk Principal
KPMG LLP

Kanika Saraiya Havelia
Technology Risk Director
KPMG LLP

Tristan Ingold
Technology Risk Manager
KPMG LLP

visit.kpmg.us/TrustedAIservices

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the authors and do not necessarily represent the views and opinions of KPMG LLP.