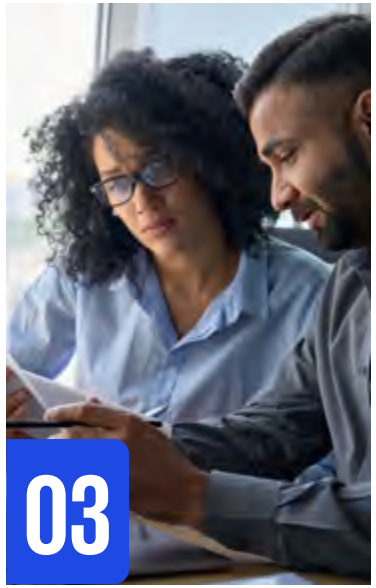
Decoding the EU AI Act

Understanding the AI Act's impact and how you can respond

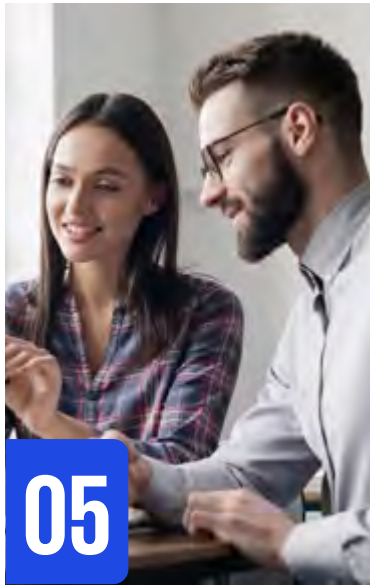
KPMG. Make the Difference.

KPMG Switzerland | kpmg.ch/digitaltrust
| kpmg.ch/cyber

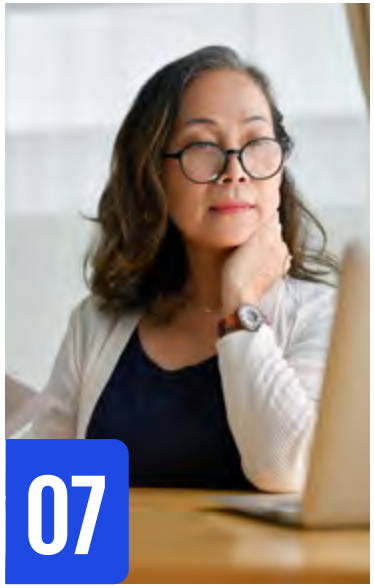
Contents



Introduction



Executive summary



Examining the AI Act's impact and scope

Unravelling the AI Act's key components

Next steps

Introduction

Artificial Intelligence (AI) is offering new benefits to society and businesses, aiming to transform the workplace and major industries along the way. Simply put, the race is on to embrace the remarkable and evolving power of AI and automation.

As KPMG's Global Tech Report 2023 reveals, most global executives (62 percent) report an increase in performance or profitability from digital transformation initiatives related to AI and machine learning over the past 24 months. And 68 percent say these technologies will play a 'vital' role in helping them achieve their business objectives over the next three years, while 57 percent believe AI and machine learning will be 'important' in meeting short-term objectives.

But as the worldwide AI proliferation in business and our everyday lives unfolds, there is a critical need for guardrails and legislation to deal with significant new risks regarding the appropriate and ethical use, development and distribution of AI. According to Trust in artificial intelligence, a global survey conducted by KPMG Australia and the University of Queensland, three in five people are wary about trusting AI systems, and 71 percent expect AI to be regulated. More recently, CEOs from global tech giants called for greater AI regulation at a meeting on Capitol Hill to protect people from the worst effects of AI.

In response, the European Union (EU) has reached a ground-breaking provisional agreement on a comprehensive Artificial Intelligence Act (AI Act) that takes a risk-based approach to protecting fundamental rights, democracy, the rule of law and environmental sustainability.[1] Though it's expected to become law in 2024, with compliance expected by 2025, this legislation — the first of its kind — is anticipated to emerge as the de-facto new global standard for AI regulation.

With the introduction of the AI Act, the EU aims to strike a balance between fostering AI adoption and ensuring individuals' right to responsible, ethical and trustworthy use of AI. In this paper, we explore what the AI Act may mean to your organization and examine the structure of the AI Act, the obligations it imposes, the timelines for compliance and the action plan that organizations should consider.

> **"Organizational leadership should drive initiatives in line with the AI Act, company brand, values and risk tolerance to promote responsible use of AI. This can help promote ethical development, regulatory compliance, risk mitigation and stakeholder trust."**
>
> **David Rowlands**
> Global AI Leader
> KPMG International

> **"AI should be developed and used with a focus on safety and ethics, turning technological advancement into a positive force for society. The EU AI Act will help foster innovation while protecting end-users."**
>
> **Laurent Gobbi**
> Global Trusted AI Leader
> KPMG International

[1] European Parliament. (December 9, 2023). Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI [Press release].

Executive summary

The AI Act aims to regulate the ethical use of AI

AI holds immense promise to expand the horizon of what is achievable and to impact the world for our benefit — but managing AI's risks and potential known and unknown negative consequences will be critical. The AI Act is set to be finalized in 2024 and aims to ensure that AI systems are safe, respect fundamental rights, foster AI investment, improve governance, and encourage a harmonized single EU market for AI.

Most AI systems need to comply with the AI Act by the first half of 2026

The AI Act's definition of AI is anticipated to be broad and include various technologies and systems. As a result, organizations are likely to be significantly impacted by the AI Act. Most of the obligations are expected to take effect in early 2026. However, prohibited AI systems will have to be phased out six months after the AI Act comes into force. The rules for governing general-purpose AI are expected to apply in early 2025.[2]

Providers and users of high-risk AI systems face stringent obligations

The AI Act applies a risk-based approach, dividing AI systems into different risk levels: unacceptable, high, limited and minimal risk.[3]

High-risk AI systems are permitted but subject to the most stringent obligations. These obligations will affect not only users but also so-called 'providers' of AI systems. The term 'provider' in the AI Act covers developing bodies of AI systems, including organizations that develop AI systems for strictly internal use. It is important to know that an organization can be both a user and a provider.

Providers will likely need to ensure compliance with strict standards concerning risk management, data quality, transparency, human oversight, and robustness.

Users are responsible for operating these AI systems within the AI Act's legal boundaries and according to the provider's specific instructions. This includes obligations on the intended purpose and use cases, data handling, human oversight and monitoring.

Guardrails for general AI systems

New provisions have been added to address the recent advancements in general-purpose AI (GPAI) models, including large generative AI models.[4] These models can be used for a variety of tasks and can be integrated into a large number of AI systems, including high-risk systems, and are increasingly becoming the basis for many AI systems in the EU. To account for the wide range of tasks AI systems can accomplish and the rapid expansion of their capabilities, it was agreed that GPAI systems, and the models they are based on, may have to adhere to transparency requirements. Additionally, high-impact GPAI models, which possess advanced complexity, capabilities, and performance, will face more stringent obligations. This approach will help mitigate systemic risks that may arise due to these models' widespread use.[5]

The AI Act does not affect existing Union law

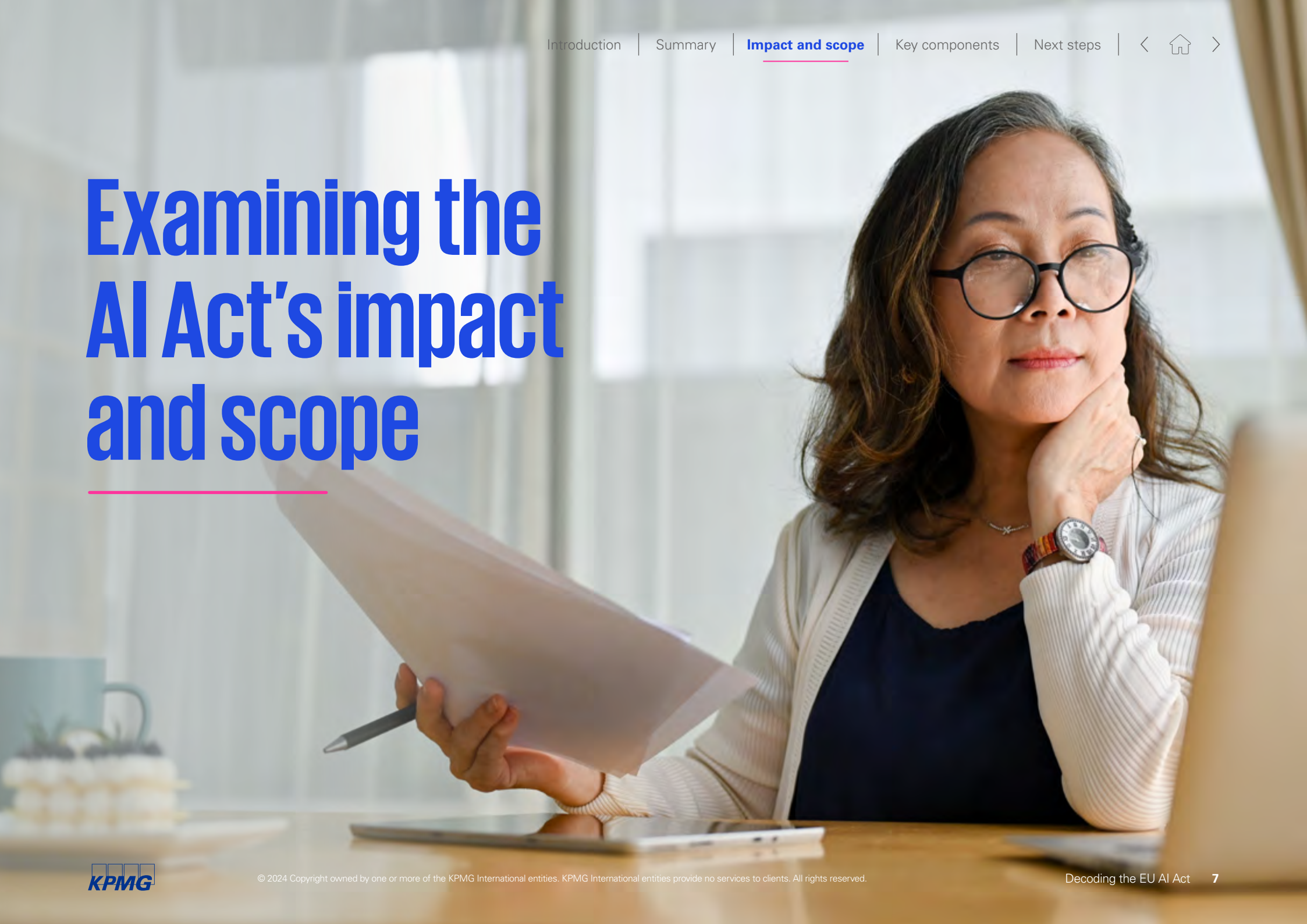
Existing Union laws, for example, on personal data, product safety, consumer protection, social policy, and national labor law and practice, continue to apply, as well as Union sectoral legislative acts relating to product safety. Compliance with the AI Act will not relieve organizations from their pre-existing legal obligations in these areas.

Understanding the AI Act's impact on your organization will be pivotal to success

Organizations should take the time to create a map of the AI systems they develop and use and categorize their risk levels as defined in the AI Act. If any of their AI systems fall into the limited, high or unacceptable risk category, they will need to assess the AI Act's impact on their organization. It is imperative to understand this impact — and how to respond — as soon as possible.

[2] European Commission. (December 12, 2023). Artificial Intelligence — Questions and Answers [Press release].
[3] European Council. (December 9, 202). Artificial Intelligence Act Trilogue: Press conference — Part 4. [Video].
[4] European Parliament. (March 2023). General-purpose artificial intelligence [Background material].
[5] European Commission. (December 12, 2023). Artificial Intelligence — Questions and Answers [Press release].

Examining the AI Act's impact and scope



The European Commission (EC) proposed the AI Act in April 2021. As of December 2023, the European Parliament, the European Council and the European Commission have reached a provisional agreement to make the AI Act law.

The proposed AI Act is expected to reshape how we think about and manage AI similarly to what has happened in data privacy over the last couple of years. Expected to become law in 2024, the AI Act will likely have an immediate wide-ranging impact on any business operating in the EU that offers AI products, services or systems. The law introduces a definition for AI in the EU, categorizes AI systems by risk, lays out extensive requirements and necessary safeguarding mechanisms for AI systems, and establishes transparency obligations.

What it aims to do?

The EC aims to balance promoting AI development and boosting innovation with managing emerging risks effectively. This is reflected in the objectives of the proposal:[6]

- Ensuring that AI systems on the EU market are safe and respect public rights and values.
- Providing legal certainty to facilitate investment and innovation in AI systems.
- Enhancing governance and effective enforcement of ethics and safety requirements.
- Facilitating the development of a single EU market for lawful, safe, trustworthy AI applications while preventing market fragmentation.

Through our lens: The potential impact of the AI Act

Stimulate the positive

- Stimulate innovation through regulatory sandboxes where small and medium-sized enterprises can test their AI systems without imminent regulatory scrutiny.
- Promote harmonization of standards, codes of conduct and certification.
- Offer greater transparency regarding AI systems.
- Create a level playing field for those involved.
- Safeguard fundamental rights and provide legal certainty for individuals residing in the EU.

Adopt best practices

- Categorize your AI systems and understand the associated risks.
- Impose more stringent requirements for high-risk AI systems (obligatory risk management, data governance, technical documentation, etc.).
- Carry out conformity assessments and post-market monitoring for high-risk AI systems.
- Establish effective oversight and enforcement mechanisms.

Manage and reduce risks

- Prohibit unacceptable risks in AI systems.
- Avoid fundamental rights violations.
- Prevent the use of subliminal or unethical techniques that might influence or distort a person's behavior in such a way that it causes harm to that person or another person.
- Minimize bias that could result in unfair or inadequate outcomes.
- Restrict the exploitation of vulnerable people or groups due to their age, disability, political opinion or other factors.

[6] European Commission. (April 21, 2021). Proposal for a Regulation of the European Parliament and of the Council, "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act."

To achieve these objectives, the AI Act applies a risk-based approach. This allows for establishing specific minimum requirements to address the risks and problems linked to AI systems without unduly constraining or hindering technological development or disproportionately increasing costs relating to placing AI systems on the market.

Who will be affected?

Most organizations, both inside and outside the EU, are developing or using AI systems that will likely qualify as AI under the scope of the AI Act. Given the short implementation period, however, organizations should gain a profound understanding of the AI systems they are developing and/or deploying and how they measure up to the AI Act's requirements.

What parties are covered?

- Any provider placing AI systems on the market or putting them into service within the EU, regardless of location.
- Any provider of AI systems located outside the EU, whose system output can or is intended for use in the EU.
- Any provider of AI systems located in the EU.
- Any importer or distributor placing AI systems on the market or making them available within the EU.
- Product manufacturers placing products with AI systems on the market or putting them into service within the EU under their name or trademark.
- Users of AI products and services within the EU.

What is not covered?

- 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 agreements.
- AI systems developed and used for the sole purpose of scientific research and discovery.
- AI systems in the research, testing, and development phase before being placed on the market or put into service (this includes free and open-source AI components).
- People using AI for personal use.

In the same way the General Data Protection Regulation (GDPR) is enforced, the EC understands that non-European entities selling their products in European markets should be regulated similarly to the member states. The EU is expected to be the center ground for global AI standards, with divergence in the US and possibly the UK. Like the GDPR, the AI Act will have and extra-territorial effect.

Who is affected in your organization?

Executives who manage compliance, data governance and the development, deployment and use of AI technologies will likely see their roles and responsibilities impacted by the AI Act. Beyond senior roles in the organization, the Board of Directors and various Governance Committees may also be affected, and they should develop awareness and knowledge. Given the broad definition of AI and the current pace of proliferation, organizations should take a holistic approach. Senior executives should collaborate on purposeful innovation and development, risk management, and governance of AI systems to achieve compliance with the AI Act.

How it will be enforced and what are the penalties

The EC has proposed a structure for enforcing AI provider requirements by establishing an Artificial Intelligence Board and Expert Group. Both parties sit at the EU level and are responsible for:

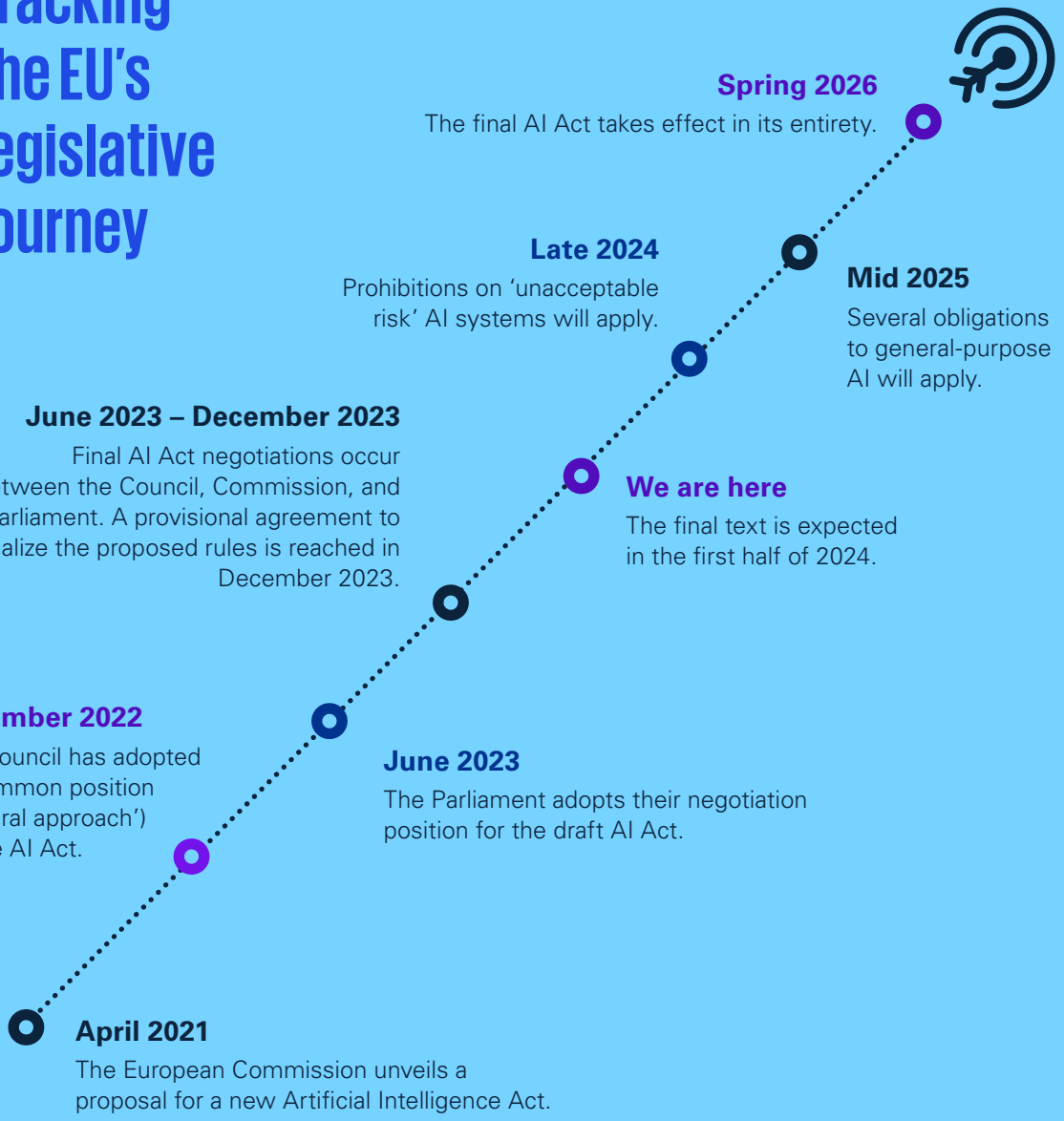
- Contributing to effective collaboration with national supervisory authorities.
- Providing recommendations for best practices.
- Ensuring consistent application of the regulation.

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

The EU's proposed regulation will likely have a far-reaching impact on all organizations leveraging the vast power of AI, and the consequences of noncompliance could range from restricting market access to significant fines depending on the level of noncompliance. Fines may range from 35 million euros or 7 percent of global turnover to 7.5 million or 1.5 percent of turnover, depending on the infringement and size of the company.[7]

[7] European Parliament. (December 9, 2023). Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI [Press release].

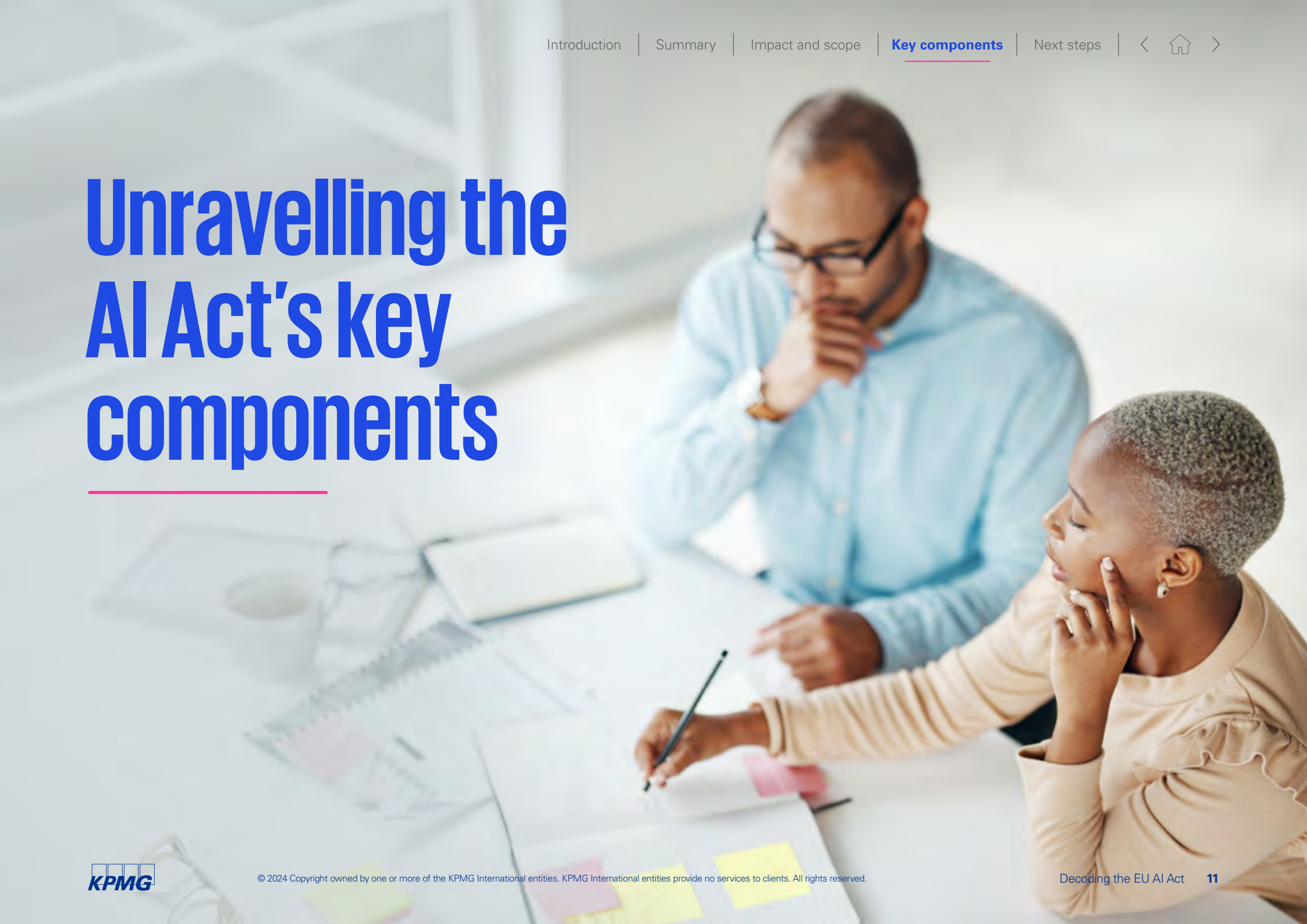
Tracking the EU's legislative journey



When will it apply?

Most of the obligations outlined in the AI Act are expected to become effective by the first half of 2026. Prohibitions are anticipated to take effect by the end of 2024, and obligations regarding general-purpose AI (GPAI) are expected to take effect as early as 2025. GPAI refers to AI systems that perform generally applicable functions, such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others, but can have a wide range of possible uses, both intended and unintended. These systems may be utilized as high-risk AI systems or incorporated as components of other high-risk AI systems.

Unravelling the AI Act's key components



The AI Act is a comprehensive document designed to help provide a clear definition of artificial intelligence, enabling EU-wide alignment and consistency with other Union laws and regulations. The AI Act's primary goal is to establish a uniform and horizontal legal framework to promote the uptake of AI systems while providing a high level of protection against their harmful effects. This framework can help to build trust in AI technology and give individuals and organizations greater confidence in using it.

Defining artificial intelligence

The AI Act applies a broad definition of an AI system derived from the recently updated Organisation for Economic Co-operation and Development (OECD) definition. While the AI Act's text is not yet publicly available, the OECD definition is as follows:

"An AI system is a machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[8]*"*

This definition is deliberately kept broad to cover the whole spectrum, from simpler technologies and systems focusing on single-use cases to advanced applications of deep learning and generative AI. As a result, **the AI Act's scope became much wider than initially anticipated**, extending significantly beyond our more recent understanding of advanced and generative AI. The AI Act's defined scope has several exemptions for AI systems, such as those used for military or defense purposes and limited exemptions for free and open-source systems.

AI risk framework and requirements

The AI Act defines a framework to understand the risks associated with AI. It classifies AI systems based on their potential risks and divides them into different categories depending on the data they capture, and the decisions or actions taken with that data.

EU obligations will vary depending on the category of AI being used. While an agreement on the context has been reached, the final text of the regulations is not yet available. However, the following sections summarize the obligations stipulated under the AI Act, based on the publicly available information.[9]

[8] Note that the earliest version of the AI Act defines AI systems as systems that were developed using one of the following techniques and approaches:
(a) Machine learning approaches, including supervised, unsupervised, and reinforcement learning, using a wide variety of methods, including deep learning.
(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems.
(c) Statistical approaches, Bayesian estimation, search and optimization methods.

[9] European Commission. (April 21, 2021). Proposal for a Regulation of the European Parliament and of the Council, "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act."

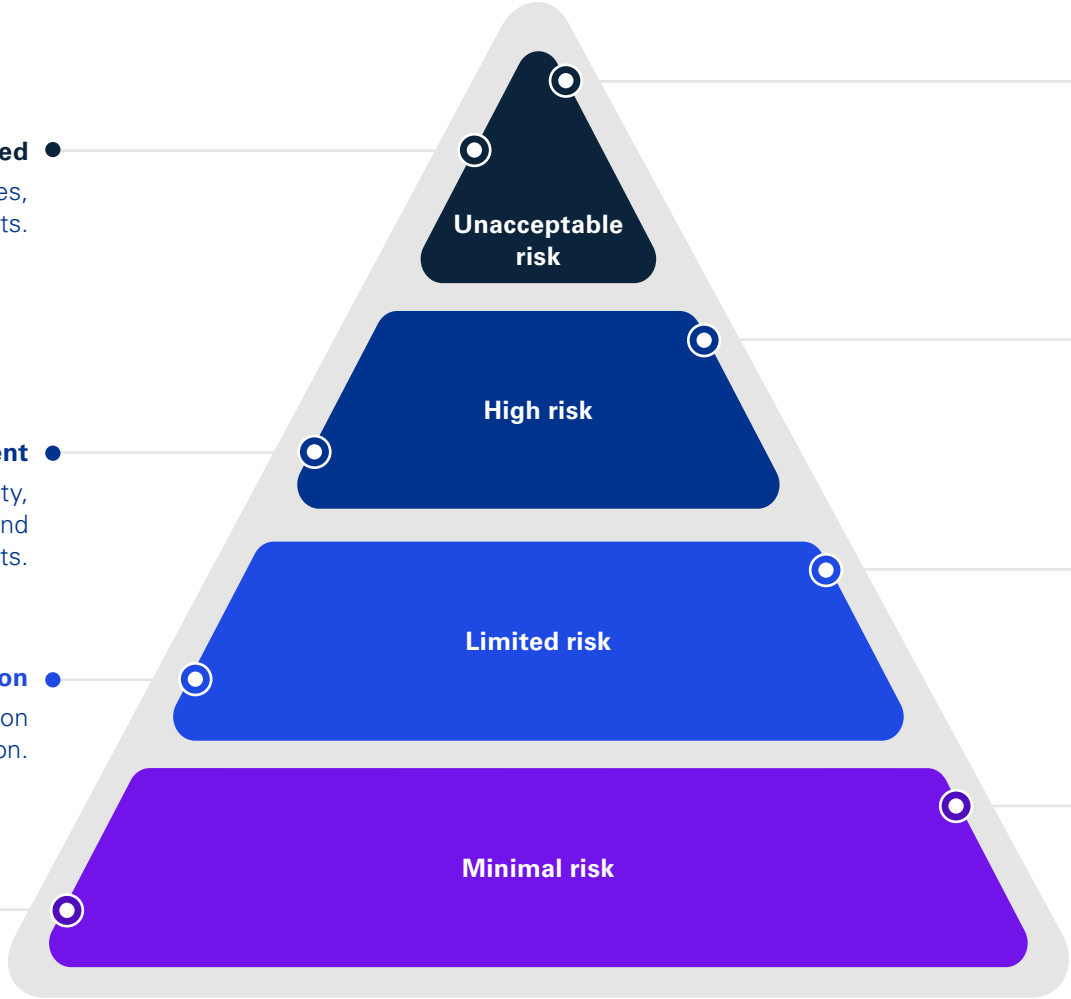
The AI Act takes a risk-based approach

Prohibited
Contravene Union values, like fundamental rights.

Conformity assessment
High risk to health, safety, environment and fundamental rights.

Transparency obligation
Risk of impersonation or deception.

No obligations
No high risks.



Examples of unacceptable-risk AI systems

- Behavioral manipulation.
- Exploitation of vulnerable characteristics of people.
- Social scoring by public authorities.
- Real-time remote biometric identification for law enforcement.

Examples of high-risk AI systems:

- Evaluation of eligibility to credit, health or life insurance or public benefits.
- Analyses of job applications or evaluation of candidates.
- Product safety components.

Examples of limited-risk AI systems:

- AI systems that interact with consumers.
- Generative AI*: AI systems generating or manipulating content (image, audio or video).

Examples of minimal-risk AI systems:

- Spam filters.
- AI-enabled video games.

* Further specific obligations to generative AI and foundation models will apply outside of this risk-based approach

Unacceptable-risk AI systems

Which AI systems are covered? AI systems that enable manipulation, exploitation and social control practices are seen as posing an unacceptable risk. This category prohibits AI for the following purposes:

- Manipulation that harms or is likely to harm an AI user or another person.
- Exploiting vulnerabilities of a specific group of persons.
- Social scoring leading to detrimental or unfavorable treatment in social contexts.
- Indiscriminate scraping of facial images.
- Emotion recognition software in the workplace and education (with some exceptions).
- Use of AI that categorizes persons based on sensitive traits such as race, political opinions or religious beliefs.
- Predictive policing on individuals (risk scoring for committing future crimes based on personal traits).
- Remote biometric identification of people (partial ban with some exceptions in law enforcement).

What are the obligations related to this category? Since the AI systems in this category pose an unacceptable risk, their use is prohibited.

High-risk AI systems

Which AI systems are covered? AI systems that negatively affect safety or fundamental rights will be considered high risk and will be divided into two categories: 1) AI systems that are used in products falling under the EU's product safety legislation. This includes toys, aviation, cars, medical devices and elevators. 2) AI systems falling into specific areas that will have to be registered in an EU database.[8] These include:

- Critical infrastructure, such as the supply of utilities.
- Educational and vocational training, for example, automated scoring of — or exclusion from — exams.
- Employment, workers management and access to self-employment, for example, automated recruitment and application triage.
- Access to essential private and public services and benefits (e.g. healthcare), creditworthiness evaluation of natural persons, and risk assessment and pricing in relation to life and health insurance.
- Law-enforcement systems that may interfere with fundamental rights, such as automated risk scoring regarding potential offenders, deepfake detection software and evidence reliability scoring.
- Migration, asylum and border control management, for example, verification of authenticity of travel documents and visa and asylum application examinations.
- Administration of justice and democratic processes, for example, legal interpretation tools to assist judicial authorities.

Most organizations use these high-risk AI systems, such as AI for recruitment purposes.

It is also important to note that the Commission can add more uses to the high-risk AI systems category through delegated acts. This is discussed further in the 'Next steps' section of this report.

What are the obligations related to this category? Since the AI systems in this category are considered high-risk, they are subject to the most stringent regulatory requirements:

- Adequate risk management to identify, evaluate and mitigate risks during the lifecycle of the AI system. This obligation will, in effect, require implementing a dedicated risk management system and the completing documented risk assessments, which must be completed continuously; they must be living documents.
- Appropriate data governance and management practices (training, validation and testing) to ensure dataset quality. This is a key obligation to help ensure that datasets do not lead to discrimination or inaccurate results. Notably, sensitive personal data must not be included unless included to ensure that both inputs and outputs are not discriminatory.
- Technical documentation must demonstrate compliance with obligations and allow for compliance assessments.
- Logging of events to ensure traceability of the system's functioning.
- Record keeping regarding tracing and monitoring high-risk situations, conforming to standards, and ensuring that the AI systems' output has not led to any discriminatory effects.
- Minimum logging must include usage, data and personnel identification.
- Registration in the EU database for high-risk AI systems.

[8] European Parliament. (December 19, 2023). EU AI Act: first regulation on artificial intelligence.

- Transparency obligations to enable correct AI interpretation and use, accompanied by instructions in an appropriate digital format.
- Implementation of appropriate human oversight.
- Appropriate levels of accuracy, robustness and cybersecurity.

High-risk AI systems will be subject to conformity assessment procedures to determine whether they comply with the AI Act's requirements. As a final step before providers place them on the market, a declaration of conformity must be signed, and the AI system must affix the CE mark confirming European conformity. However, the specifics of such standards still need to be clarified.

Post-market monitoring obligations will apply once the AI system is on the market. This includes reporting serious incidents or malfunctions of high-risk AI systems to the relevant market surveillance authorities.

What are the obligations of the deployers?

Deployers of high-risk AI systems, including public bodies and private entities providing essential services, such as banks, insurers, hospitals, and schools, bear specific obligations to ensure responsible use. These obligations include:

- Completing a fundamental rights impact assessment (FRIA) before deploying the AI system.
- Implementing of human oversight by trained individuals.
- Ensuring that input data is pertinent to the system's intended use.
- Suspending system usage in case of national-level risks.
- Reporting serious incidents to the AI system provider.
- Retaining automatically generated system logs.
- Complying with registration requirements if the user is a public authority.
- Adhering to GDPR obligations for data protection impact assessments.
- Verifying compliance with the AI Act and ensuring all relevant documentation is available
- Informing individuals about the potential use of high-risk AI.

Importers and distributors, before introducing a high-risk AI system to the market, share the responsibility of verifying compliance, documenting relevant information, and engaging in communication with the provider and market surveillance authorities.

General-purpose AI, foundation models and generative AI

Which AI systems are covered? General-purpose AI (GPAI) and foundation models were not defined in the original proposal but have been included in the current version to address situations where AI systems serve various purposes or are integrated into other high-risk systems.

- GPAI systems are intended to perform generally applicable functions such as image/speech recognition, audio/video generation, pattern detection and other applications. Well-known examples include generative AI applications such as ChatGPT and Dall-E.
- Foundation AI models are trained on broad data at scale, designed for the generality of output, and can be adapted to a wide range of tasks. A well-known example is GPT-4, the foundation model under the latest ChatGPT.

What are the obligations related to this category? GPAI systems must comply with transparency requirements. These include technical documentation, complying with EU copyright law and providing information on AI training data.

For the most powerful foundation models, more stringent obligations will apply. Providers must: conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents and ensure cybersecurity and energy efficiency.

The rationale behind regulating this category of AI systems separately is the supply chain dynamics: foundational models are likely to continue to be an important source for downstream AI 'providers' and AI 'users' who reuse these models for more specific applications. Because of these downstream actors lack of control and bargaining position against providers of foundational models, the providers of these models are being required under the Act to assume a targeted share of the regulatory responsibility. This is also an area we address in the next steps section of the report.

Limited-risk AI systems

Which AI systems are covered? Some AI systems intended to interact with natural persons or generate content would not necessarily qualify as high-risk AI systems but may entail risks of impersonation or deception. This includes the outputs of most generative AI systems. In practice, the following AI systems are to be identified in this category:

- Chatbots, such as ChatGPT-based systems.
- Emotion-recognition systems.
- Biometric-categorization systems.
- Systems generating 'deepfake' content.

What are the obligations related to this category? AI systems in this category are subject to transparency obligations. Unlike high-risk systems that impact development and risk management in a broad sense, obligations for limited-risk systems focus on outputs and users:

- People must be informed that they are interacting with an AI system.
- People exposed to a (non-prohibited) emotion recognition or biometric system must be informed about the system's presence.
- Deepfake content must be disclosed as being artificially generated or manipulated.

Minimal-risk AI systems

Which AI systems are covered? The AI Act does not define this category. It includes AI systems not in other categories, like AI-enabled video games or spam filters.

What are the obligations related to this category? This AI category will not be subject to stringent obligations except for adhering to general product safety standards. Nevertheless, the promotion of establishing codes of conduct is strongly encouraged to foster wider adoption of reliable AI within the EU.

Next steps

As the agreed text of the AI Act awaits formal adoption by the European Parliament and the European Council to become EU law, organizations can proactively begin preparing for compliance.

The first step is to ensure the right people in your organization start preparing for these upcoming regulatory requirements as soon as possible. Early engagement gives you more time to understand the requirements and their impact across the AI lifecycle. The AI Act identifies various roles, including legal, privacy, data science, risk management and procurement professionals. A multidisciplinary task force responsible for compliance with the AI Act should cover this full range of expertise.

The second step is to comprehensively understand AI systems developed or used in your organization and categorize them based on the risk levels defined in the AI Act. If any of your AI systems fall into the minimal, high, or unacceptable risk category, you may be required to make significant changes to processes and operations before 2026 or sooner for AI systems with unacceptable risk. It is crucial to have a clear plan of what needs to be done as quickly as possible to manage the necessary organizational transformation and ensure timely compliance with the new legal framework when it comes into effect.

Here is a list of key actions your organization can take immediately and in the long term to help ensure sustainable compliance with current regulations and future developments in the AI regulatory landscape.

Key actions for the short-term

01 Define the appropriate governance

- **Define policy to identify risk levels for AI systems:** Determine how to categorize your AI systems based on the risk categories outlined in the AI Act. It's worth noting that the list of prohibited and high-risk AI systems in the AI Act may be expanded. To avoid costly remediation, your policy should take into consideration the legislative reasoning behind these categories: (i) prohibited AI systems may enable manipulative, exploitative and social control practices; and (ii) high-risk AI systems may have a significant negative impact on the health, safety and fundamental rights of individuals in the Union.
- **Manage stakeholder expectation:** Communicate transparently with all stakeholders, including customers and partners, about how your company addresses the AI Act requirements and outlines expectations and requirements for each stakeholder group in managing ongoing compliance.
- **Implement (or improve) your AI governance framework:** Implement standards and good practices for AI system development, deployment and maintenance in alignment with the AI Act's requirements and other emerging regulatory standards to ensure consistency and scalability. Here again, leveraging an automated solution to manage various aspects of compliance mapping, obligations tracking, and workflow management can help.
- **Set up sustainable data management practices:** Implement and maintain robust data governance frameworks that ensure long-term data quality, security and privacy — agile and adaptable to future technological and regulatory changes.

Policy. Communication. Governance. Data.

02 Know your risks

- **Prioritize and manage AI risks adequately:** Understand the risks that AI systems pose internally and externally to the public, your organization, stakeholders and the entire ecosystem. This includes understanding what a fundamental rights impact assessment and a systemic risk assessment cover (to the extent relevant). Review and, if necessary, update your data handling practices to ensure they comply with applicable laws, regulations and industry good practice, including data privacy and security.
- **Perform inventory and classify current AI landscape:** Review existing AI systems and use cases and categorize them to identify high-risk systems requiring compliance with the AI Act. Leveraging an automated detection and identification solution, such as automating intake questionnaires or implementing a workflow platform, can aid in accelerating the discovery, inventory and classification activities required to support and map compliance obligations.
- **Conduct a gap analysis:** Conduct a thorough gap analysis to identify areas of noncompliance and develop an action plan to address these gaps. This analysis could be expedited using an automated or rapid AI assessment approach against established governance frameworks or AI Act compliance obligations.
- **Test AI systems thoroughly:** Ensure the AI systems operate as intended. The AI Act also established a regulatory sandbox that can be used for testing. Leveraging automated threat detection, analysis and intelligence solutions can drastically reduce the effort required to support testing and technical documentation requirements outlined in the AI Act.
- **Define third party risk management process:** Enhance your third party risk assessments to cover AI-specific considerations. If your organization uses foundational models to develop more specific applications, you should continually monitor how those providers intend to comply with the AI Act. Determine what technical documentation they will make available to enable you to manage your risks and the downstream impact on you. Such providers are likely to make their 'acceptable use' policies more stringent to avoid the risk that their GPAI models are used for purposes outside the risks they have assessed against.

Prioritize. Classify. Assess gaps. Test.

03 Initiate actions requiring a scaled approach

- **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.
- **Document and keep record:** Establish a documentation repository and management system to ensure appropriate documentation processes are in place to ensure AI systems are well-documented and compliant with the AI Act.
- **Train employees on AI ethics and compliance:** Educate your workforce on the AI systems' legal and ethical implications and intended use, ensuring they are prepared to handle new responsibilities and compliance tasks.
- **Consumer terms and conditions:** Where using AI Systems with consumers, consider whether: (i) changes are required to your terms and conditions, privacy policy and consent notices; (ii) develop your 'explainability' statement to enable consumers to understand the decision-making processes of your AI systems.

Automate. Document. Train. Protect.

Key actions for the mid- to long-term

01 Anticipate regulation impact on your business

- **Build consumer trust through transparency:** Prioritize transparency in AI operations to build and maintain public trust, ensuring long-term viability and acceptance of AI solutions.
- **Align strategically with regulatory changes:** Align your business strategies with the evolving regulatory landscape of AI, anticipating future amendments to the AI Act.
- **Collaborate and keep an open dialogue:** Participate in industry discussions and policy-making processes related to AI regulation to influence and stay ahead of future regulatory trends.

02 Develop ethics and governance

- **Prioritize 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.
- **Maintain ongoing AI literacy and training programs:** Develop long-term training programs to enhance AI literacy across the organization, fostering a culture of ethical AI use and compliance.

03 Embed trusted AI in innovation, design and control

- **Innovate within ethical boundaries:** Foster an environment of innovation that respects ethical boundaries and regulatory requirements, balancing technological advancement with social responsibility.
- **Implement trusted AI and security by design:** Adapt the building of AI systems to include Trusted AI and AI Security in the design phase.
- **Audit and update the AI system regularly:** Conduct periodic reviews and updates of AI systems to ensure ongoing compliance and to integrate advancements in AI transparency and explainability.

How this connects with what we do

We believe in the transformative power of AI and that it can only reach its full potential when it is paired with human expertise, ingenuity and effective risk management.

At KPMG, our purpose is to inspire confidence and empower change. Tracing our origins back over 150 years, KPMG people have played a leading role in harnessing the power of new technologies and providing assurance and direction in implementing them.

By combining deep industry expertise and process know-how with leading technology alliances, KPMG professionals are accelerating value from AI and making the difference for clients, people and communities all around the world.

Many aspects of the AI Act will be challenging for organizations to implement and address, especially in terms of technical documentation for the testing, transparency and explainability of AI applications. Adding to this challenge is the fact that every AI application comes with its own business processes, impacts and risks.

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

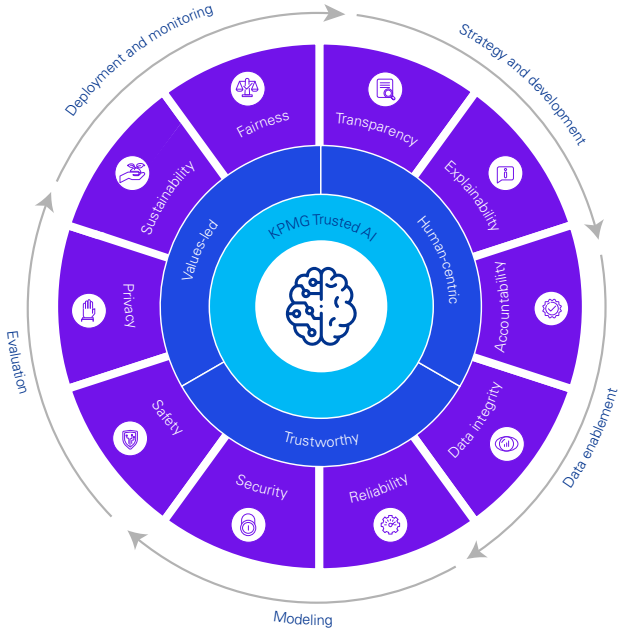
KPMG Trusted AI

KPMG Trusted AI is our strategic approach and framework to designing, building, deploying and using AI solutions in a responsible and ethical manner so we can accelerate value with confidence. It was developed based on the combination of our extensive experience in AI risk management and input from existing global standards.

This multi-faceted framework provides coverage across operational business lines, compliance lines and internal audit — integrating broad expertise in AI solutions, governance and assessment. It is designed with controls and tools to help establish trustworthy and ethical assessment, design and deployment of your AI systems.

We offer a broad approach that enables your organization to effectively manage these upcoming regulatory changes. Through our services, we assist you in embarking on your transformation and compliance journey aligned with and customized to your business requirements.

To learn more visit: kpmg.ch/digitaltrust



Acknowledgments

We would like to sincerely thank the following subject matter professionals for contributing to this report.

Leanne Allen
Partner
KPMG in the UK
leanne.allen@kpmg.co.uk

Stuart Fuller
Partner
KPMG Australia
stuartfuller@kpmg.com.au

Paul Henninger
Partner
KPMG in the UK
paul.henninger@kpmg.co.uk

Francois Maartens Heynike
KPMG Law in Germany
fheynike@kpmg-law.com

Dirk Distelrath
Director
KPMG in Germany
ddistelrath@kpmg.com

Sylvia Klasovec Kingsmill
Partner
KPMG in Canada
skingsmill@kpmg.ca

Vincent Maret
Partner
KPMG in France
vmaret@kpmg.fr

Bryan McGowan
Principal
KPMG in the US
bmcgowan@kpmg.com

Matthew Miller
Principal
KPMG in the US
matthewpmiller@kpmg.com

Melinda Rankin
Associate Director
KPMG Australia
mrankin1@kpmg.com.au

James Thomas
Partner
KPMG in the UK
james.thomas2@kpmg.co.uk

Oskar Trpisovsky
Senior Manager
KPMG in Canada
otrpisovsky@kpmg.ca

Frank Van Praat
Director
KPMG in the Netherlands
vanpraat.frank@kpmg.nl

Usman Wahid
Partner
KPMG Law in the UK
usman.wahid@kpmg.co.uk

Contacts

Dr. Matthias Bossardt
Partner,
Head of Cyber & Digital Risk Consulting

E: mbossardt@kpmg.com
T: +41 58 249 36 98

Dr. Thomas Bolliger
Partner,
Cyber & Digital Risk Consulting

E: tbolliger@kpmg.com
T: +41 58 249 28 13

Yves Bohren
Partner,
Cyber & Digital Risk Consulting

E: ybohren@kpmg.com
T: +41 58 249 48 95

Nicolas Tinguely
Partner,
Cyber & Digital Risk Consulting

E: ntinguely@kpmg.com
T: +41 58 249 21 44

KPMG AG
Badenerstrasse 172
PO Box
8036 Zürich

Michele Daryanani
Director,
Cyber & Digital Risk Consulting

E: micheledaryanani@kpmg.com
T: +41 58 249 61 74

kpmg.ch/digitaltrust
kpmg.ch/cyber

Transforming for a future of value

Connected. Powered. Trusted. Elevate. KPMG firms' suite of business transformation technology solutions can help you engineer a different future of new opportunities that are design to create and protect value.

KPMG Connected Enterprise

Rebuild your business, end to end, around your customers.

KPMG Powered Enterprise

Drive outcome-driven functional transformation.

KPMG Trusted Imperative

Build and sustain the trust of your stakeholders.

KPMG Elevate

Unlock financial value quickly and confidently.

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

kpmg.ch

Designed by Evalueserve.
Publication name: Decoding the EU AI Act
Publication number: 139211-G
Publication date: February 2024