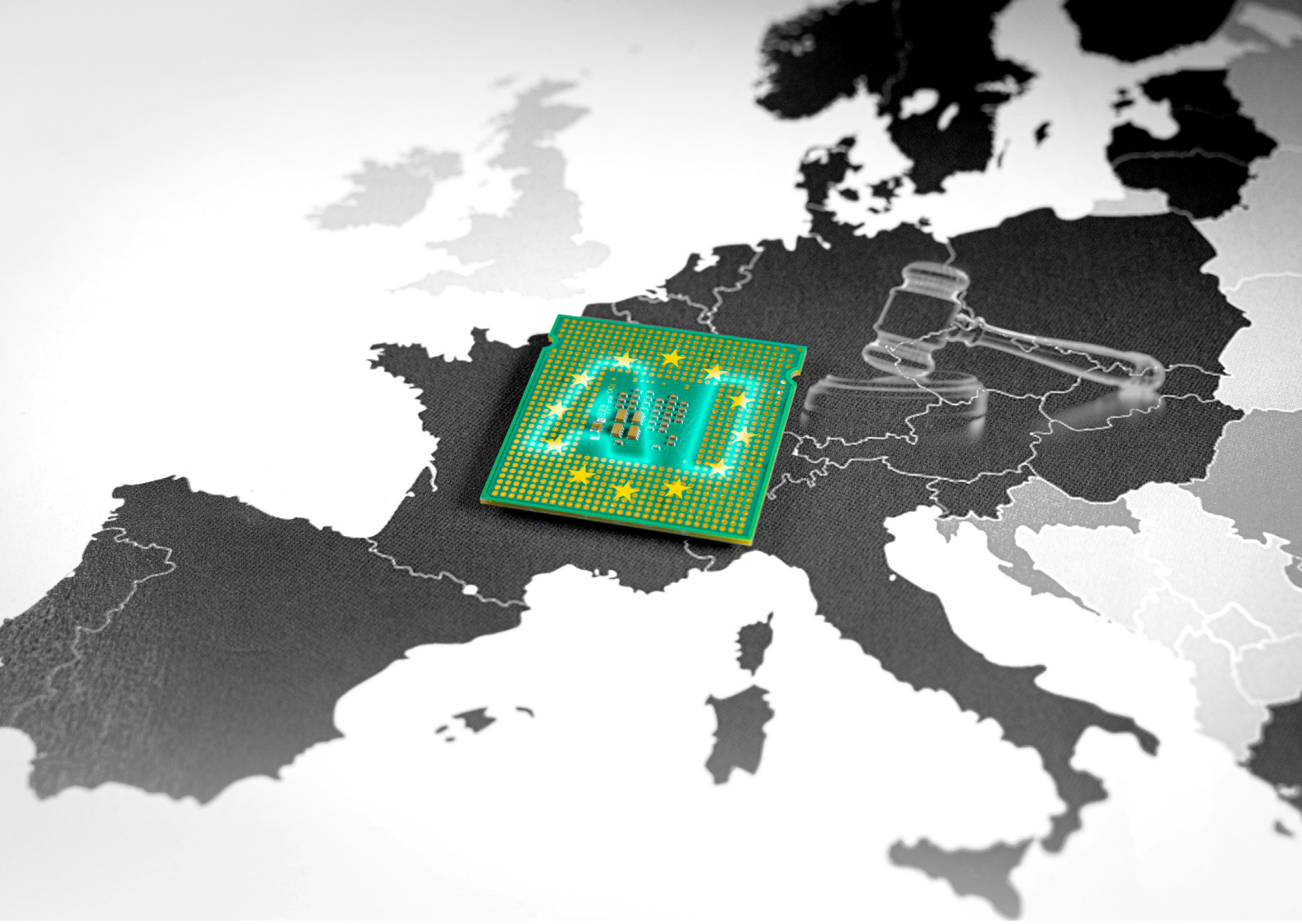


● Whitepaper

The EU AI Act: Time to accelerate your AI ambitions

eraneos

Contents

Executive Summary 03

Why is the AI regulation relevant for European government agencies or companies? 04

If your recruiter is an algorithm 06

Why AI is different and how the EU plans to respond 07

The importance of good preparation for companies 10

How to comply with the AI regulation 12

AI: Your co-pilot in regulatory compliance 15

Talk to our experts 17

Contact 18

Executive Summary

This whitepaper offers a comprehensive overview of the EU AI Act, which came into effect in August 2024, and explores its wide-ranging implications for organizations across various sectors.

The regulation introduces a binding legal framework for AI applications, including customer service chatbots, large language models (LLMs) like ChatGPT and Claude, and AI assistants such as Microsoft Copilot. Its core focus is on transparency, fairness, and accountability, requiring organizations to document decision-making processes, manage data responsibly, and address algorithmic bias.

The AI Act classifies AI systems based on risk - ranging from minimal to unacceptable -and imposes strict obligations on high-risk applications, particularly those used in recruitment, finance, and other critical domains. Organizations operating such systems must ensure robust documentation, monitoring, and governance practices. With enforcement phased in between 2025 and 2026, early preparation is essential to reduce legal exposure and gain a strategic advantage.

To support organizations facing this regulation, we've introduced an AI Assessment Framework. This framework guides organizations in assessing regulatory requirements, evaluating their AI maturity, and implementing a structured compliance strategy.

We also explore how AI itself can be leveraged to support compliance, including through document management, risk analysis, and operational tools.

Ultimately, effective AI governance relies not only on technology but also on strong data quality, ethical oversight, interdepartmental collaboration, and continuous improvement. By aligning early with the EU AI Act, organizations can navigate regulatory complexity while unlocking the full potential of responsible AI adoption.



Katharina Fulterer
Partner - Data & AI
Eraneos

Katharina.Fulterer@eraneos.com

Why is the AI regulation relevant for European government agencies or companies?

It is impossible to imagine daily life without artificial intelligence. Many organizations are already using artificial intelligence to support their employees in making daily tasks and processes more efficient. Innovations such as the car, the mobile phone, the internet and the cloud have shown how quickly new technologies become necessary. Eraneos expects dependence on AI to increase rapidly because it offers a competitive advantage. However, the implementation of AI also carries risks. For this reason, the European Commission has drawn up the AI Regulation.

In an increasingly competitive market, the use of AI is slowly shifting from an interesting possibility to an absolute necessity. Companies must observe the measures of the AI regulation to prevent problems such as unethical use of AI, restrictions in data collection and processing, or wrong and unexplainable decisions. Moreover, violations of the AI law can result in hefty fines. It is therefore crucial to fully understand what this regulation means for your company.

How far along are you? The AI regulation has already entered into force. From February 2025, the provisions on prohibited practices will come into force and organizations that use AI will be required to promote AI literacy. More and more parts of the regulation will come into force in the coming years. Use this time to make the right decisions that suit your company and technical situation. Let's take a closer look at how this can work out specifically for your company.

How to deal with ChatGPT?

Since the introduction of the AI regulation in 2024, it has been clear that the use and development of AI in the EU and beyond will change significantly.

Organizations that use LLM within the EU must be transparent about the entire process, from data collection to the final results.



In almost all companies where AI is not completely banned or blocked, employees often use ChatGPT as a useful tool in their daily work. Other providers of large language models (LLMs) such as Claude and Anthropic are also popular. Their interfaces are often integrated into various organizational and technical processes, such as sales and marketing content creation or text summarization. But to what extent do the new rules actually affect the „normal" users of LLM?

These users do not need to document the tool's decision-making process, such as how it predicts word order. But even people who use it only occasionally will notice that some things have changed due to the new rules:

- Organizations using LLMs within the EU must be transparent about the entire process, from data collection to final results. For example, a process description needs to be created that identifies the LLM. It is important that the legal obligations of the AI system itself are understood, as well as the obligations arising from its specific use, whether this is due to contextual changes or new legal requirements due to combinations of processing.

- Generative AI must inform users about AI interactions, prevent content that violates EU law, and disclose information about the training data. This leads to restrictions that companies need to be aware of to avoid legal issues such as copyright infringement.

- Companies need to prepare for the AI regulation by making AI governance part of their product strategy, identifying AI applications, classifying AI technology by risk, and being transparent about the use of AI. This approach requires openness and proactive planning to comply with the AI Regulation.

It is clear that simply relying on the manufacturer or supplier of an AI solution does not relieve a company of its legal obligations. Companies must properly assess their use of AI themselves, including documenting, classifying, and taking appropriate action based on the level of risk. Let's look at an example of a high-risk application situation to see what the consequences are.

If your recruiter is an algorithm

Let‘s look at an example where AI assistants are becoming more prevalent. Every day, a recruiter looks at countless resumes, compares qualifications, and conducts initial interviews to find candidates who match the company‘s needs. This painstaking process requires distinguishing the right mix of skills and experience from a large pool of candidates. Automating this task could significantly streamline the search for the perfect candidate.

This is already happening. AI applications are already transforming recruitment and selection by processing and analyzing vast amounts of candidate data. These systems automate the screening of resumes, match qualifications to job requirements, and manage communication with candidates. These algorithms evaluate candidates‘ experience and skills based on specific job criteria, which can improve the efficiency of the hiring process.

The use of AI in hiring also carries the risk of reinforcing biases. Algorithms trained on historical data can pick up on old prejudices, inadvertently favoring certain demographic groups and overlooking unique qualities in candidates that cannot be quantified. Strict requirements have been set for such high-risk applications under EU AI legislation:

- A comprehensive risk assessment of the AI-driven recruiting system must be performed to identify potential biases, inaccuracies, or unfair practices. Ongoing monitoring and updates are required to address these inherent risks.
- The data used to train the AI model must be diverse and represent all demographics. It is important that candidate data is protected with strict measures.
- Detailed documentation of the AI recruitment tool is mandatory, including the methods for processing applications, the criteria for making decisions, and the rationale for those decisions. This documentation should be accessible to stakeholders and regulators as necessary.
- A human review process should be implemented to oversee the AI system‘s hiring recommendations, allowing HR professionals to adjust the AI‘s decisions as necessary.
- Where required by law, the AI recruitment tool must be registered with relevant regulatory bodies, and candidates must be informed that an AI system is assisting in the processing of their applications.
- In order to detect potential bias or unfairness, the tool must be extensively tested with various mandatory data sets before it is implemented. This process must be ongoing to account for changes in the labor market and diversity goals.

This example shows that while AI can lead to significant cost savings, it also brings with it various obligations. However, complying with these regulatory requirements opens the door to new risk management opportunities, enabling organizations to make more thoughtful and robust decisions.

In addition, the implementation of AI can be integrated into existing processes, such as those for GDPR compliance. In the remainder of this white paper, we develop an effective approach to complying with these directives that is specifically tailored to each organization‘s unique starting point.

Why AI is different and how the EU plans to respond



AI systems work very differently from humans; they learn from large amounts of data, which can sometimes lead to unexpected and undesirable results. Without malicious intent, these systems can incorporate and perpetuate biases that can increase social inequality and undermine fairness. In addition, some AI algorithms are so complex that they are difficult to understand and predict, which in turn creates accountability and transparency challenges. These problems are compounded when AI applications are used to make high-impact decisions. To address these challenges, the European Union has introduced the AI Regulation, which sets out rules to address these issues. The main objectives of the law include:

01.
Protect EU citizens from AI applications that could pose risks to their security or fundamental rights, such as privacy, non-discrimination and freedom of expression.

02.
Build public trust, which is crucial for the acceptance and widespread use of AI applications in society.

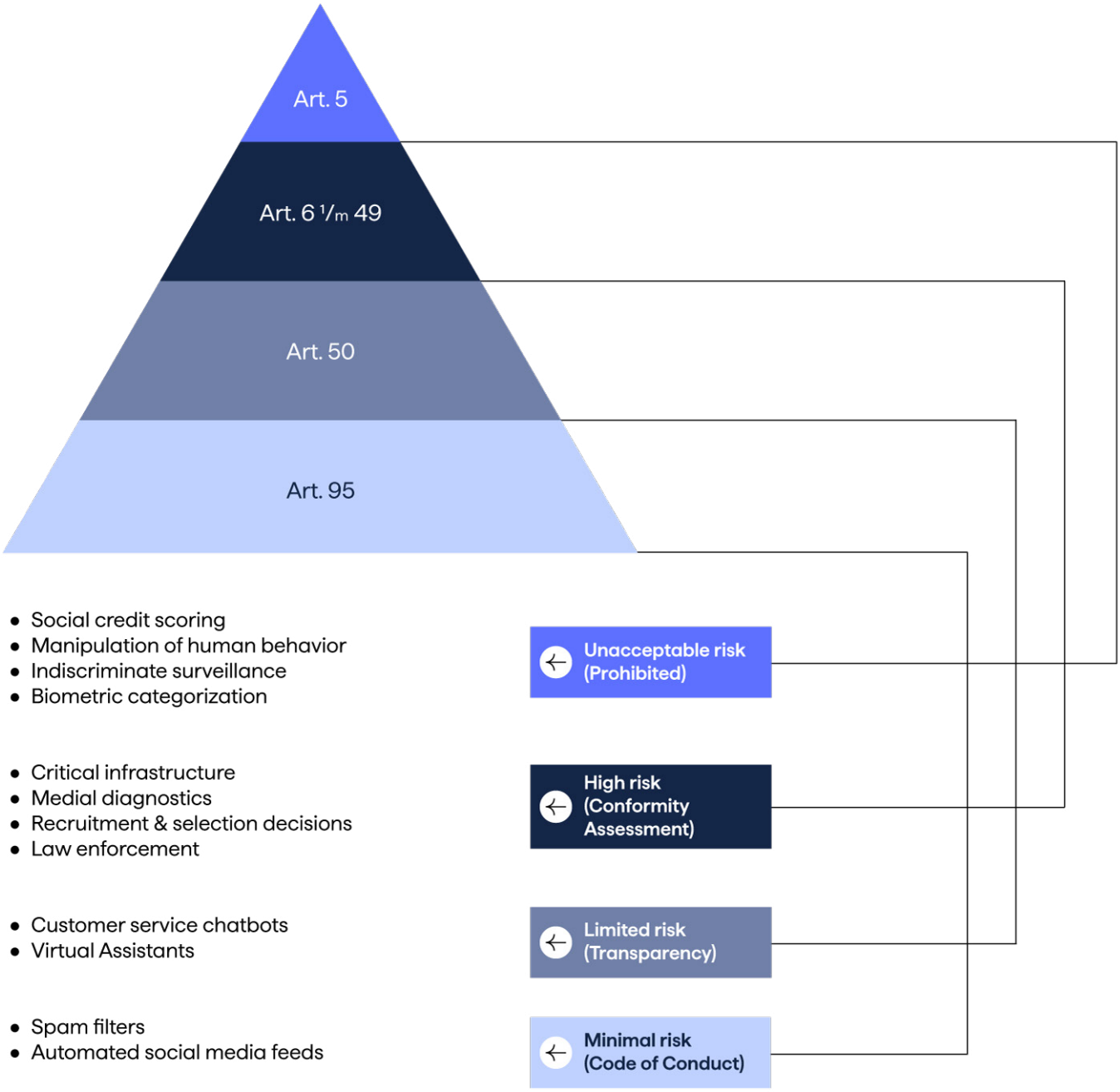
03.
Provide legal clarity for companies operating in the EU by establishing a harmonized regulatory framework for AI, which is essential to encourage investment in these technologies.

04.
Promote the development and adoption of AI in Europe to ensure that the EU remains competitive in the global technology landscape.

To achieve these goals, the AI Regulation classifies AI applications based on their level of risk, from minimal to unacceptable, and imposes strict requirements on high-risk systems to protect the public. These rules apply not only within the EU, but also impact providers and users of AI worldwide. The law applies to:

- Providers and distributors of AI applications in the EU
- Users within the EU, regardless of where the AI applications were developed
- Providers and users outside the EU if their AI applications are used within the EU

Therefore, almost all AI applications, whether already available or still under development, must fall into one of the following categories:





The regulation's implementation schedule is designed to allow for phased compliance:

- February 2025: Ban on AI applications with unacceptable risk and AI literacy requirements.
- May 2025: European Commission adopts codes of conduct for general AI applications.
- August 2025: Implementation of rules for general AI applications, designation of competent authorities by Member States, start of annual evaluations by the Commission and consideration of possible amendments.
- February 2026: Implementation guidelines for high-risk applications available, including post-market surveillance.
- August 2026: The rest of the AI Regulation is in force, except for AI systems that are high risk because they are a safety application of a regulated product (Article 6, paragraph 1).
- August 2027: Article 6① is also in force.
- December 31, 2030: Certain large-scale IT systems put into service before August 2, 2027 must comply with the AI Regulation.

Other national legislation is expected to follow.

The importance of good preparation for companies

The looming deadlines underscore the need for companies to act quickly. Compliance with the AI Regulation is demanding for organizations, often requiring them to fundamentally rethink their approach to implementing AI. Failure to comply can result in hefty fines, which can damage both the company's financial health and its image. Good preparation is essential, and surprisingly, AI can play a role in this, as we will see in the next chapter.

But early preparation offers more than just compliance-it offers a strategic advantage. Because compliance for AI systems that are already in use is more expensive and complex than for systems that are still in development, we advise companies to start preparing now.

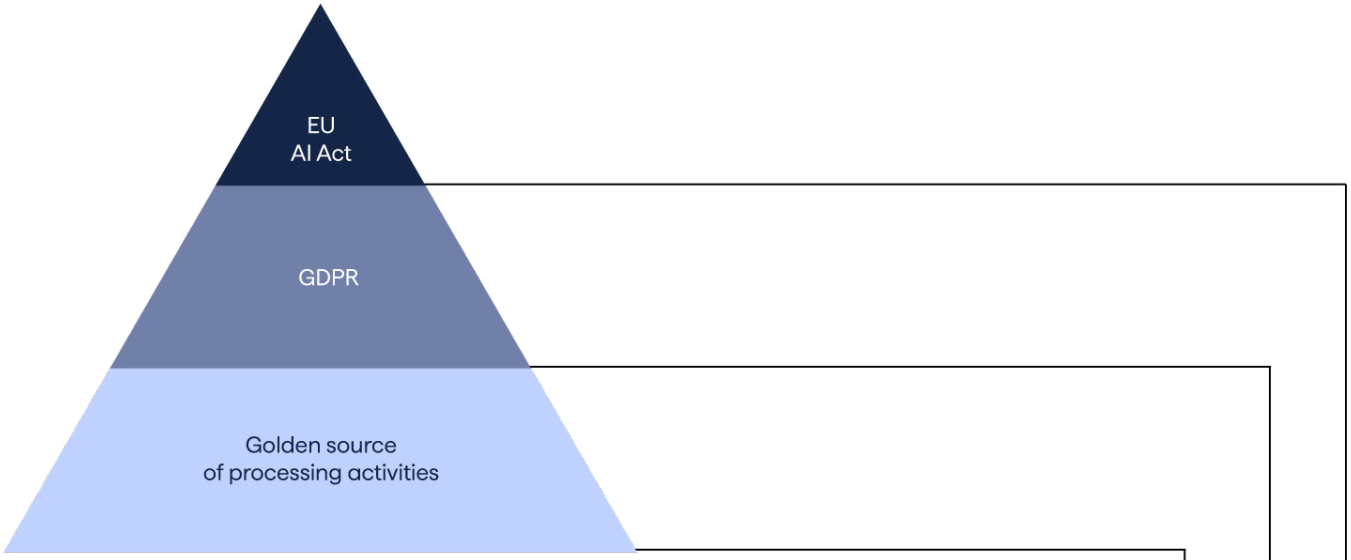
Companies that closely align their practices with legal standards will stand out in the marketplace and demonstrate that they take ethical AI seriously. Good risk management also helps to better identify and manage risks, which makes for a stronger and more sustainable business.

As the example of hiring shows, accurate and up-to-date documentation of AI and a central repository for AI activities are essential. Companies must establish risk management procedures that fit the AI Regulation's risk model to mitigate, accept, and document risks. AI activities must be categorized to ensure that all necessary steps and rules are followed. It is also important to not only assess at certain points in time, but to assess on an ongoing basis.

This requires regular assessment and monitoring of AI activities to address issues such as bias and incorrect results. It is also important to ensure that the use of data remains strictly necessary and compliant with regulations and ethical standards.

In addition, it is important to have a clear reporting system in place to manage and escalate risks associated with specific AI activities, particularly those that are high risk or in the event of a data breach. The diagram below illustrates the structure for meeting the legal requirements for data processing:

Contents of the modules:



Illustrative content of building blocks

- Introduce control and review regime of high-risk AI activities
- Implement continuous risk assessment
- Enhance existing DP questionnaires
- Update policies, review process & documentation regime

Specific requirements

- Repository of processing activities enhanced with data protection information (e.g. data transfers, data protection impact assessments)
- Review & Control process established
- Data protection policy implemented

Existing review & control elements

- Repository of processing activities within the company
- Process ID, Process Owner, Description, Data subjects & elements
- Tracking of last assessments, Link to documentation
- Reporting & Downstream availability for compliance activities
- Streamlined data base for all compliance activities

Basic requirements of compliance activities

Companies that align their working methods with the standards of the law stand out in the market and show that they take ethical AI seriously.

How to comply with the AI regulation

Organizations have until August 2026 to comply with the rules for high-risk applications. Failure to comply could result in fines of up to €40 million or 7% of annual revenue. Meeting these requirements, however, presents a number of challenges:

- Incorrect risk classification can lead to inadequate action being taken on certain AI systems.
- Inadequate documentation can lead to an inability to demonstrate compliance during audits, resulting in sanctions and business disruption.
- Inadequate data management can lead to data leaks, loss of user confidence, and hefty fines.
- Failure to meet the technical requirements of the law can result in costly remediation.
- Misunderstanding the rules can lead to non-compliant practices and penalties.

Implementing these measures is often complex and time-consuming. Companies need to plan their approach carefully, taking into account their specific situation.

Some companies require immediate action, while others can benefit from a phased implementation plan. To address these challenges, Eraneos has developed a compliance approach that includes an AI Assessment Framework. This framework provides:

- Guidance on regulatory requirements
- Assess the use of AI systems and the extent to which the regulations apply
- Assist organizations in understanding their current status in relation to the requirements of the regulations and determine the extent to which they are ready to comply.
- Analyze organizational maturity to set priorities
- Thoroughly evaluate specific AI systems based on the requirements of the regulation.

This framework builds on lessons learned from previous regulations, such as the implementation of the GDPR. It includes best practices and templates developed with input from technical and legal experts. These templates provide an objective basis for assessing the impact of new regulations on business objectives and product development. Experience has shown that the involvement of an independent party is extremely helpful. This avoids conflicts and ensures a smooth transition to compliance.

Implementation of the EU AI Act as a handy three-phase model

	Screen & Assess	Cluster & Plan	Mobilize & Anchor
Targets	• Regulatory landscape • Initial Assessment	• Requirements priorization • Risk-based implementation plan	• Operating Model implementation • Handover to business
Activities	• Analyze legal interpretation of the EU AI Act • Update of regulatory landscape • Map regulatory endeavors to business plan • Assess and cluster requirements • Assess maturity regarding implementation of related regulations (e.g. GDPR) • Identify processing activities that involve AI • Document AI-maturity assessment	• Map requirements to processes and evaluate impact (regulatory matrix) • Develop AI classification regime • Define effort and risks • Assess dependencies & define responsibilities • Revise Target Operating Model based on assessment results	• Adopt new governance • Establish new operating model • Update policies & controls based on AI risk classification regime • Apply new risk classification regime • Test new processes, measures & conditions • Conduct relevant Training & communication measures • Establish continuous risk assessment & AI oversight
Added value	• Transparency on AI-maturity • Joint view on feasibility and priorities	• High-risk activities covered first (e.g. priorities and dependencies identified) • Simplification of review processes and leveraging existing information (e.g. GDPR)	• Risks managed and monitored based on robust risk & control framework • Compliance with EU AI Act, positively impacting the reputation

Eraneos has developed an effective and simple phase model for a structured implementation of the requirements of the EU AI law. The model consists of three phases: Screen & Assess, Cluster & Plan and Mobilize & Anchor. Depending on the company's starting point, it is not always necessary to go through all the steps. As we saw in the previous chapter, AI itself can play a role in streamlining the compliance process at any stage.

Chapter quote: Establishing continuous risk assessment and monitoring of AI ensures that the organization is always in compliance with AI law.



Screen & Assess Phase:

This first phase lays the foundation for successful implementation by gaining a clear understanding of the regulatory landscape. This includes analyzing how the AI regulation is being interpreted, periodically reviewing regulations, and linking them to the business plan. This phase also includes mapping and clustering requirements, assessing how well the organization is prepared for AI-related regulations such as GDPR, and identifying processes where AI plays a role. The value of this phase is in assessing the maturity of compliance, and laying a solid foundation for further project planning.

Cluster & Plan Phase:

This phase is about organizing and preparing for action. Requirements are clustered and a risk-based implementation plan is created. This means creating a matrix of issues and expected impacts, and carefully classifying AI systems. Efforts and risks are identified, dependencies are analyzed, and responsibilities are clearly assigned. The goal is an efficient, targeted, and practical implementation plan, with a focus on high-risk activities so that they can be addressed quickly and effectively.

Mobilize & Anchor Phase:

The final phase is about executing the plan, implementing the operating model, and business handover. This includes establishing project governance and updating policies and controls. New processes are tested, followed by training and communication to embed the changes in the organization. Establishing ongoing risk assessment and monitoring of AI ensures that the organization is always in compliance with AI law. The result is an organization that is better prepared for success, more resilient, and has a solid risk management and control framework.

AI: Your co-pilot in regulatory compliance

Organizations today face an ever-changing regulatory landscape, from privacy regulations and sustainability mandates to industry-specific compliance frameworks. In this climate, AI has become a valuable ally, able to quickly analyze complex regulatory documents, identify compliance gaps, and reduce manual effort. By streamlining compliance efforts, AI enables teams to focus on strategic, value-added tasks instead of getting bogged down in repetitive reviews and administrative work.

At Eraneos, we see in practice how AI creates new efficiencies while maintaining strict standards across industries. Our experience shows that the best AI solutions fit seamlessly into existing regulatory and operational processes, ensuring flexibility and transparency. Below, we outline how organizations can use AI to proactively comply with regulations and reduce time-to-market risks.

Key AI-driven Opportunities:				
01.	**Document and contract management**	a. Automated summaries: AI quickly scans large volumes of regulations, laws and contracts and extracts the relevant clauses. This allows compliance teams to focus on risk assessment and decision making.	b. Drafting and generation: AI uses previous contracts and existing policies to draft initial versions of documents with standard clauses. This reduces repetitive drafting and helps identify potential compliance issues early.	c. Real-time updates: AI tools signal changes as soon as regulations change. This prevents outdated clauses from creating legal or financial risks.
02.	**Compliance and Risk Analysis**	a. Gap analysis: AI compares regulations with internal processes and quickly identifies missing or conflicting components. This makes it easier to expand into new markets.	b. Risk prioritization: Machine learning models assess the severity and likelihood of specific compliance risks. This allows you to focus resources where they are most needed.	c. Proactive action: Based on historical data and industry benchmarks, AI suggests targeted improvement actions - from policy adjustments to early intervention.
03.	**Operational AI Tools**	a. Knowledge bases and chatbots: Internally, AI chatbots provide instant answers to policy questions, making employees less dependent on specialist teams. Externally, they answer compliance questions from customers and provide consistent and reliable information.	b. Supplier assessments: AI analyzes supplier data such as certifications, performance, and costs. This makes it easy to select reliable partners that meet compliance requirements and contribute to ethical and sustainable goals[YT1].	



Building effective AI-driven compliance solutions

While AI offers many opportunities for compliance and risk management, success does not depend on technology alone. The following considerations will ensure that AI-driven regulatory solutions remain agile, transparent, and well-aligned with the changing regulatory landscape:

01.
Data quality and governance: AI is only as good as the data it operates on. Organizations must ensure that regulatory texts, contracts, and operational data remain clean, accurate, and up-to-date.

02.
Interdepartmental collaboration: AI compliance solutions often span multiple departments, such as legal, finance, IT, and operations. By collaborating effectively, teams can combine insights and get the most out of AI.

03.
Human oversight: AI can perform repetitive tasks and identify patterns, but human expertise is still essential when making important decisions. Think of AI as a support, not a replacement, for human expertise.

04.
Ethical and privacy considerations: AI systems must comply with data privacy laws (such as GDPR and HIPAA), and adhere to ethical standards for data use. Transparency about how AI processes and interprets data builds trust.

05.
Continuous improvement: Regulations are constantly changing. Therefore, AI models must be regularly updated and improved to stay current and quickly respond to new laws and business needs.

AI can significantly improve the way organizations address compliance, reduce manual work, and identify risks early. By combining AI with good data governance, ethical policies and human oversight, organizations can build flexible compliance frameworks that adapt to changing regulations. At a time when non-compliance can result in financial or reputational damage, AI is no longer just useful, it has become essential.

Talk to our experts

Eraneos specializes in cybersecurity, resilience, risk management and privacy, and helps companies navigate the dynamic landscape of AI and cybersecurity to safeguard their activities and thrive in a digital world. Are you ready to maximize the potential of AI tools while implementing robust security measures? Contact Eraneos today for more information on how we can help you use AI technologies safely and effectively, support you in activities in the field of threat analysis and risk management and/or help you to continue to comply with, for example, the AI Regulation or the GDPR.

Our Experts:



Katharina Fulterer
Partner - Data & AI
Eraneos

Katharina.Fulterer@eraneos.com



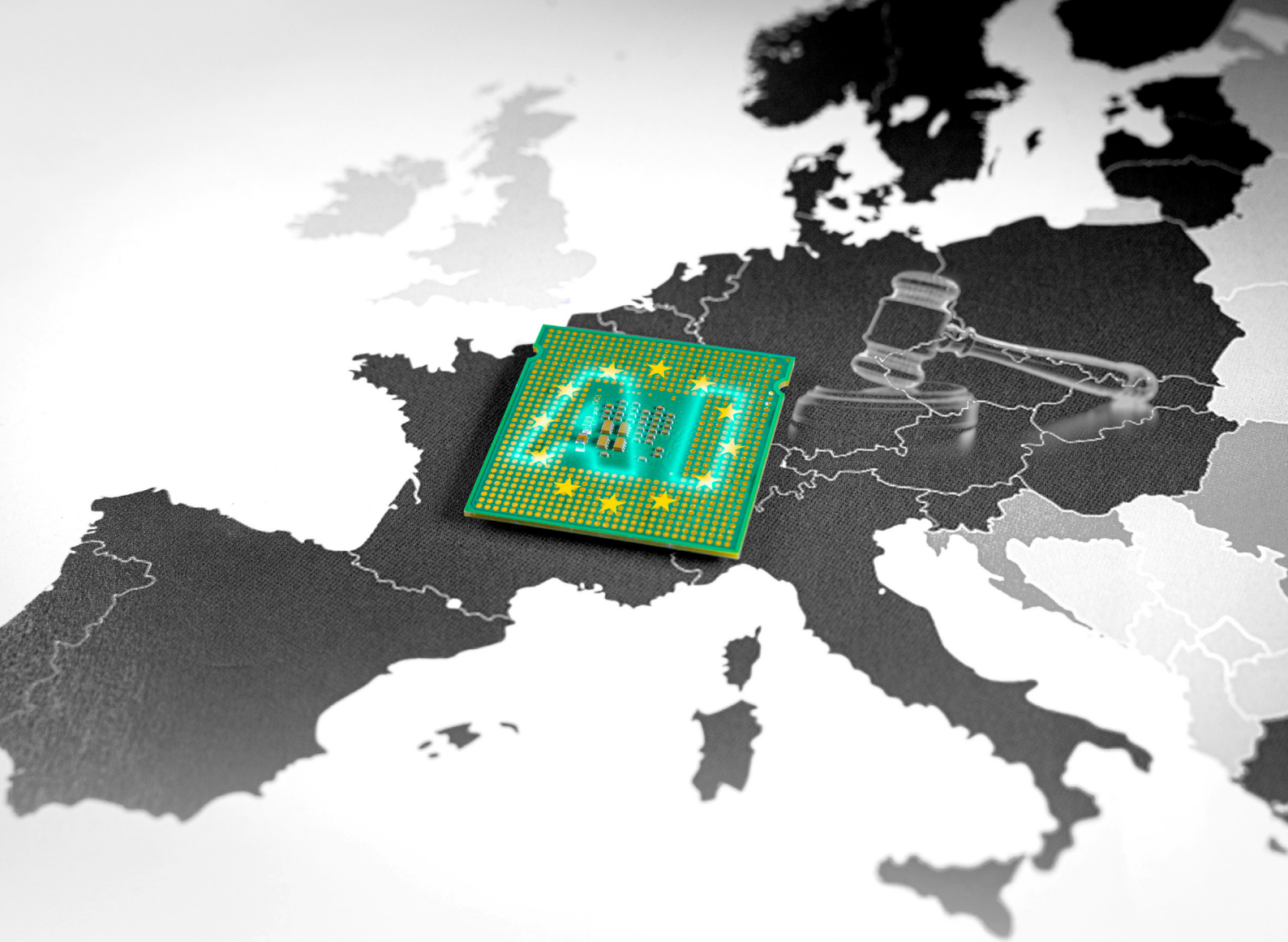
Roman Regenbogen
Senior Manager - Financial Services
Eraneos

Roman.Regenbogen@eraneos.com



Adrian Anderegg
Partner - Private Industries

adrian.anderegg@eraneos.com



Get in touch

Katharina Fulterer
Partner - Data & AI
Eraneos
Katharina.Fulterer@eraneos.com

Roman Regenbogen
Senior Manager - Financial Services
Eraneos
Roman.Regenbogen@eraneos.com

Adrian Anderegg
Partner - Private Industries
Eraneos
adrian.anderegg@eraneos.com

Eraneos Switzerland AG
Andreasstrasse 11
CH-8050 Zurich
+41 58 411 95 00
info.ch@eraneos.com
eraneos.com/ch