

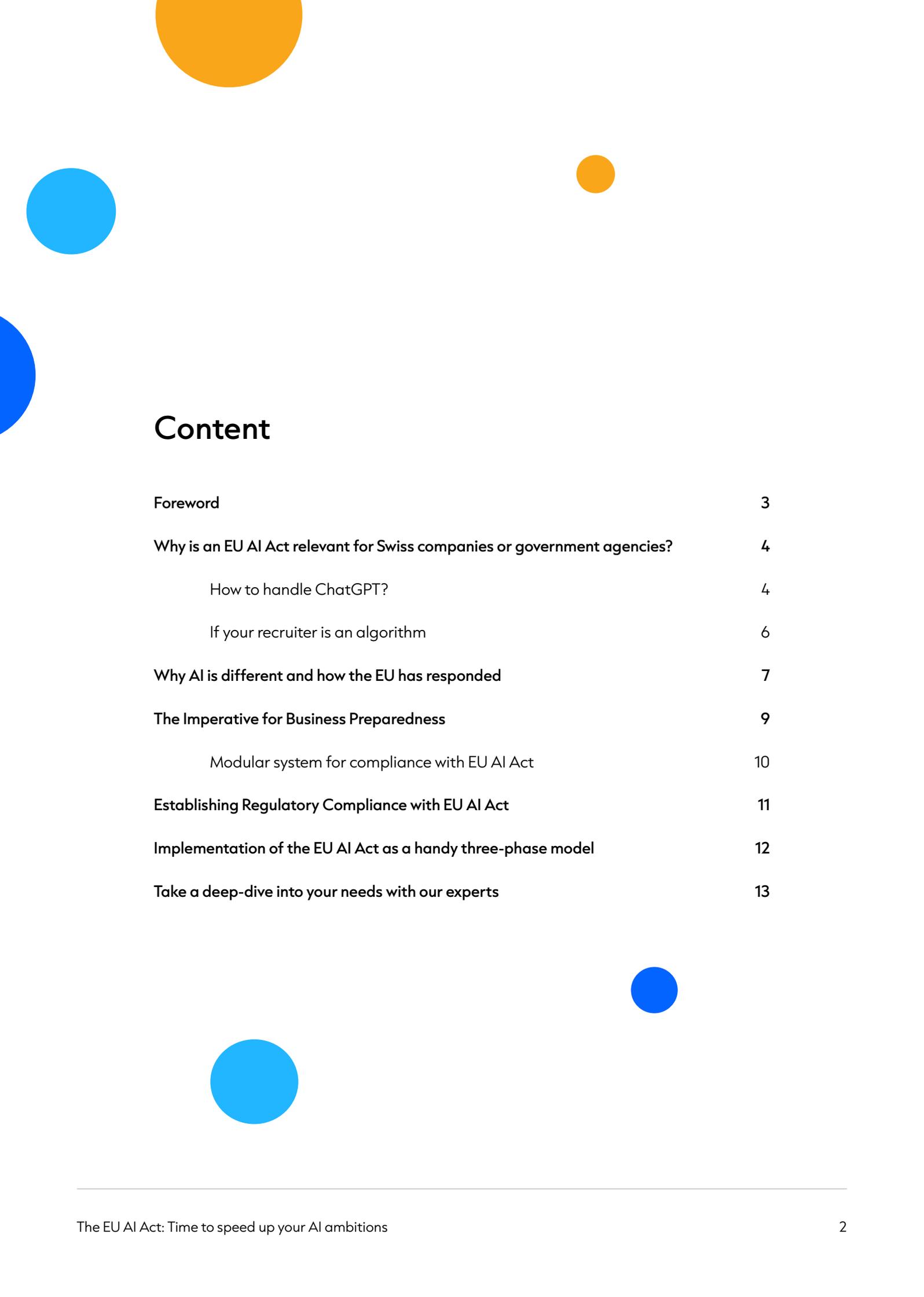
eraneos



Whitepaper

The EU AI Act: Time to speed up your AI ambitions

July 2024



Content

Foreword	3
Why is an EU AI Act relevant for Swiss companies or government agencies?	4
How to handle ChatGPT?	4
If your recruiter is an algorithm	6
Why AI is different and how the EU has responded	7
The Imperative for Business Preparedness	9
Modular system for compliance with EU AI Act	10
Establishing Regulatory Compliance with EU AI Act	11
Implementation of the EU AI Act as a handy three-phase model	12
Take a deep-dive into your needs with our experts	13

Foreword

Do you already have concerns about the EU AI Act? From the conversational nuances of a customer service chatbot to the intellectual assistance of ChatGPT, and even the sophisticated support of Microsoft's Copilot: the Act will lay down base regulations and requirements for all these platforms and use cases. They will now operate under stringent regulatory frameworks that everyone must abide by – also relevant for most of Swiss companies and governmental bodies. But what does that mean?

- Chatbots, designed to streamline customer service, will face new transparency directives, ensuring users are aware of their AI-driven nature. This requirement will not only change user interactions but also how these systems are designed and the extent to which they can be deployed.
- ChatGPT, the more complex AI known for generating human-like text, will require rigorous documentation of its decision-making processes and mitigation of biases, demanding deeper scrutiny into its training data and algorithms.
- Microsoft's Copilot, an AI-driven office assistant, will necessitate enhanced transparency, meticulous data handling, and strict compliance checks. One could continue this list with all systems using AI, a consistently growing number after all.
- Besides these examples, AI will be used to expedite, simplify and harmonize recruiting, finance, marketing or product offering procedures with many different Standard or Self-Developed AI Solutions. This upcoming cosmos of new Solutions will also have to follow the EU AI Act.



Why is an EU AI Act relevant for Swiss companies or government agencies?

The EU AI Act is highly relevant to Swiss companies and government agencies because it affects providers and distributors of AI systems within the EU, applies to EU-based users of AI systems regardless of the system's origin, and affects providers and users outside the EU when their AI system outputs are used within the EU. As a result, Swiss companies must understand and comply with these regulations to ensure that their AI systems can be effectively deployed and used within the European Union.

Are you prepared for this? The EU AI Act has now been ratified, but there is still time before it becomes legally effective. However, until then,

it is important to use the time and make the right decisions, which depend on your specific business and the technical setup in place. Let's dive a little deeper into the topic to see exactly how it could affect your business.

How to handle ChatGPT?

Following the adoption of the EU AI Act in March 2024, it has become clear that the development and use of AI in the EU (and abroad) is about to change. In almost all companies that have not completely banned or blocked its use, ChatGPT is now either occasionally or even systematically used by employees as a useful tool in everyday life. In addition, the system's interfaces may already be integrated into other processes in organizational and / or technical terms (e.g. sales processes, generation of marketing content, summarization of texts). But to what extent do the new regulations affect the "normal" users of ChatGPT at all?



After all, they do not, for example, have to document how the tool arrives at its decisions (i.e. its sequence of probable words). Even if this is true, "simple" users will also notice the new legislation in the following changes:

- Entities in the EU using AI systems like ChatGPT must ensure transparency in their usage, from data collection to impact. This involves creating a process flow that includes ChatGPT and understanding both the legal obligations of the AI system itself and those arising from its specific application, whether through contextual changes or new legal obligations due to processing combinations.
- Generative AI is required to inform users of AI interactions, prevent content that breaches EU laws, and disclose training data usage. This leads to content restrictions that could affect business processes, highlighting the need for vigilance against potential legal issues such as copyright infringements.
- Businesses must embed AI governance into their product strategies, readying for the AI Act by identifying AI use cases, classifying AI technologies by risk, and enhancing transparency. This approach demands a shift towards greater disclosure and proactive compliance planning with the AI Act.

One can easily tell that the mere reference to the manufacturer or provider of an AI solution does not exempt a company from the legal responsibility to assess its own context of use in terms of documentation and classification and to take appropriate measures according to the criticality levels. Let's take a closer look at a high-risk example and see what the responsibilities are.



If your recruiter is an algorithm

A recruiter starts each day by sifting through a mountain of resumes, each a gateway to a potential new hire and identifying the nuanced web of skills and experience that matches the company's needs. They compare qualifications, conduct initial interviews and try to find the right person for the right job as they work their way through the crowd of applicants to find the hidden gems. Wouldn't it be great if this task could be automated by a machine?

That's exactly what's already happening: AI applications are applied in recruitment and employment decisions and involve processing and analyzing large volumes of applicant data.

These systems can automate the screening of resumes, match qualifications with job requirements, and manage communications with applicants. AI algorithms are used to evaluate candidates' experiences and skills against specific role criteria, potentially improving the efficiency of the recruitment process.

However, their downside is the risk of embedding and perpetuating bias in the hiring process. Algorithms trained on historical data may inherit past biases and inadvertently favor certain demographics over others. In addition, unique candidate qualities may be overseen, as algorithms cannot quantify those. Irrespective of technical considerations, the EU AI Act places high demands on the use of such a high-risk application in any case:

- You need to conduct a thorough risk assessment for the AI-driven recruitment system to identify potential biases, inaccuracies, or unfair practices. Additionally, you need to continuously monitor and update the system to mitigate those inherent risks.
- The data used for training the AI recruitment tool must be diverse and representative of all demographics. Implementing strict data handling and protection measures (that is data governance) to safeguard applicants' personal information is key.
- You must maintain detailed documentation about the AI recruitment tool, including how it processes applications, the criteria it uses for decision-making, and the logic behind these decisions. This documentation should be accessible to stakeholders and regulatory bodies if required.
- Setting up a human review process to oversee the AI system's recommendations for recruitment and employment decisions is required. Human HR professionals should have the ability to override AI decisions when necessary.
- If required by law, you must register the AI recruitment tool with the appropriate regulatory bodies and notify candidates that an AI system assists in processing their applications.
- Before deployment, it is mandatory to carry out rigorous testing with diverse datasets to check for any bias or unfairness in its recommendations. This process should be ongoing to adapt to changes in the job market and diversity goals.

This example illustrates that the huge savings potential offered using AI comes with various obligations. However, implementing these legal obligations unleashes new potential to perform risk management, enabling businesses to draw better and more resilient conclusions.

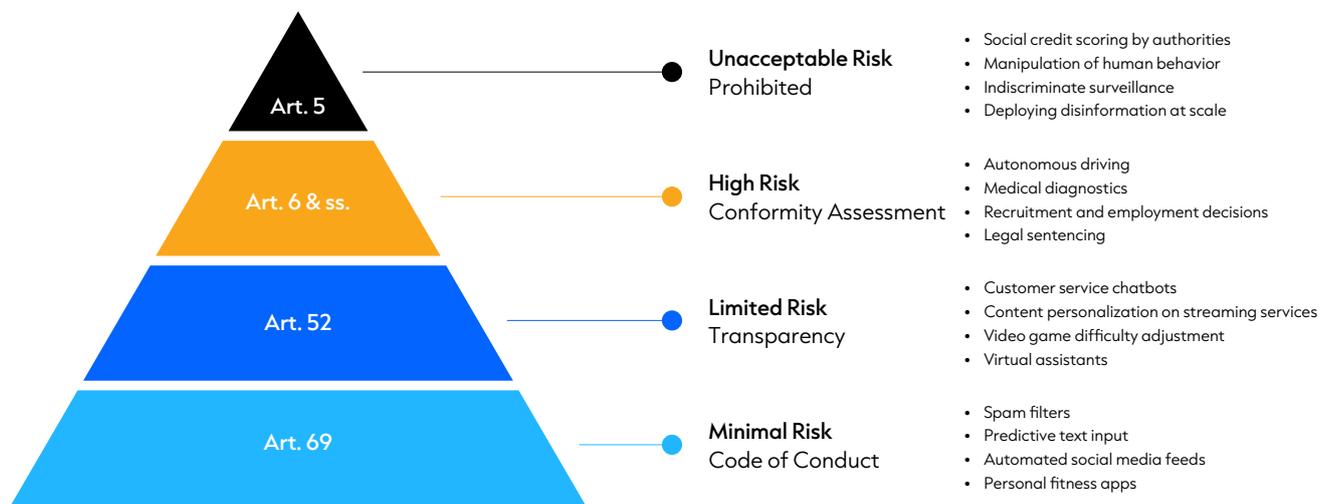
Furthermore, their implementation can be based on existing processes, e.g. as part of existing GDPR implementations. In the remainder of this whitepaper, we will present an approach that allows the guidelines to be mapped efficiently, considering the individual starting conditions.

Why AI is different and how the EU has responded

AI systems, by their very nature, learn and make decisions in ways fundamentally different from human reasoning. This divergence can lead to unexpected (and unwanted) results, as AI models follow their own logic derived from underlying large datasets. Training of AI models can inadvertently encode and propagate biases, perpetuating societal inequalities and undermining fairness. Furthermore, the opaque nature of some AI algorithms makes it challenging to understand and predict their behavior, raising concerns about accountability and transparency. All these shortcomings are compounded when these systems are used to make decisions at scale. This is why the European Union has recognized the urgent need for a regulatory framework such as the EU AI Act. The primary goals of the Act are:

1. To protect EU citizens from AI systems that might pose risks to their safety or fundamental rights, including privacy, non-discrimination, and freedom of expression.

2. To build public trust which is seen as crucial for the acceptance and widespread use of AI applications in society.



3. To provide legal clarity for companies operating in the EU by offering a harmonized regulatory framework for AI, which is a prerequisite for investment in these technologies.

4. To promote the development and uptake of AI in Europe, ensuring that the EU remains competitive in the global technology.

To achieve the above goals, the EU AI Act categorizes AI systems based on their risk level, from minimal to unacceptable risk, and imposes requirements on high-risk applications to protect the public interest. Its regulatory reach extends beyond the EU borders, affecting AI system providers and users worldwide. Its jurisdiction encompasses:

- Providers and distributors of AI systems within the EU
- EU-based users of AI systems, regardless of the system's origin
- Providers and users outside the EU, if the AI system's outputs are used within the EU

This means that basically all AI systems available or to be developed are covered and must be classified in one of the following categories:

The implementation timeline of the Act is structured to ensure a staggered approach to compliance:

- **November 2024:** Enforcement of prohibitions on AI practices classified as posing unacceptable risks.
- **February 2025:** Establishment of codes of practice for General Purpose AI.
- **May 2025:** Application of General Purpose AI rules, designation of competent authorities by Member States, initiation of annual Commission reviews, and potential amendments.
- **November 2025:** The Commission's issuance of implementing acts to standardize high-risk AI providers' post-market monitoring plans.

It goes without saying that legal requirements and acts on a national level will follow, detailing the EU AI Act and possibly impose even stricter rules.



The Imperative for Business Preparedness

The approaching deadlines underline the pressing need for businesses to act swiftly. Adapting to the EU AI Act's requirements will demand significant effort, as organizations must reassess and, in many cases, revamp their AI deployment strategies. Failure to comply with the Act's provisions could result in substantial penalties, jeopardizing not only financial stability but also brand reputation.

However, beyond compliance, early preparation offers a strategic edge. Given the higher costs and complexities associated with ensuring compliance for AI systems once they are operational compared to during their development phase, we advise firms to begin their preparations immediately. Additionally, organizations that successfully align their operations with the Act's requirements can

differentiate themselves in the marketplace, showcasing their commitment to ethical AI practices. Last but not least, comprehensive and efficient implementation of risk frameworks enable businesses to better understand their risk exposure, ideally leading to a more resilient and sustainable operating model.

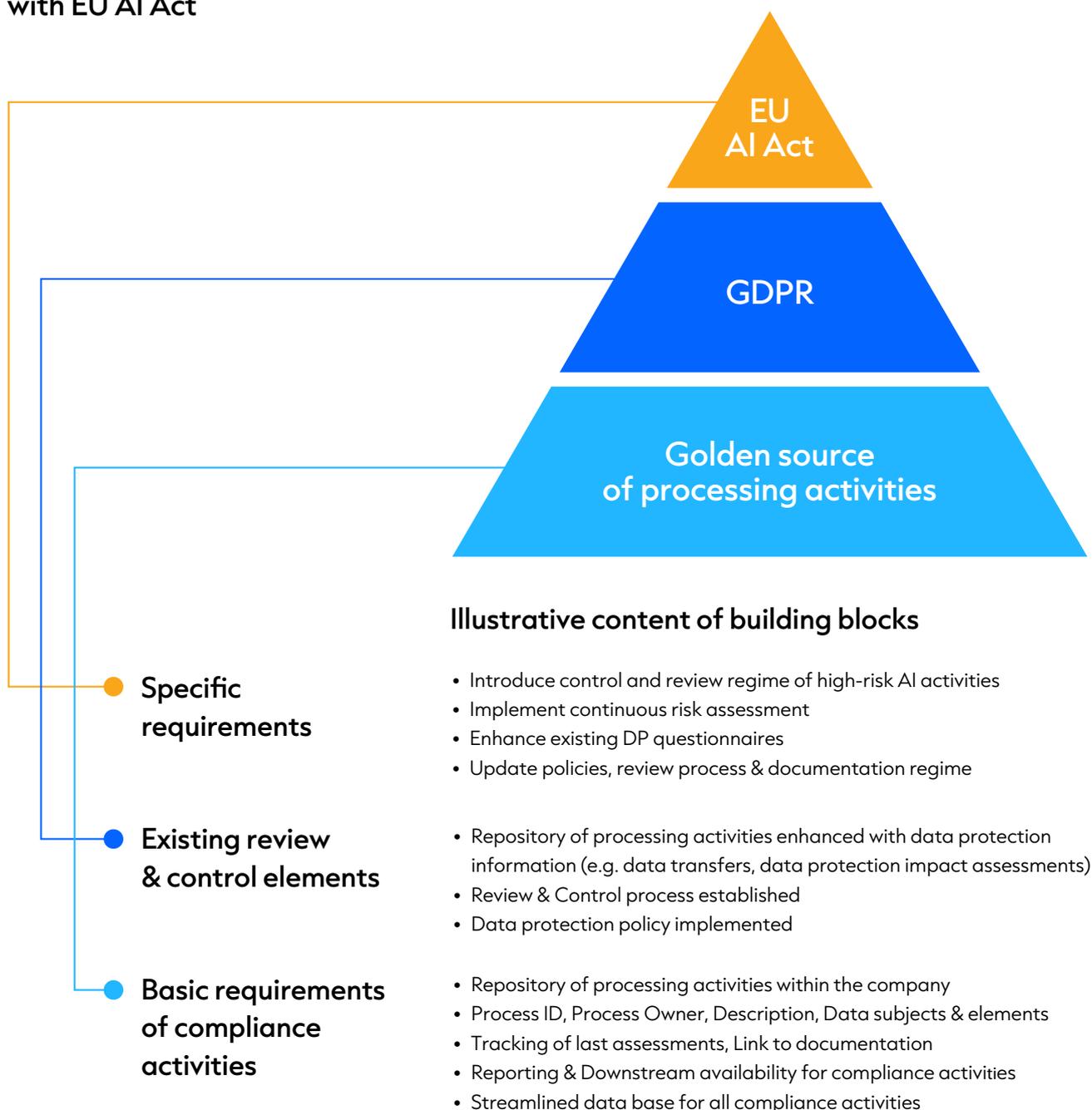
As already shown with the recruiting example, an accurate, up-to-date, and correct AI documentation as well as a centralized repository for AI activities is required. Risk management procedures must be set up in line with the EU AI Act's risk-based model to mitigate, accept, and document the inherent risks associated with the deployment of AI systems. AI activities must be categorized to take all necessary steps and regulatory compliance measures that need to be implemented. A paradigm shift is also required from a point-in-time assessment to a continuous assessment framework.



This means consistently reviewing and controlling AI activities to manage issues such as bias, incorrect conclusions, and ensuring that the purposes and amount of data usage are limited to what is absolutely necessary and aligned with ethical and regulatory standards.

Finally, a dedicated notification regime should be introduced to manage and escalate risks associated with certain AI activities, such as those classified as high-risk or in the event of data breaches. The following diagram shows the structure for the compliance of data processing processes along the legal requirements:

Modular system for compliance with EU AI Act



Cluster & Plan implementation of EU AI Act compliance based on single source of processing activities within the company

Establishing Regulatory Compliance with EU AI Act

As regulators finalize the last changes to the AI Act, organizations have until May 2026 to comply with the requirements for high-risk applications, or face fines of up to €40 million or 7% of revenue if they fail to do so in time. The specific challenges of meeting the requirements of the laws include:

- Mistakes in risk classification could lead to **underestimating the regulatory requirements** for certain AI systems, resulting in insufficient controls.
- Inadequate documentation practices might **fail to prove compliance** during assessments, risking sanctions and operational disruptions.
- **Poor data governance** could expose companies to breaches of sensitive data, undermining user trust and attracting hefty fines.
- **Technical misalignments** with the AI Act's requirements could necessitate costly re-engineering of AI systems post-deployment.
- **Insufficient legal guidance** might result in misinterpretation of the AI Act provisions, leading to non-compliant practices.

The systematic application of operative compliance changes is often a challenging and lengthy process. It is important to translate the implications into planning in a considered and targeted manner taking the specific characteristics of the company into

account. In some cases, it is important to start as quickly as possible, in others a gradual introduction of individual elements may be sufficient. Therefore, Eraneos developed a regulatory compliance approach including an AI Assessment Framework to::

- Help organizations navigate through the regulation's requirements
- Assess the use of AI systems and the extent to which the regulation applies
- Support organizations in understanding where they stand regarding the regulation's requirements and determine to what extent organizations are ready to comply with the regulation
- Assess organizational maturity and determine areas of prioritized focus
- Perform a deep dive on specific AI systems in view of the legal requirements set by the Act

Experience from various compliance mandates, such as the introduction of the GDPR, has been incorporated into the framework. Components of the framework are best practice processes and templates, which were also created and optimized on the basis of technical and legal expert knowledge. These templates, which are based on abstract principles, also make implementation more objective when it comes to the impact of new regulations on business objectives and product developments, for example. In general, it has been shown that an independent authority is very valuable in this adaptation process and helps to prevent later conflicts.

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



	Screen & Assess	Cluster & Plan	Mobilize & Anchor
Targets	<ul style="list-style-type: none"> Regulatory landscape Initial Assessment 	<ul style="list-style-type: none"> Requirements prioritization Risk-based implementation plan 	<ul style="list-style-type: none"> Operating Model implementation Handover to business
Activities	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Transparency on AI-maturity Joint view on feasibility and priorities 	<ul style="list-style-type: none"> High-risk activities covered first (e.g. priorities and dependencies identified) Simplification of review processes and leveraging existing information (e.g. GDPR) 	<ul style="list-style-type: none"> Risks managed and monitored based on robust risk & control framework Compliance with EU AI Act, positively impacting the reputation

Eraneos designed a proven but simple phase model for a “packaged” implementation of the requirements of the EU AI Act. It contains Screen & Assess, Cluster & Plan and Mobilize & Anchor. Depending on the company’s starting position, the phases may be different in complexity and effort.

Screen & Assess Phase:

This initial phase sets the groundwork for successful implementation by thoroughly understanding the regulatory environment. It involves analyzing the legal interpretation of the EU AI Act and conducting periodic reviews of the regulatory landscape to align it with the business plan. This stage is about screening, collecting and assessing new requirements regarding relevance, evaluating the company’s maturity in AI-related regulations (like GDPR), and identifying AI- involved processing activities. The value added in this phase is gauged by the assessment of compliance maturity and the groundwork laid out for a joint view on feasibility and priorities.

Cluster & Plan Phase:

Focus of the second phase is on organizing and preparing for action. Requirements are grouped and a risk-based action plan is formulated. Tasks include mapping requirements to the records of processing activities / the IT inventory, creating a regulatory matrix of AI requirements to be addressed and expected impacts on processes, and rigorously classifying AI systems. Efforts and risks are defined, dependencies are assessed for impact, and responsibilities are assigned to the relevant role within the company.

This phase aims for efficient, targeted, and business-friendly implementation, planning of critical requirements like the assessments for high-risk systems as well as prioritizing high-risk activities to address them promptly and effectively.

Mobilize & Anchor Phase:

The final phase focuses on implementing the operating model and transforming compliance from a mere requirement into a core asset.

This involves establishing organizational and operational governance, along with updating policies and controls. A testing phase for new processes is followed by comprehensive training and communication to embed these changes within the organization. Ongoing risk assessment and AI oversight will ensure continuous alignment with the AI Act. This approach results in an organization that is fully compliant with the EU AI Act, thereby enhancing its reputation and effectively managing risks through a robust risk and control framework.

Take a deep dive into your needs with our experts

Eraneos has a profound and long-lasting track- record of successfully completed compliance projects in various industries. For example, we played a pivotal role in advancing AI governance and compliance standards for a Swiss insurance company by conducting thorough assessments of AI use cases. In another instance, Eraneos supported a Swiss federal authority in developing a robust data protection and security framework, overseeing an extensive review of business operations. We also assisted a major Swiss bank in establishing a thorough data and records management system, enhancing accountability and efficiency in data protection.

So get in touch with us, we look forward to getting you ready for a compliant AI future.

Authors:



Bjorn Sieger
Head Privacy & Compliance
bjoern.sieger@eraneos.com



Roman Regenbogen
Head Regulatory & Compliance FS
roman.regenbogen@eraneos.com



Severin Kefer
Regulatory & Compliance Expert
severin.kefer@eraneos.com



Experienced in a wide range of industries

ABOUT ERANEOS SWITZERLAND AG

Eraneos Switzerland AG (formerly AWK Group AG) is an international management & technology consulting firm. It specializes in supporting its clients with the development of digital business models and complex transformation projects which enable clients to fully exploit the potential of digitalization.

As a member of the internationally networked Eraneos Group, which stretches from Switzerland, to Germany, Austria, The Netherlands, China, Singapore, and the USA, the firm ensures their clients retain access to the more than 1075 highly qualified experts, along with their extensive knowledge.

The unique combination of competencies in the areas of Strategy and M&A, Digital Business &

Innovation, Organizational Excellence & Transformation, Data & AI, Cyber Security & Privacy, Sourcing Advisory, IT Advisory, and Technology & Platforms is applied to all industries and sectors, enabling the firm to provide comprehensive support to a full portfolio of clients.

Local Swiss offices in Zurich, Basel, Bern and Lausanne employ over 500 professionals. Eraneos Switzerland AG is a repeated recipient of the "Great Place to Work" award.

[Contact us >](#)

[Our offices >](#)

[Visit our website >](#)