European Union AI Act in practice

What does it mean for your AI applications?

validio

Disclaimer

Since the law is not yet formally adopted, the validity of this content might change over time. This whitepaper is based on the European Union AI Act originally proposed in April 2021 together with the amendments made along the way. The contents of this whitepaper is not to be regarded as legal advice.

Contents

01 Introduction

Ever since ChatGPT launched publicly on 30 November 2022, AI has been on everyone's mind, and investments in and adoption of AI are at an all-time high. The same also holds true when it comes to regulation—governments across the globe are racing to regulate the powerful technology.

For example, the United Kingdom hosted the inaugural AI Safety Summit at Bletchley Park in November 2023 with political leaders invited from leading AI nations such as the US, China, and countries within the European Union. The following month, in December 2023, the European Union reached a provisional agreement on the law to govern AI within the union—the European Union AI Act (EU AI Act).

The EU AI Act is considered one of the most stringent AI regulations internationally, and follows a risk-based approach: the higher the risk, the stricter the rules. It is expected to be formally adopted by both the EU Parliament and Council to become EU law in early 2024. **Non-compliance with the EU AI Act can result in fines up to 35 mEUR or 7% of global annual revenue.** As a result, it is of high urgency for all businesses applying AI within the EU to be on top of the compliance work regarding the EU AI Act. That is what this whitepaper is here to help you with—let's dive in!

Risk regulation categories explained in chapter 3

02 Definition of AI

AI is a terminology with many different definitions and meanings. Given that the EU AI Act is regulating AI systems, it is important to first clarify its definition of AI. The EU AI Act has chosen to adopt a definition inspired by OECD's definition of AI, and reads as follows:

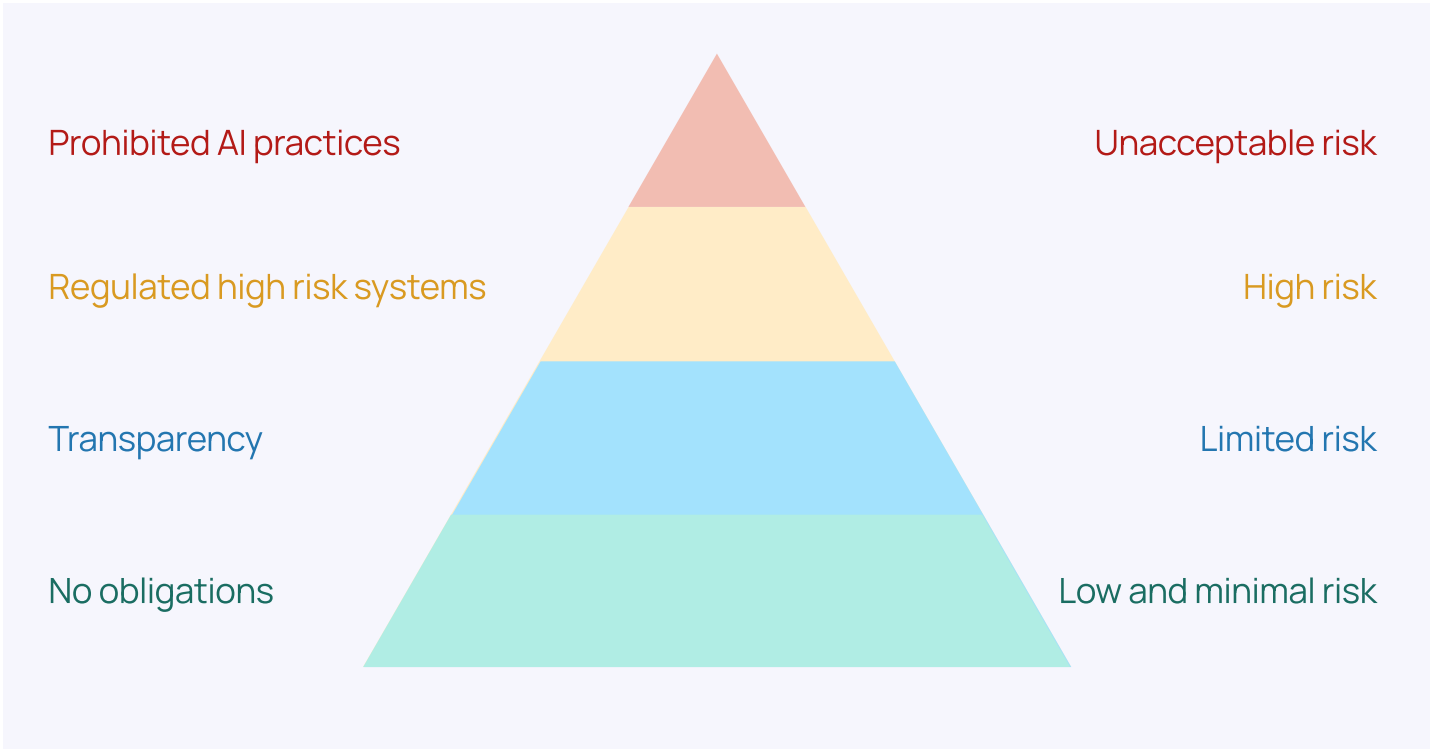
> "Artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches [listed in Annex I] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"
>
> The EU AI Acts definition of AI

03 Risk-based approach

The EU AI Act regulates AI applications through a risk-based approach, which essentially means: the higher the risk, the stricter the rules.

The risk categories are divided into the following; 1) Unacceptable risk, 2) High risk, 3) Limited risk and 4) Low and minimal risk. General purpose AI systems will also be included in- and governed by the law. These are AI systems, such as Large Language Models, that have a wide range of possible uses, both intended and unintended by the developers, often without the need of substantial modifications and fine-tuning.

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk



1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

Unacceptable risk applications - banned

The EU AI Act completely bans AI applications that pose an unacceptable level of risk. The following AI applications are deemed to be of unacceptable risk:

- AI systems that deploy harmful manipulative 'subliminal techniques'
- AI systems that exploit specific vulnerable groups (physical or mental disability)
- AI systems used by public authorities, or on their behalf, for social scoring purposes
- 'Real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except in a limited number of cases

Companies that have AI systems in any of these application areas will have to phase them out within six months after the adoption of the law to avoid breaches.

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

High risk applications - comprehensive requirements

AI use cases are regarded as high risk if at least one of the following two requirements are fulfilled:

1. AI systems used in products that are covered under the **EU's product safety legislation**, including toys, aviation, cars, and medical devices.

2. AI systems falling into specific areas that will have to be registered in an EU database:

- → Management and operation of critical infrastructure
- → Education and vocational training
- → Employment, worker management and access to self-employment
- → Access to and enjoyment of essential private services and public services and benefits
- → Law enforcement
- → Migration, asylum and border control management
- → Assistance in legal interpretation and application of the law.

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

Among the permitted AI systems, high risk AI systems are the most heavily regulated ones. Regulations include (but are not limited to):

High quality data

The EU AI Act recognizes that high quality data is essential for the performance of many AI systems. High quality data is also recognized as being important for ensuring that the AI systems perform as intended and safely and does not become a source for discrimination. Training, validation and testing data should be sufficiently relevant, representative and free of errors, and complete in regard to the purpose of the AI system.

Record-keeping and technical documentation

To be able to verify compliance with the EU AI Act, information regarding the following should be kept and documented: general characteristics, capabilities and limitations of the AI system, algorithms, data, training, testing and validation processes used, and documentation on risk management systems.

Transparency

To ensure that AI systems do not become too complex or incomprehensible for humans, a certain degree of transparency is required. Users should be able to interpret the output of the AI systems and use it appropriately.

Human oversight

The AI system should be developed and designed in a way which allows people to oversee their functioning. This includes the identification of proper human oversight measures of the AI system before it is put into service. More concretely, such measures should guarantee that the AI system is subject to constraints that cannot be overridden by the AI system itself and is responsive to the human operator.

Consistency, accuracy, robustness and cybersecurity

The AI system should perform consistently throughout its lifecycle and fulfill appropriate levels of accuracy, robustness and cybersecurity in accordance with what is generally acknowledged as state-of-the-art.

Technical robustness

The AI systems need to be resilient against risks connected to limitations of the systems as well as malicious actions against them, which could result in for example errors, faults, inconsistencies and unexpected situations.

CE marking

The AI systems should bear CE marking to indicate their conformity with the EU AI Act.

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

Real-life example

An example of the types of incidents that the EU AI Act aims at preventing was reported in April 2021. A **TUI flight took off from Birmingham Airport** with a plane load that was 1,200 kg heavier than calculated due to a computer glitch that counted every woman onboard with the title "Miss" as a child. The event was described as a "serious incident" by the Air Accidents Investigation Branch, since it affected how the aircraft was flown, including its thrust level during takeoff. The incident was later found to be caused by a glitch in the airline's reservation system.

TUI is not unique in facing data quality issues due to lack of technical robustness in their systems. In fact, a study in Harvard Business Review showed that only 3% of companies' data meet basic quality standards. In other words, 97% of data among corporations is of poor quality and should not be used for any business critical use cases, let alone high risk AI systems. The poor data quality situation is estimated to cost US companies several trillions USD per year. Most companies are far from fully compliant with the strict requirements that the EU AI Act imposes on the high risk systems, meaning that companies will have to either pause their high risk systems until they have managed to fulfill the requirements or make sure to step-change their ways of working with AI systems before the end of the grace period of the law.

"A TUI flight took off from Birmingham Airport with a plane load that was 1,200 kg heavier than calculated due to a computer glitch that counted every woman onboard with the title "Miss" as a child."

"...a study in Harvard Business Review showed that only 3% of companies' data meet basic quality standards. In other words, 97% of data among corporations is of poor quality and should not be used for any business critical use cases, let alone high risk AI systems.

Reach out to Validio to learn more about how the Data Trust Platform can help you stay compliant with the EU AI Act.

Contact us →

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

Limited risk applications - Transparency requirements

The limited risk category covers AI systems that interact with humans (such as chatbots), emotion recognition systems, biometric categorisation systems, and AI systems that generate and/or transform image, audio and/or video data. The requirements on limited risk AI systems focuses on transparency, with the goal to make users of these systems aware that they are interacting with a machine. This information empowers the users to make informed decisions on how to consume the output of those systems.

1 Unacceptable risk | 2 High risk | 3 Limited risk | 4 Low and minimal risk

Low or minimal risk applications - no obligations

AI systems that are not considered unacceptable, high, or limited in risk are categorized as low or minimal in risk. The EU AI Act does not impose any legal obligations on AI systems in this category.

General purpose AI systems

The EU AI Act will also include provisions governing General purpose AI systems, which will be tiered into high-impact and low-impact based on the degree of systemic risk they are associated with. High impact General purpose AI systems will be subject to more stringent obligations around areas such as model evaluations, assessments and mitigations of systemic risks, the conduction of adversarial testing, reporting of serious incidents to the European Commission, and reporting on energy efficiency. In addition, all providers of General purpose AI systems will have to fulfill transparency requirements on technical documentation and provide detailed summaries about the content used for training.

The provisions governing General purpose AI systems are the most recently added ones and are not yet fully completed, which means that more information will come as more clarity is being given by the regulators.

04 Timeline ahead

The EU AI Act is expected to be formally adopted by both the EU Parliament and Council to become EU law in early 2024, whereafter there is a two year grace period for compliance. However, use cases with unacceptable risk are likely to have a lower grace period of only six months after adoption whereas high risk AI systems will have a grace period of 12 months.

What can be done now to stay compliant?

Check out Validio's Data Trust Platform that helps you get full control of your data for AI systems.

Contact us →

05 Summary

The EU AI Act is the first regulation of its kind internationally and will govern AI systems within the EU market. Comprehensive requirements on for example data quality, record-keeping and technical documentation, human oversight, transparency, consistency, robustness, accuracy and cybersecurity are imposed on high risk AI systems. Most companies are nowhere close to fulfilling these strict requirements, which means that they will either have to step-change their processes and ways of working with their high risk AI systems or pause them altogether until compliance is ensured.

Discover how Validio can help bring trust to your data assets

Request a demo →

About Validio

Validio was founded in Stockholm in 2019, with the mission to help companies manage their data debt and get return on their data investments. To do this, Validio provides a Data Trust Platform that combines deep data observability, quality, lineage and catalog into one single platform—taking observability past its early experiments towards the first comprehensive platform to deliver return on data and AI investments.

Contact us
Validio.io

HQ

Linnégatan 78, 115 23
Stockholm