Holistic AI White Paper

The EU AI Act's Risk-Based Approach:

High-Risk Systems and What They Mean for Users

November 2022

Holistic AI

HOLISTICAI.COM

CONTENTS

KEY TAKEAWAYS

- The proposal for the EU AI Act sets forth a risk-based approach for regulating AI systems.
- The concept of high-risk AI system is not explicitly defined in the proposal. Instead, the proposal provides two lists along with certain conditions according to which high-risk AI systems shall be identified.
- Annex III provides a list of use-cases where an AI system may be considered high-risk unless the output of the system is purely accessory.
- Everyone in the lifecycle of a high-risk AI system may have obligations. Different obligations are imposed on providers, importers, distributors, and users. Users may be deemed as providers and become responsible as such depending under some conditions.

SUMMARY

The EU AI Act proposes a risk-based approach for regulating AI systems where some are prohibited due to unacceptable risk, some are considered high-risk and associated with stringent obligations, some have limited risk and are subject to transparency obligations, and others have no restrictions. However, neither the full list of high-risk AI systems nor the whole scope of associated obligations is set in stone just yet and the debate is on-going, particularly with respect to the use-cases listed in Annex III of the proposal.

This whitepaper outlines the general framework for high-risk AI systems in light of the latest compromise text proposed by the Czech Presidency since the determination of whether a given AI system is considered high-risk and is subject to these obligations will be of key importance for both the providers and users of AI systems under the upcoming regulatory framework.

THE EU AI ACT

The European Commission's proposed Harmonised Rules on Artificial Intelligence, colloquially known as the EU AI Act, seeks to lead the world in AI regulation. Likely to become the global gold standard for AI regulation, much like the general data protection regulations did for privacy, the rules aim to create an 'ecosystem of trust' that manages AI risk and prioritizes human rights in the development and deployment of AI. Since first being proposed, an extensive consultation process has resulted in a number of amendments being proposed to the rules in the form of compromise texts. Among those shaping this regulation are the European Council and the French Presidency, who have both published compromise texts, but others are also contributing to the developments through studies, discussion papers, and reports.

Under the Act, **providers of AI systems established in the EU** must comply with the regulation, along with **those in third countries that place AI systems on the market in the EU**, and those **located in the EU that use AI systems**. It also applies to providers and users based in third countries if the output of the system is used within the EU. Exempt from the regulation are those who use AI systems for military purposes, and public authorities in third countries.

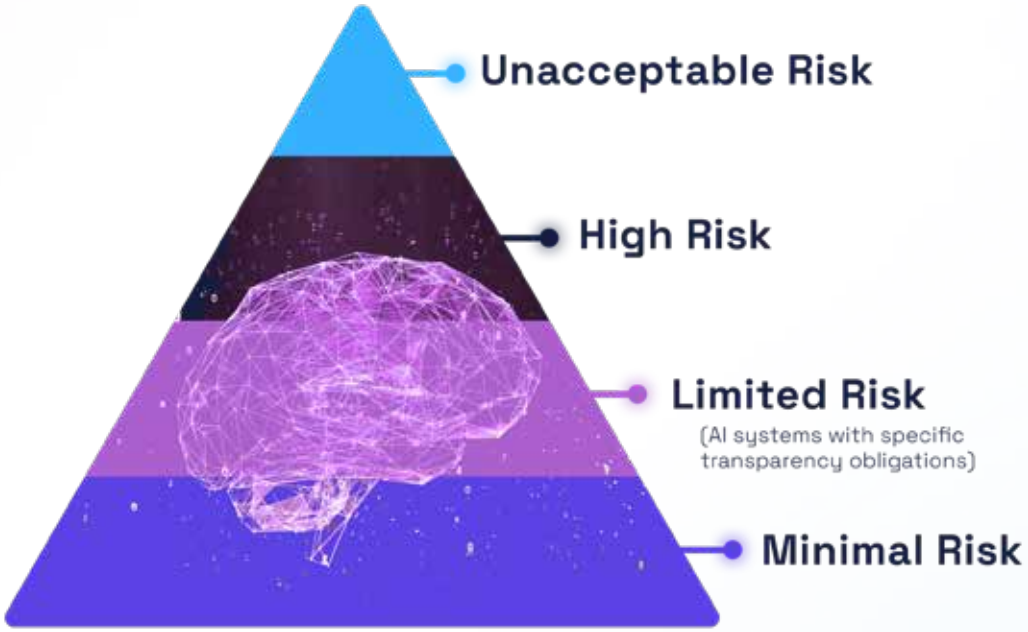
RISK-BASED APPROACH

The EU AI Act proposes a "risk-based approach" for regulating AI systems, where systems are classed as having low or minimal risk, limited risk, high-risk, or unacceptable risk. The risk associated with a system has implications on the risk management obligations on users of the system, and can dictate whether the system can be made available on the EU market.

Indeed, Recital 14 of the EU AI Act stipulates the following:

> *"In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems."*

Below we focus our attention on how high-risk systems have been defined and how the approach to managing the risks of these systems has evolved in the various iterations/compromise texts.



THE CLASSIFICATION OF HIGH-RISK AI SYSTEM

High-risk AI systems are governed under Chapter 1 of Title III (High-Risk AI Systems) of the EU AI Act. The concept of "high-risk AI system" is not explicitly defined. Instead, a group of AI systems are classified as such provided that certain conditions are met.

The question of which AI systems should be prohibited (and how exactly these are defined) and what kinds of AI systems should be classified as high-risk remains a topic of on-going debate as well as criticism since the circulation of **the Commission's original proposal**.

However, what we do know is the following:

- **Products and Safety Components:** Since the Commission's proposal, AI systems that are intended to be used as safety components of a product or are themselves products covered by the Union harmonization legislation listed in Annex II of the EU AI Act classified as high-risk under a condition. AI systems that are required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product as per the legislation concerned are considered high-risk. The Union harmonization legislation list in Annex II is, to this date, unchanged. Minor amendments have been made to the expression of Article 6 with respect to these AI systems and the first paragraph has been divided into two separate paragraphs for clarification **in the Slovenian Presidency's compromise text**. Still, the substance remained mostly the same.

- **List of Use-Cases:** Additionally, certain AI systems are classified as high-risk. These systems are listed as use-cases with some specific features in Annex III of the EU AI Act. Article 7 of the EU AI Act empowers the Commission to amend Annex III with some conditions.

While the Commission proposal had no general exception to the classification of the systems provided in Annex III as high-risk, **in the second presidency compromise text**, the Czech Presidency introduced conditions upon which systems provided in Annex III shall be considered high-risk pursuant to Article 6(3).

Accordingly, systems provided in Annex III were to be considered high-risk if the output of the system is immediately effective with respect to the intended purpose without the need for a human to validate it and/or the output of the system consists of information that is **not purely accessory** to the relevant action and may, therefore, lead to a **significant risk to the health, safety, or fundamental rights**. The first condition was deleted in **the third presidency compromise text for Articles 1-29 and Annexes I-IV** as automation does not necessarily denote high-risk and this condition could be prone to circumvention by putting a human in the loop. This structure is protected **in the fourth presidency compromise text** - which is the latest as of time the time of writing of this piece - with minor amendments to clarify the condition on purely accessory nature.

In other words, for an AI system in Annex III to be considered high-risk, the output of the system should not be purely accessory in respect of the relevant action or decision to be taken and lead to a significant risk to the health, safety, or fundamental rights.

WHAT ARE HIGH-RISK AI SYSTEMS?

According to the latest presidency compromise text there are eight main use-cases where an AI system may be classified as high-risk. These are

Biometrics

Critical infrastructure

Education and vocational training

Employment, workers management and access to self-employment

Access to and enjoyment of essential private services and essential public services and benefits

Law enforcement

Migration, asylum and border control management

Administration of justice and democratic processes

It must be emphasized, however, that not every AI system in these categories is considered high-risk. There are sub-paragraphs to each of these fields, which must be examined in detail to determine whether a given AI system indeed is considered high-risk or not.

THE DEBATE ON HIGH-RISK CONTINUES

The debate concerning what should be considered as a high-risk AI systems is a highly dynamic one.

To illustrate the nature of the discussions and details thereof, two issues with the latest presidency compromise text may be used.

- **Biometrics:** The prohibition or restriction of biometric identification via AI systems is one of the most controversial topics in the field. The Commission's original proposal was referring to "real-time and post remote biometric identification of natural persons". The term "remote" had been removed by the Slovenian Presidency last year due to the risk of confusion but has been reinstated in the fourth presidency compromise text. The justification for the reinstatement and the accompanying changes is that certain systems used for identification, such as fingerprint-based identifications, should not be covered. Accordingly, the definition of the remote biometric identification system has been amended to require the system to function "typically at a distance" and without "the active involvement" of the person who is to be identified.

- **Insurance:** Secondly, the Slovenian Presidency Compromise Text added AI systems intended to be used for insurance premium settings, underwritings, and claim as an additional high-risk use-case, something that was removed by the Czech Presidency in their first proposal. However, AI systems intended to be used for risk assessment and pricing in insurance products,including life and health insurances, are classified as high-risk in the fourth presidency compromise unless these systems are put in service by providers that are micro and small-sized enterprises.

These latest amendments, combined with the somewhat ambiguous wording of the provisions related to the classification of high-risk AI systems, clearly call for a meticulous monitoring of the developments and a rigid examination for a proper compliance.

WHAT ARE THE IMPLICATIONS OF HIGH-RISK AI SYSTEMS?

EU AI Act sets forth requirements for high-risk AI systems under Chapter 2 and subsequently imposes obligations on providers as well as users of these systems.

There are seven main requirements provided under Articles 9 to 15:

Compliance with these requirements is mandatory for covered entities.

However, the compliance level shall be determined by taking into account the generally acknowledged state of the art pursuant to Article 8(1). Additionally, compliance with these requirements may demand the consideration of provisions on other contentious issues including, but not limited to, product liability, data protection, copyright, intellectual property, and trade secrets. Thus, a proper compliance would require a detailed and multi-faceted analysis that is tailored to the specific circumstances of each AI system.

PROVIDERS AND USERS

Regarding obligations, a distinction has to be made between the provider and the user of a given high-risk AI system. Under Article 3 of the latest presidency compromise text, provider is defined as:

> *"a natural or legal person, public authority, agency, or other body that develops an AI system or that has an AI system developed and places that system on the market or puts it into service under its own name or trademark, whether for payment or free of charge"*

whereas user is defined as:

> *"any natural or legal person, including a public authority, agency or other body, under whose authority the system is used"*

Providers are the primary targets in terms of compliance as well as obligations under the EU AI Act. In addition to satisfying the previously-mentioned requirements, they have obligations to cooperate and provide information under certain circumstances. In addition to providers, importers and distributors of AI systems have some obligations under Articles 26 and 27, respectively. These obligations, however, are mostly for confirmation, verification, and information provision purposes.
Users' obligations are provided under Article 29 according to which users shall use high-risk AI systems in accordance with the instructions, implement human oversight and monitor the operation of the high-risk AI system, keep the logs, take data protection provisions into account, and cooperate with national authorities. There are additional specific obligations for users that are financial institutions.

It must also be emphasized that the user or provider status for a given high-risk AI system may change depending on the subsequent actions of these actors. Pursuant to Article 23a of the latest presidency compromise text, the person who puts their trademark on or makes substantial modifications to a high-risk AI system already placed on the market or put into service, modifies intended purpose of a non-high-risk AI system in a manner that makes it as such, or places on the market or puts into service a general purpose AI system as a high-risk AI system or as a component thereof shall be considered provider for the purposes of the EU AI Act.

HOLISTIC AI CAN SUPPORT YOU IN YOUR PATH TOWARDS TO COMPLIANCE WITH THE EU AI ACT

As the explanations above demonstrates, whether a given AI system is considered high-risk or not according to the EU AI Act is an important question with many practical implications for everyone involved with the lifecycle of an AI system. Despite currently not being in force, the EU AI Act and developments thereof shape the industry practice along with the formation of new rules as well as standards. Taking steps to manage the risks of your AI systems is the best way to get ahead of this upcoming regulation, and can help you to embrace AI with greater confidence. At Holistic AI, we have a diverse team of experts in computer science, algorithms, auditing, law, and public policy who combine their expertise to make AI more ethical, legal, and safeguard against potential harms.

To learn more on how we can empower your enterprise to adopt and scale AI with confidence, **get in touch** with us today.

GOT QUESTIONS OR WANT TO SCHEDULE A CHAT? CONTACT US AT

holisticai.com we@holisticai.com

Holistic AI