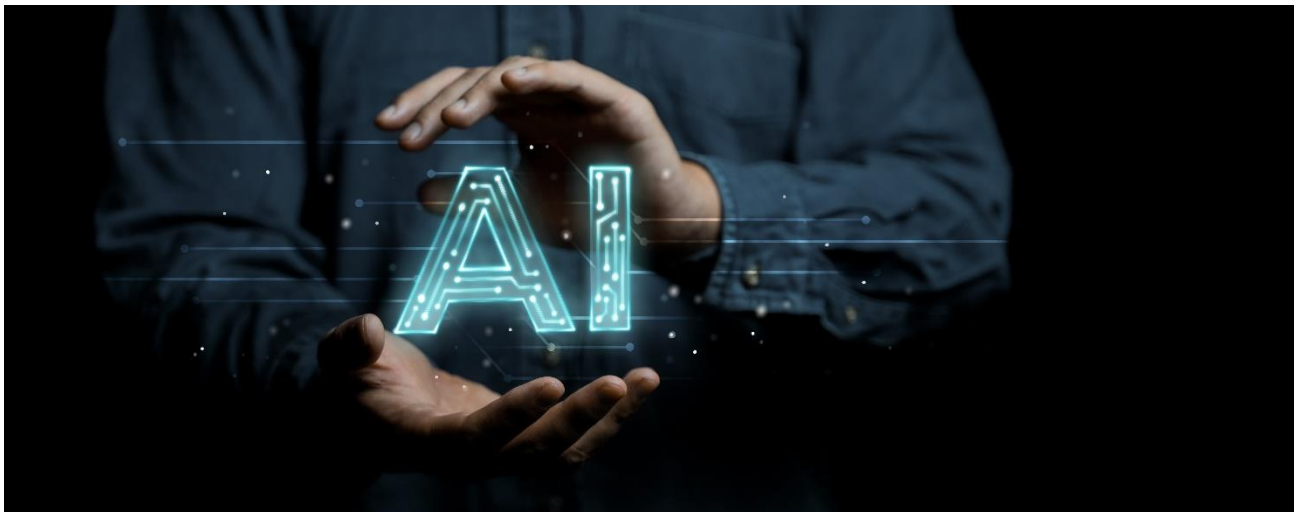
EU AI Act: the world's first legal framework for artificial intelligence

THE EU PARLIAMENT HAS GIVEN THE GREEN LIGHT FOR THE ARTIFICIAL INTELLIGENCE ACT



Executive Summary

- On 13 March 2024, the EU Parliament adopted the regulation laying down harmonised rules on artificial intelligence (AI Act).
- The Act creates a cross-sectoral legal framework for the development and application of AI in the EU, which will be fully applicable by the end of a transitional period of two years.
- The Act takes a risk-based approach, defining various risk levels for AI systems. The higher the potential risks of an application, the higher the legal requirements that apply, up to and including a complete ban of certain AI practices.
- "AI sandboxes" and testing procedures under real conditions shall encourage innovation.

Introduction

Artificial intelligence ("**AI**") is no longer a vision of the future. It is already part of our lives. The development and application of AI systems will determine whether companies are able to compete in the digital age. ChatGPT is a striking example of what is in store with the advent of AI. While such applications allow users to create content or texts on any topic without any prior knowledge, the problems with these text-generating AI systems are already becoming apparent. For example, AI often confidently states facts that are entirely made up or feeds into existing prejudices. At the same time, the potential uses of AI are seemingly unlimited: completely new research avenues and applications are opening up in the healthcare sector, development in the field of self-driving vehicles is accelerating, while artificial intelligence can also facilitate the structured searching and evaluation of huge amounts of data or the optimisation of production processes.

1. Definition and risk categories under the AI Act

The AI Act defines the term "AI system" very broadly as a machine-based system that is designed to operate with varying levels of autonomy and that can generate certain outputs (such as digital content, predictions, recommendations or decisions) that are clearly defined by humans and influence physical or virtual environments.

The main aim of the Act and its risk-based approach is to set limits on the use of high-risk systems without imposing restrictions on risk-free systems. The AI Act distinguishes between the following risk categories:

(1) Unacceptable risk – prohibited practices AI solutions that come with "unacceptable" risks are completely prohibited. This includes systems that are intended for "social scoring" purposes, i.e., evaluating or manipulating human behaviour.

(2) High risk High-risk systems generally pose a significant threat to safety, fundamental rights, the environment, democracy and rule of law if they malfunction. This applies in particular to AI systems in the areas of critical infrastructure management, including self-driving vehicles, but also AI-based systems that make decisions over access to employment. Furthermore, AI systems that can be used for essential private and public services – such as healthcare or banking – are considered high-risk. In addition to extensive documentation and transparency obligations, such high-risk systems are also subject to considerable security requirements with regard to the decision-making process and the data used for training them. Such systems require human oversight. In addition, a mandatory impact assessment – as is commonly used in other regulated areas of the economy – has been introduced to evaluate any infringement of fundamental rights.

(3) Limited risk AI systems that are designed to interact with natural persons (e.g., in customer service applications) may be associated with limited risks due to a lack of transparency regarding the use of AI. The AI Act introduces specific transparency obligations with respect to such systems. For example, if an AI system such as a chatbot is being used, people shall be made aware that they are interacting with a machine. AI providers must also ensure that AI-generated content is identifiable. In addition, AI-generated text that is published with the aim of informing the public in general must be labelled as such. This also applies to AI-generated audio and video content.

(4) Minimal or no risk AI systems that pose only a minimal risk or no risk can be used freely under the AI Act. These include other systems that optimise production processes, for example, or applications such as AI-enabled video games or spam filters.

2. General purpose AI

Foundation models and general purpose AI ("GPAI"), such as those behind ChatGPT, are covered by a separate category under the AI Act. Such general purpose AI systems (as defined in the AI Act) must fulfil specific legal requirements. This includes an internal conformity assessment procedure and adequate technical documentation. Above all, these systems must also fulfil certain transparency requirements, including compliance with EU copyright law and the publication of detailed summaries of the content used for training the systems. Additional requirements apply to more powerful models that could entail systemic risks, including model evaluations, systemic risk assessments and incident reports.

3. Exceptions for law enforcement authorities

In principle, the Act does not allow the use of biometric identification systems by law enforcement authorities. However, there will be exceptions for narrowly defined emergency scenarios and in compliance with strict safety regulations. For example, it will be permitted to use AI systems for targeted searches for missing persons or to prevent a terrorist attack.

4. General civil rights

In future, any natural or legal person will have the right to lodge a complaint about AI systems and to receive an explanation for decisions made on the basis of high-risk AI systems that affect their rights. Complaints can be lodged

with the competent market surveillance authority of the respective EU Member State.

5. Fostering innovation: AI sandboxes and "flexible" official discretion in favour of businesses

In addition to regulating AI, legislators also hope to actively support European providers. To this end, the Act includes provisions for the introduction of AI sandboxes. These are test phases supported by the authorities during which AI systems can be developed and trained. Within these sandboxes, companies are allowed to process personal data more extensively and receive support regarding the regulatory requirements. The Act also stipulates that no fines will be imposed for violations of the law – provided that the recommendations of the authorities are complied with. In addition, authorities are to exercise their discretion "flexibly" during this test phase.

6. Sanctions mechanism

The AI Act specifies that the rules are to be enforced in a decentralised manner by the Member States. The sanctions provisions are largely based on fines, which vary in amount depending on the severity of the offence:

The use of prohibited AI systems is subject to a fine of up to EUR 35 million or – if the offender is a company – up to 7% of its total worldwide annual turnover, whichever is higher.

In the case of permitted AI systems, fines of up to EUR 15 million or – if the offender is a company – up to 3% of its worldwide annual turnover, whichever is higher, may be imposed if the requirements and obligations laid down in the Act are not complied with. In practice, this is likely to account for the majority of fine offences.

Fines of up to EUR 7.5 million or – if the offender is a company – 1% of its worldwide annual turnover, whichever is higher, may still apply if incorrect, incomplete or misleading information is provided to the competent authorities in response to a request for information.

The amount of the potential fines thus even exceeds the fines stipulated by the EU General Data Protection Regulation (GDPR).

The AI Act sets lower fines for SMEs and start-ups.

7. Entry into force of the AI Act

The EU Parliament adopted the AI Act on 13 March 2024. The Act still needs to be adopted by the European Council and will then be published in the Official Journal of the EU.

The AI Act should enter into force 20 days after publication and, with a few exceptions, will apply in full 24 months after entering into force. Some provisions will apply before this date. For instance, the provisions on prohibited AI practices will apply after just 6 months and the obligations relating to general purpose AI after 12 months. In contrast, rules on specific high-risk systems will only apply after three years.

8. Outlook and what companies should do now

Overall, the AI Act represents a comprehensive approach to regulating AI systems and their applications that aims to strike a balance between fostering innovation and protecting fundamental rights and social values. The aim is to create a reliable and competitive environment for the development and use of AI in the European Union.

The central focus on system security and the protection of fundamental rights in the AI Act is to be welcomed. Defining clear rules and standards for AI systems should help strengthen the trust of users and consumers, which is an essential condition for the widespread introduction of AI applications that will benefit both companies and society as a whole.

While European businesses may currently criticise the imbalance with regard to the US and Chinese markets, some of which are (still) unregulated or far less regulated, the EU AI Act – despite all the criticism of the proportionality of the new compliance requirements and the negative impact on international competition – represents a milestone in terms of creating legal certainty, which the USA

and China will ultimately not be able to avoid. Not only are similar regulations to be expected in the USA and China, but global companies based in these countries will also have to comply with the AI Act if they want to export to the EU. In this respect, European companies can benefit from a better understanding of the compliance obligations.

Regardless of whether they produce AI systems or merely intend to use them as part of their business, companies should familiarise themselves with the provisions of the AI Act as soon as possible and check whether they are relevant to their business model. This does not only apply to providers of high-risk AI systems. Providers of such systems would in any case be well advised to start adapting their compliance structures and the corresponding documentation to the requirements of the AI Act now and preparing for the mandatory conformity assessment, for example. Even companies that use or are planning to use AI systems with only limited or minimal risk should, as a first step, carry out a legal and technical/organisational survey of these systems or have one carried out in order to determine what the corresponding obligations are under the AI Act.

Overall, it is to be hoped that the new AI Act will help set global standards for the legally watertight use of AI and ultimately boost Europe's reputation as a centre of innovation and technology.

Dr Jörg Kahler
Lawyer, Partner
Berlin
Tel +49 30 2039070
joerg.kahler@gsk.de

Dr Jörg Wünschel
Lawyer, Senior Associate
Berlin
Tel +49 30 2039070
joerg.wuenschel@gsk.de

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason, we recommend you to request personal advice.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxembourg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
London branch
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Registered office: Munich
Munich Local Court
HRB 281930
Managing directors:
Dr Mark Butt, Andreas Dimmling

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM