World's first Artificial Intelligence Act

EUROPEAN COMMISSION PRESENTS THE WORLD'S FIRST DRAFT LEGISLATIVE FRAMEWORK FOR REGULATING ARTIFICIAL INTELLIGENCE (AI)

Executive summary

- On 21 April 2021, the European Commission presented its legislative proposal for an AI Regulation. It aims to set a robust and flexible legal framework for ensuring that AI systems will be trustworthy, safe, and secure.
- In order to avoid unnecessary trade restrictions and foster innovation, a risk-based regulatory approach is being pursued.
- The requirements and obligations imposed on manufacturers and providers will vary based on the degree of risk associated with their AI systems and practices.
- Infringements can result in heavy fines. Sanctions can be up to EUR 30 million Euros or 6% of total annual turnover.

1. Introduction

Artificial intelligence (AI) is beginning to make its way into our everyday lives. The benefits and conveniences that AI can offer are offset by the not inconsiderable risks in ethics and data protection. Likewise, the risk of discriminatory outcomes when using systems of this nature should not be underestimated.

The AI Regulation being proposed aims to establish proportionate regulation at the EU level which is limited to minimum requirements necessary for addressing the risks and problems associated with AI. Improving the transparency and trustworthiness of AI are the clear objectives for this regulatory measure. Yet there is also an attempt to avoid unduly restricting or hindering the technological development of novel AI systems.
This regulation will completely ban certain systems which bear unacceptable risks. Restrictions and safeguards are specified for high risk systems. Additionally, transparency and notification obligations are established for certain kinds of other AI systems.

2. Scope of application

The AI regulation uses an open definition for the term artificial intelligence. Accordingly, an "artificial intelligence system" (AI system) means a software that is developed with special techniques and can, for a given set of human-defined objectives, generate outputs (such as content, predictions, recommendations, or decisions) that influence real or digital environments. The regulatory approach pursued here has a focus on high-risk systems. This will leave a high number of AI systems unaffected. AI systems which are developed and used exclusively for military purposes also won't be covered by the regulation.

The goal is to have full legal harmonisation for the placing on the market, putting into service, and utilisation of AI systems within the European Union. The regulation will apply to providers of AI systems irrespective of whether they have a domicile in the EU or not.

3. Risk groups

The AI Regulation divides AI systems into various risk groups. This risk-based approach will be used to determine whether an AI system may be used at all and, if so, whether and which requirements and obligations must be met in order to use that AI system.
The risk groups are:

Unacceptable risk: AI systems which threaten the safety, livelihood, or rights of people will be banned from the outset. This particularly includes AI systems and practices that exploit a person's age, physical or mental disability, or otherwise in some manner exploit a person's

subconscious to manipulate their free will or behaviour in a way that causes or is likely to cause physical or mental harm to them or another person. There is also a ban on AI systems which place a person at a particular disadvantage because of their social behaviour or affiliation (so-called "social scoring").

Exceptions will be made for real-time remote biometric identification in public spaces, something which is otherwise generally prohibited. The use of these kinds of AI systems may be authorised for law enforcement measures when elevated requirements are met, in particular in order to search for victims of crimes or to avert immediate threats to life and limb or terrorist attacks.

High risk: The core of the AI regulation lies in the regulation of high-risk AI systems. The relevant measure for classification under this risk group consists of severity of potential damage and degree of probability for the damage occurring.

The draft bill lists AI systems to be classified as high-risk using a catalogue of cases. The list will be updated on a regular basis. The focus in classification is not on technical characteristics. Rather, the technology's specific application is what will be decisive. In particular, AI systems for use in the following areas are classified as high-risk:

- Real-time remote biometric identification (to the extent permissible as an exceptional case);
- Management and operation of critical infrastructures;
- Education and vocational training;
- Safety components for certain products (especially in the aviation and automotive sectors);
- Law enforcement;
- Migration, asylum, and border control management;
- Judiciary.

The draft regulation spells out extensive requirements and obligations for providers of high-risk AI systems (see 4. and 5.) which must be observed before and after placement on the market.

Low risk: AI systems of low risk will be subject to a minimum transparency obligation. Especially in cases involving "deep fakes" and AI systems for customer contact ("chatbots"), it must be clearly recognisable to a user that they are interacting with an AI system and not a real person.

Minimal risk: The majority of AI systems currently in use (e.g. AI-supported video games or spam filters) will receive classification as minimal risk under the regulatory proposal. These kinds of minimal risk AI systems can be used freely without being subject to regulatory requirements.

4. Requirements and obligations for high-risk AI systems

Providers and manufacturers of high-risk AI systems must undergo a conformity assessment procedure to determine whether the regulatory requirements are met. In addition to high standards in terms of system robustness, (cyber-)security, and accuracy, this particularly includes the establishment of a risk and quality management system, human oversight, sufficient transparency, and the provision of information.

Providers whose business domicile lies outside of the EU must appoint an authorised representative in the EU to ensure compliance in their AI systems.

5. Compulsory registration

The draft regulation provides for a public database for providers of high-risk AI systems. These AI providers would be required to register their systems prior to market launch. The database will contain information that enables supervisory authorities, users, and other stakeholders to audit high-risk systems with respect to the regulation's requirements.

6. Data security and incident response

Trustworthy AI systems depend on high-quality datasets that developers and providers use to learn and fine-tune AI. It is crucial that these records be protected against access or interference by unauthorised third parties. That kind of influence could impact AI data output (irrespective of sector) and lead to unintended consequences, including biased results and outright wrong conclusions. That is why the draft regulation requires technical precautions be implemented in terms of AI security to prevent the following:
(i) manipulation of training datasets via third parties, (ii) inputs designed to cause the model to make a mistake, and (iii) other flaws.

7. Enforcement and sanctions

Compliance with the respective requirements and obligations will be monitored and controlled by the competent national supervisory authorities.

As with the EU General Data Protection Regulation, this legislative proposal places enforcement of these provisions in the hands of Member States, and also features a similar system of fines consisting of multiple levels.

For example, trading in prohibited AI systems can trigger fines of up to 30 million Euros or 6% of the total world-wide annual turnover for the preceding financial year. A fine of up to 10 million Euros or 2% of the total worldwide annual turnover for the preceding financial year will be imposed on anyone who fails to comply with the requirements and obligations under the Regulation.

8. Outlook

The draft regulation presented will now go through the EU legislative procedure in the European Parliament and the European Council. This process will likely take a year or more. Upon adoption of the regulation, there will be a 24-month transition period to enable companies to implement these wide-ranging regulatory requirements.

It will be interesting to see whether these regulatory provisions will become even more stringent in certain areas as the legislative process moves forward. With regard to the current draft, there is already a critical discussion as to whether the AI regulation is setting the right benchmark for promoting innovation, or whether it will ultimately stifle innovation in the AI sector. In any case, the upcoming regulation will have a significant impact on AI-based business models.

Jörg Kahler
Attorney-at-Law (Germany), Partner
Berlin office
Tel +49 30 2039070
joerg.kahler@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

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.
Taunusanlage 21
60325 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