New draft AI (Artificial Intelligence) Regulations of 11 November 2022 - key assumptions

According to Eurostat, in 2020, only 0.7% of EU entrepreneurs with 10 or more employees were using AI applications. As regards chat services, in which a chat-bot or virtual agent generated natural language responses for customers, this was used in 2% of entities. The same percentage of entities, 2%, used service robots that have a certain degree of autonomy, e.g. to perform cleaning, hazardous or repetitive tasks, such as cleaning up toxic substances, sorting items in a warehouse, and helping customers with their purchases or at the point of payment, etc.[1]

The lack of regulation in the manufacture, offering, and use of AI systems creates a state of considerable uncertainty for all market participants, especially as regards the most advanced AI systems. In April 2021, the European Commission unveiled its AI package, which included, i.a. a proposal for a new draft regulation establishing harmonised rules for AI ("**AI Act**"). Over the past year, the need to update and amend the proposed rules to better reflect the specificities of advanced AI systems and provide greater security for their users has been recognised twice.

The new - third version of the draft Artificial Intelligence Act of 11 November 2022 makes some changes in relation to the two previous versions. The definition of AI system adopted in the previous versions of the act was only slightly amended. In the current version, the definition of AI has changed. In the new wording, the definition takes into account the elements of the autonomy that AI has[2].

It has been assumed that an artificial intelligence system is a system that has been designed to operate with elements of autonomy and which, based on data and information provided externally - either by a human or a machine, infers how to achieve the goals set by a human. In doing so, the system is supposed to use *machine learning* or logic and knowledge-based approaches.

„An Artificial Intelligence system (AI system) is a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts."

The catalogue of entities covered by the current version of the draft regulation remains unchanged from the previous (second) version of this draft act. The current proposal has retained the new categories of entities introduced in the previous version to which the regulation will apply. These are:[3]

- importers and distributors of AI systems,
- product manufacturers that place an AI system on the market or put it into service with their product and under their own name or trademark, and
- authorised representatives of suppliers established in the European Union.

[1] *https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210413-1*
[2] *Art. 3 (1) of the draft regulation, https://artificialintelligenceact.eu/wp-content/uploads/2022/11/AIA-CZ-Draft-General-Approach-11-Nov-22.pdf*
[3] *Article 2 (1) (d) – (f) of the draft regulation.*

Exemptions

The draft also contains certain exemptions[4] which can be divided into few main categories. The provisions of the regulation will not apply to:

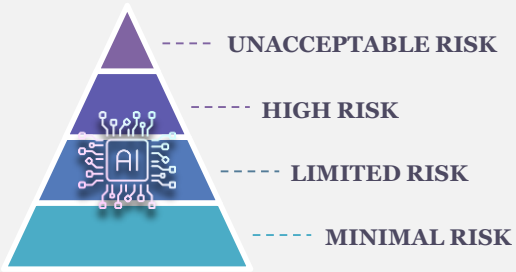
AI systems for purposes outside the scope of EU law, in particular, activities concerning military, defence, or national security purposes, regardless of the type of entity carrying out these activities.

AI systems developed and put into use solely for research and development (R&D) purposes.

Public authorities in a third country and international organisations if they use AI systems under international agreements on law enforcement and judicial cooperation with the EU or with one or more Member States.

Users who are individuals (natural persons) using AI systems as part of a purely personal non-professional activity, with certain exemptions.

It is also crucial to change the parameters for classifying systems into different risk groups, i.e. unacceptable, high, limited, and minimal.



High-risk AI systems

In practice, the criteria for classifying AI systems, especially high-risk systems, are debated and controversial. According to Eurobarometer[5] data, just over half of Europeans (51%) believe that public policy intervention is needed to ensure the ethical use of AI systems. Up to 80% of respondents believe that they should be informed when a digital service or mobile application they use uses AI.

As currently drafted, the AI systems with the highest risk is a system that:

- is a product covered by the relevant EU legislation if it is required to undergo a conformity assessment in order to be placed on the market or put into service[6],
- a system listed in Annex III to the Regulation, unless the output of that system is purely ancillary to the relevant action or decision to be taken and is not likely to lead to significant risks to health, safety or fundamental rights . These are i.a.[7]:

[4] *Article 2 (3), (6) and (7) of the draft regulation.*
[5] *https://ec.europa.eu/commission/presscorner/detail/es/ip_20_383*
[6] *Article 6 (1) of the draft regulation.*
[7] *Article 6 (3) of the draft regulation.*

- remote biometric identification systems,
- systems to control individuals' access to institutions, education or training programmes,
- systems designed for use to recruit or select individuals i.a. for targeted job advertisements, analysing and filtering job applications and assessing applicants,
- systems designed for assessing the creditworthiness of individuals or determining their credit score (with some exceptions),
- systems designed for use by or on behalf of law enforcement agencies to assess the credibility of evidence in the course of investigating or prosecuting crimes,
- systems designed for use in assessing risk to individuals and pricing life and health insurance (with the exception of AI systems deployed by micro and small business providers).

Additional security requirements

From the perspective of market participants, in addition to the efficiency (effectiveness) of technological solutions, the security aspect is particularly important. For these reasons, it has been stipulated that even general-purpose AI systems that can be used as high-risk systems or as components of such systems should meet additional security requirements. First and foremost, they should[8]:

- have a risk management system,[9]
- comply with data management requirements,[10]
- have appropriate technical documentation and instructions for use,[11]
- have an appropriate level of accuracy, resilience, and cyber security, and behave consistently in these respects throughout its life cycle.[12]

In addition to the technical aspect, emphasis is also placed on ethical issues and those related to protecting the privacy of the users of AI systems. The draft provides that, i.a. the following are prohibited:[13]

- AI systems that use **subliminal techniques beyond the person`s awareness that have the purpose or effect of materially distorting** the user's behaviour in a way that may cause the user (or another person) physical or **psychological harm**,
- AI systems that exploit **the vulnerability of a particular group of people because of their age** (e.g. children or the elderly) or a **disability or social or economic circumstances to materially distort the behaviour of such person** in a way that may cause them (or another person) physical or **psychological harm,**
- AI systems to assess or classify individuals over a period of time based on their **social behaviour or known/predicted personal or personality characteristics** that lead to their harmful or disadvantageous treatment (discrimination), and
- 'real-time' biometric **identification systems in public spaces by or on behalf of law enforcement agencies for law enforcement purposes** unless absolutely necessary, e.g. to facilitate the search for specific potential victims of crime, to detect or identify an individual during a criminal investigation, or to prevent a specific and significant threat to critical infrastructure, life, health or safety; or to prevent terrorist attacks.

[8] *Article 4b(1) of the draft regulation.*
[9] *Article 9 of the draft regulation.*
[10] *Article 10 of the draft regulation.*
[11] *Article 13 of the draft regulation.*
[12] *Article 15 of the draft regulation.*
[13] *Article 5 of the draft regulation.*

Given the large number of general concepts and vague phrases used, e.g. '*significant distortion*', '*significant threat*', or 'strictly necessary', doubts are bound to arise in practice as to the correct interpretation of the various concepts used in the regulation. At present, there is not yet sufficient practice by authorities and case law in this area (at national and EU levels). However, it seems that, as in other cases, the interpretation will be made taking into account the objectives of the regulation adopted by the legislator and the functions AI is supposed to perform socially and economically.

Liability - severe financial penalties

Due to the existence of a risk of harm - tangible or intangible - depending on the circumstances and the application of the AI system in question, for preventive purposes, the draft provides for significant financial penalties for non-compliance with its provisions. For example, a breach of any of the prohibitions referred to in Article 5 of the draft regulation (i.e. the prohibited practices described above) is to be punishable by an administrative fine of **up to €30,000,000** or, if the offender is an enterprise, **up to 6% of its total worldwide annual turnover** for the preceding financial year. For small and medium-sized enterprises, including start-ups, the fines are to be **up to 3% of their total worldwide annual turnover** for the preceding financial year.[14]

[14] *Article 71 (3) of the draft regulation.*

dr hab. Ewa Skrzydło-Tefelska
Senior Partner, attorney-at-law
✆ +48 608 420 802
✉ ewa.skrzydlo-tefelska@skslegal.pl

Marta Kowalczuk-Kędzierska
Associate
✆ +48 883 391 699
✉ marta.kowalczuk-kedzierska@skslegal.pl

Warszawa
Jasna 26, 00-054 Warszawa
T +48 22 608 70 00
F +48 22 608 70 70
E office@skslegal.pl

Katowice
Wojewódzka 10, 40-026 Katowice
T +48 32 731 59 86
F +48 32 731 59 90
E office.katowice@skslegal.pl

Poznań
Mickiewicza 35, 60-837 Poznań
T +48 61 856 04 20
F +48 61 856 05 67
E office.poznan@skslegal.pl

Wrocław
Plac Solny 16, 50-062 Wrocław
T +48 71 346 77 00
E office.wroclaw@skslegal.pl

www.skslegal.pl