DOI: https://doi.org/10.12700/btsz.2025.7.4.167

FROM THEORY TO PRACTICE: ANALYSIS OF ARTIFICIAL INTELLIGENCE REGULATION IN THE EUROPEAN UNION – RECOMMENDATION ON GENERAL TERMS AND CONDITIONS

ÚT AZ ELMÉLETTŐL A GYAKORLATIG: A MESTERSÉGES INTELLIGENCIA EURÓPAI UNIÓS SZABÁLYOZÁSÁNAK ELEMZÉSE – AJÁNLÁS AZ ÁLTALÁNOS FELHASZNÁLÁSI FELTÉTELEKRE

ANTAL Tímea[1] – SZÁMADÓ Róza[2]

Abstract

The rapid development of artificial intelligence (AI)-based applications has brought with it new legal and security challenges. In order to reduce the pitfalls and risks of practical application, it is necessary to examine the stages of development of European Union regulations and, based on this, make proposals for the main elements of the general terms of use for artificial intelligence applications. Regulations and the general terms and conditions of use that appear in specific applications play a key role in ensuring regulatory compliance. The aim of this study is twofold: on the one hand, to present and analyze the development of EU artificial intelligence regulation, and on the other hand, to formulate recommendations for the general terms of use of AI applications on a scientific and legal basis.

Keywords

artificial intelligence regulation, European Union, general terms of use of AI, compliance

Absztrakt

A mesterséges intelligencia (MI) alapú alkalmazások gyors fejlődése új jogi és biztonsági kihívásokat hozott magával. A gyakorlati alkalmazás buktatóinak, kockázatának csökkentése érdekében szükséges vizsgálni az európai uniós szabályozás fejlődési lépcsőit, és erre alapozva javaslatot tenni a mesterséges intelligencia alkalmazások általános felhasználási feltételeinek főbb elemeire. A szabályozás és a konkrét alkalmazásoknál megjelenő általános felhasználási feltételek kulcsfontosságú szerepet játszanak a szabályozási megfelelőség (compliance) biztosításában. Jelen tanulmány célja kettős, egyrészt be kívánja mutatni majd elemezni az uniós mesterséges intelligencia szabályozás kialakításának folyamatát, másrészt kísérletet tesz arra, hogy tudományos és jogi alapokon nyugvó ajánlást fogalmazzon meg az MI-alkalmazások általános felhasználási feltételeire vonatkozóan.

Kulcsszavak

mesterséges intelligencia szabályozás, Európai Unió, MI általános felhasználási feltételek, compliance

[1] timea.antal0@gmail.com | ORCID: 0009-0006-7258-1715 | PhD student, Óbuda University | doktorandusz hallgató, Óbudai Egyetem

[2] szamado.roza@bgk.uni-obuda.hu | ORCID: 0009-0000-9684-335X | Assistant Professor, Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering | egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

The spread of artificial intelligence is an important driver of the digitization of the European economy. The importance of this topic is reflected in the fact that the European Commission has set key objectives in the areas of digital infrastructure, skills, business and government services, and has also identified performance indicators that will enable the measurement of progress towards the 2030 goals of the digital decade in the Digital Decade Program [1]. According to the program's 2025 report [2] by 2025, the artificial intelligence revolution will gain further momentum due to breakthroughs in fundamental technologies, as they transform the boundaries of innovation, redefine competitiveness, and radically change people's everyday lives. Employees are already using artificial intelligence tools to increase productivity, simplifying work tasks and supporting decision-making processes. At the same time, however, new potential risks and challenges have emerged with the use of artificial intelligence.

The European Union Agency for Cybersecurity (ENISA) ranked artificial intelligence ninth among the ten factors posing the greatest potential threat to society in its 2024 March report [3]. This may rightly undermine people's initial trust. The use of artificial intelligence applications from a compliance perspective can be aided by a recommendation on general terms of use. The topic of this article is therefore timely and has practical benefits in this regard.

METHODOLOGY

During the research, I analyzed eleven publicly available documents (strategies, recommendations, guidelines, statements, regulations) related to artificial intelligence in the European Union. The methodology of the study was qualitative document analysis, which enabled the systematic processing and comparison of the content of the documents and the identification of structural patterns. The time frame for the selection of documents was 2017–2025. I examined only documents directly related to the topic. The analysis for the development of the regulatory map was based on the definition of objectives and principles, the development of a legal and ethical framework, and the guarantee of security. The artificial intelligence regulatory map formed the basis for the preparation of the recommendation on artificial intelligence.

EUROPEAN UNION ARTIFICIAL INTELLIGENCE REGULATORY MAP

The European Union has been working on developing regulations for artificial intelligence for years. The main reason for these efforts is that the EU recognizes the importance of AI, which it primarily associates with economic development. Since 2017, numerous recommendations, strategies, guidelines, and statements have been issued on this subject. It took seven years for the EU's regulatory framework to come into force. The main focus of the regulations is on defining basic principles, developing a legal and ethical framework, and guaranteeing safety by minimizing risks:

- Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy [4];

- European Parliament Report 27.1.2017 with recommendations to the Commission on Civil Law Rules on Robotics [5];
- The European Council EUCO 14/17. conclusions [6];
- EU Declaration on Cooperation on Artificial Intelligence [7];
- Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe [8];
- High-Level Expert Group on Artificial Intelligence - Ethical Guidelines for Trustworthy Artificial Intelligence [9];
- Digital Europe Strategy [10];
- Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence [11];
- White Paper On Artificial Intelligence [12];
- Artificial Intelligence Act [13];
- Artificial Intelligence Code of Practice [14].

The EU primarily associates AI with economic development and the strengthening of technological and industrial capacities (Digital Europe Strategy, Artificial Intelligence for Europe, Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence), i.e. the strategic idea that digitization will primarily determine the future of industry has come to the fore, and therefore views AI as a tool that contributes to the integration of intelligent technologies into industrial processes, thereby expanding the range of service elements (Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy).

The specific definition of AI is as follows: artificial intelligence refers to a system that is capable of intelligent behavior and examines its environment in order to achieve specific goals, then—with a certain degree of autonomy—takes action. (Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe) [15].

Although the current regulations only define general principles, they emphasise the importance of developing ethical and legal frameworks (EU Declaration on Cooperation on Artificial Intelligence, Recommendations to the Commission on Civil Law Rules on Robotics). According to the statement, building on the fundamental rights and values of the EU, the main objective of Member States should be to develop continuous cooperation and common thinking. It also highlights the importance of measures to support small and medium-sized enterprises and innovative start-ups operating in the robotics sector, creating new market segments or using robots. With regard to ethical principles, it emphasises risk analysis and proposes the development of a clear, strict and authoritative ethical framework for the development, design, manufacture, use and modification of robots (Recommendations to the Commission on Civil Law Rules on Robotics). Another significant achievement of the Recommendation is that it makes charter-like proposals: it precisely defines the code of conduct for robotics engineers, i.e. the rules to be used when examining robotics protocols, the rules to be applied by research ethics committees, and sample licences for designers and users.

The European Council has stated that a European model for artificial intelligence must also be developed: among other things, the establishment of a forward-looking regulatory framework, the creation of an unified regulatory framework for cyber security, and swift action to respond to emerging trends are essential for the successful development of the Digital Europe Programme (The European Council EUCO 14/17. conclusions).

The EU has recognised the need to prepare for the socio-economic changes resulting from artificial intelligence and considers it important to ensure an appropriate ethical and legal framework based on the values of the Union and in line with the EU Charter of Fundamental Rights. It has stated that it is necessary to develop draft ethical guidelines on artificial intelligence, while also analysing the adequacy of certain existing rules on safety and civil liability issues. The experts also recognised the importance of ideas that have emerged in relation to the modernisation of the legal frameworks for product liability and data protection (Artificial Intelligence for Europe).

The EU considers trustworthiness to be a key factor (Ethical Guidelines for Trustworthy Artificial Intelligence), and has therefore set out the basic elements of trustworthy artificial intelligence, which must be fulfilled throughout the entire life cycle of the system.

- legality, i.e. compliance with applicable legal regulations;
- ethics, i.e. ensuring compliance with ethical principles;
- ensuring technical and social stability.

The ethical guidelines were formulated to promote compliance with ethical principles based on fundamental rights (respect for human autonomy, prevention of harm, fairness, explainability). The guidelines define seven key requirements that a reliable artificial intelligence system must meet:

- Human agency and oversight
- Technical stability and security
- Data protection and data management
- Transparency
- Diversity, non-discrimination and fairness
- Social and environmental well-being
- Accountability.

These requirements undergo continuous technical and non-technical testing processes to filter out operational deficiencies in order to verify their necessity and effectiveness.

The Digital Europe Strategy has defined artificial intelligence as a specific, unique objective in Article 5. The objective of artificial intelligence is to achieve the following operational objectives:

- building and strengthening the basic capacities of artificial intelligence in the Union, including data sources and algorithm libraries that comply with data protection legislation;
- ensuring access to such capabilities for all businesses and public administrations;
- strengthening and networking existing artificial intelligence testing and experimentation facilities in Member States.

White Paper On Artificial Intelligence [12]: The EU aims to create a legal environment that promotes innovation and reduces risks. The White Paper is the first document to explicitly define a possible legal framework for the development and application of artificial intelligence. The book emphasises that, as a general rule, EU legislation remains fully applicable regardless of the involvement of AI. However, it is necessary to bear in mind that it is advisable to strictly manage the risks arising from artificial intelligence: it may even be necessary to adjust certain legal instruments. In this regard, the basic principle is that the new regulatory framework for artificial intelligence must be effective and safe, which can only be achieved through a risk-based approach. According to the Commission's position, an AI application should, as a general rule, be considered high-risk if it meets the following two cumulative conditions:

- It is used in a sector where, given the nature of the activities typically carried out, significant risks can be expected.
- The AI application is used in the sector in a way that could cause significant risks.

The White Paper also set out the main elements of the requirements for high-risk AI applications:

- data used to train systems;
- data and record retention;
- communication;
- stability and accuracy;
- human oversight;
- specific requirements for certain specific AI applications.

In order to verify and ensure compliance with the requirements, an objective ex ante conformity assessment is necessary, which may include testing, inspection or certification procedures. Conformity assessment would be mandatory for all operators: monitoring by national authorities and effective judicial redress mechanisms would also be necessary.

The content of the White Paper had a fundamental influence on the drafting of the Artificial Intelligence Act.

It is clear, therefore, that the AI Act is a significant milestone in the regulation of artificial intelligence. It establishes a complex, risk-based regulatory environment and allows for fines of up to 6% of global turnover. Although the regulation does not define the concept of artificial intelligence, it does define what an AI system is and what the basic operating requirements are for systems based on such technology. The legislation also sets out its specific objectives, as well as the expected results and performance indicators arising from its application. It is worth examining the data that make up the performance indicators in advance in order to track changes as accurately as possible. I see the essence of the risk management system detailed in Article 9 as following the plan-do-check-act logic in order to minimize and prevent risks. In other words, professionals first plan what needs to be done, then carry out the task, check the results, and finally intervene in the process to make the work more efficient next time; they do this over and over again, monitoring the entire process each time. The risk management system is an iterative process that runs continuously throughout the entire life cycle of a high-risk AI system and requires regular and systematic updating of data.

Article 53 of the Regulation sets out the practical obligations for providers of general-purpose AI models. It emphasizes that technical documentation for the model must be prepared and kept up to date, and that information and documentation must be developed, kept up to date, and made available to providers of AI systems who wish to incorporate the general-purpose AI model into their AI systems. A policy for compliance with EU law on copyright and related rights is needed, as well as a sufficiently detailed summary, and it is also essential to publish educational material used to teach the functioning of the general-purpose AI model.

Article 54 of the Regulation serves to ensure security and transparency, as service providers established in third countries must appoint a representative based in the Union by written authorization prior to placing a general-purpose AI system on the Union market.

Article 55 imposes additional obligations on providers of general-purpose AI models that pose a systemic risk. Accordingly, model evaluation must be carried out in accordance with standardised protocols and tools that reflect the current state of the art, and the EU and systemic risks arising from the development, marketing or use of general-purpose AI models that may pose systemic risk must be assessed and mitigated. Serious and unexpected events must be monitored, documented and reported without undue delay to the AI Agency and, where appropriate, to the competent national authorities, so that the relevant information on corrective measures taken to address them can be analyzed by the competent bodies in order to ensure an appropriate level of cybersecurity protection.

At the level of EU regulation, Article 56 also contains practical regulations, according to which practical codes must be developed for the proper practical application of the regulation. This led to the creation of the MI general practical code, which will apply from the 2nd August 2025. Table 1 shows the relationship between this code of practice and the AI Regulation and also contains a summary of its content relevant to the research.

Artificial Intelligence Code of Practice	AI Act	Content
Transparency chapter	Article 53	It provides a practical template for developing data, measurements, and methodologies related to the content of the documentation. Its main elements are: general information; model properties; distribution methods and licenses; usage parameters; training process; information on data used for training, testing, and validation; computing resources (during training); energy consumption (during training and application).

Artificial Intelligence Code of Practice	AI Act	Content
Copyrifght chapter	Article 53	Defines a 5-point action plan for the protection of copyright. It is necessary to develop, update, and implement a copyright policy. When searching the World Wide Web, only legally accessible, copyright-protected content may be reproduced and used. When mapping the World Wide Web, copyright restrictions must be identified and respected. The risk of results that infringe copyright must be reduced. A contact person must be designated and a mechanism for submitting complaints must be provided.
Safety and security chapter	Article 55	This chapter provides the most accurate and detailed practical recommendations for managing systemic risks by defining ten commitments: • Developing, implementing, and renewing a security and protection framework. • dentifying system-level risks within a structured process by developing system-level risk scenarios. • Developing a system-level risk analysis. • Defining system-level risk acceptance. • Defining security measures. • Defining protection measures. • Developing security and protection model reports. • Clearly dividing system-level risk responsibility. • Reporting serious incidents. Defining additional documentation tasks and ensuring transparency.

1. Table: The relationship between the Artificial Intelligence Code of Practice – AI Act and the summary of its content (Source: own edited)

Alongside the practical advancement of artificial intelligence, the practical application of legal regulations is an essential task: without regulations, data, processes, methodologies, and measurements, artificial intelligence is a one-armed giant. Based on the above, it is clear that the role of AI system regulation is becoming increasingly important for a number of reasons.

Since the use of artificial intelligence is associated with increased security risks, the application of practical tools to respond to these risks plays a key role. EU AI regulations focus on security, human-centeredness, and sustainability. For the time being, EU documents mainly provide theoretical frameworks for practical work. The EU's increasingly comprehensive legal regulations show that decision-makers recognize the importance of AI:

therefore, practical guidelines have followed strategies and statements, and risk management has also taken on a more prominent role. The following key aspects have appeared in EU AI regulations and documents:

- Emphasis on economic development;
- Consideration of ethical and legal frameworks;
- Definition of terms;
- Identification and management of risks;
- Identification of processes;
- Ensuring transparency;
- Establishment of security and protection.

RECOMMENDATION ON THE TERMS OF USE FOR ARTIFICIAL INTELLIGENCE APPLICATIONS

The legal, ethical, risk, and security regulation of artificial intelligence applications is ongoing. There is a need to ensure the accountable and appropriate functioning of artificial intelligence systems, which requires regulated processes, legal regulations, and enforcement tools. Regulated processes must be designed, applicable, and monitored to maintain security. Processes and appropriate regulations can ensure that risks become identifiable and manageable.

A sufficiently detailed and accurate set of terms of use that can be understood by users enables the safer use of artificial intelligence applications. Below, I set out 14 recommendations concerning the main content elements:

- Definitions - Precise definition of data related to the AI application and its use (Article 3 of the EU AI Act).
- Service provider contact details: name, registered office, website; customer service contact details.
- Service description and changes - Presentation of the operating environment, exclusion of errors, definition of prohibited uses (Articles 5-6 of the EU AI Act). Presentation of model characteristics, distribution methods and licenses, usage parameters.
- Application availability - Determination of availability.
- Data processing conditions - Ensuring compliance with GDPR [16], data retention and deletion rules [17].
- User rights and obligations - Access, modification, correction, deletion, data portability [16].
- Security measures, protection rules - Cybersecurity standards (GDPR Article 32 [16]; NIS2 Article 21 [18]).
- Fees - Determination of the basic fee, other fees payable based on usage, and payment terms.
- Copyright, intellectual property rights - Copyright status of content generated by AI.
- Liability regulation - Human supervision of high-risk decisions, limitation of liability.

- Contract conclusion, changes, and notification - Acceptance of terms of use, rules for modification, and notification obligations.
- Jurisdiction and applicable law - Definition of national and international law.
- Ethical and transparency supplements - Definition of detailed documentation, training process, information on data used for training, testing and validation.
- Customer relations, complaint handling - Complaint handling and process, fee complaints.

In the interests of transparency, I recommend creating a table of contents and clearly indicating the date of entry into force. I recommend that the general terms and conditions be published on the service provider's website in an easily accessible, downloadable, storable, displayable, and printable format, with searchability within the text.

CONCLUSION

The practical application of EU regulations on artificial intelligence could be ensured by detailed and compliance-oriented general terms of use. Legal compliance, protection, security, and ethical responsibility also need to be regulated within the framework of general terms of use for AI. Transparent and detailed contractual terms and conditions can contribute to building trust, transparency, and minimizing regulatory risks. In the future, it will therefore be worth examining what regulatory conditions are included in the general terms and conditions of use of ChatGPT, DeepL, Microsoft Copilot, and other similar services in practice.

REFERENCES

[1] European Parliament, European Council, Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. In: https://net.jogtar.hu/jogszabaly?docid=a22h2481.eup
[2] European Commission, „State of the Digital Decade 2025 report ”. In: https://digital-strategy.ec.europa.eu/hu/library/state-digital-decade-2025-report
[3] European Union Agency for Cybersecurity (ENISA), „ENISA Foresight Cybersecurity threats for 2030 - UPDATE.”, 2024. In: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-full-report_en_0.pdf
[4] European Commission, Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy. COM/2017/0479 final. In: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52017DC0479
[5] European Parliament, Report 27.1.2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). In: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017IP0051&from=EN
[6] Eurpean Council, „European Council EUCO 14/17. conclusions”. In: https://www.consilium.europa.eu/media/21607/19-euco-final-conclusions-hu.pdf
[7] European Commission, „EU Declaration on Cooperation on Artificial Intelligence”. In: https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence

[8] European Commission, „Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe”. 2018. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

[9] High-Level Expert Group on Artificial Intelligence, Ethical Guidelines for Trustworthy Artificial Intelligence . In: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[10] European Commission, Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM(2018) 434 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN

[11] Europena Parliament, „Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence 6177/19”. In: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf

[12] European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust. In: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52020DC0065

[13] European Parliament,European Council, 2024/1689 12.7.2024 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). In: https://net.jogtar.hu/jogszabaly?docid=a2401689.eup

[14] European Commission, „Az MI általános célú gyakorlati kódexe”. 2025. In: https://digital-strategy.ec.europa.eu/hu/policies/contents-code-gpai

[15] European Commission, „Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe”. 2018. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

[16] European Parliament, European Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: https://net.jogtar.hu/jogszabaly?docid=a1600679.eup

[17] P. Voigt és A. Von Dem Bussche, The EU General Data Protection Regulation (GDPR). Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-57959-7.

[18] European Parliament, European Council, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). In: https://net.jogtar.hu/jogszabaly?docid=a22i2555.eup