BERNITSAS briefing

Technology - Artificial Intelligence: Special Edition

Artificial Intelligence in the EU: Where Do We Stand?

This Briefing is an introductory practical guide to the anticipated EU Artificial Intelligence Regulation (the EU AI Act); it aims to outline the key aspects of the EU AI Act and help companies understand and assess whether and how they will be affected. The briefing is based on the initial text published by the EU Commission[1] also taking into account the most recent developments in the legislative procedure[2].

In This Issue

A. Introduction

1. Artificial Intelligence (AI) is a rapidly evolving technology, which already affects many aspects of human activity. Its potential seems unlimited and its implications are considerable for both the individual and the public sphere of life. On the other hand, many reasonable reservations and concerns about its use are being expressed.

2. At a European level, the introduction of harmonised rules regulating AI throughout the European Union is essential for the strengthening of the internal market and for the protection of fundamental rights in accordance with the European principles and standards. Following the 2021 proposal by the European Commission and months of intense negotiations, the European Parliament and the Council reached, last December, a political agreement for an EU Artificial Intelligence Regulation (the EU AI Act). The agreement was welcomed as historical, as it signals the final stage of the legislative process for the adoption of the first comprehensive regulatory framework on AI globally. Safety and trust, fundamental rights, legal certainty and innovation are the underlying principles of the Act.

B. Key Points

1. The following table summarizes the most important points of the EU AI Act.

---

[1] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final/ 21.4.2021.

[2] Certain technical and other aspects of the AI Act are still subject to finalisation. The final text of the Regulation and its formal adoption are expected in the coming weeks or months. Information which has, in the meantime and up to date, become public is taken into consideration to the extent that such information is officially confirmed.

BERNITSAS briefing

C. Who Will the EU AI Act Affect?

1. The EU AI Act will apply to:
    a. EU or third country providers (either public or private bodies) placing or putting in service AI systems within the EU;
    b. users of AI systems located in the EU; and
    c. providers and users of AI systems located in a third country if the output of the system is used in the EU.
2. Additional categories, like distributors and manufacturers, are likely to also be included in the scope of the EU AI Act, under its final version.
3. Certain AI systems, for example systems of military use, are exempted from the scope of the EU AI Act.

D. Definition of AI Systems

1. Various definitions of AI have been given over time within the scientific community or in various fora and jurisdictions. However, in view of the global character of AI and the need for interoperability, consensus on a definition is important. To enhance legal certainty, EU legislators, in their recent agreement, proposed a new definition aligning with the updated definition of the OECD. The final wording is still to be finalized, however the following elements are (so far) used to define an AI system as such:
    a. machine-based system;
    b. autonomous operation (the degree of autonomy may vary);
    c. adaptiveness or possible adaptiveness after deployment;
    d. generation of output (content, decision etc) by inferring, for explicit or implicit objectives, from input received; and
    e. possibility of output to influence physical or virtual environments.

E. Classification / Risk-based approach

1. The proposed Act adopts a risk-based approach; AI systems are classified depending on the risk they present to security, safety and fundamental rights and they are accordingly either banned or allowed under certain conditions.

INDICATIVE EXAMPLES[3]	OBLIGATIONS
UNACCEPTABLE RISK LEVEL **Permissibility: Prohibited**	
▪ AI systems deploying subliminal techniques or exploiting vulnerabilities of a group of persons to materially distort a person's behaviour in a manner that may cause physical/psychological harm; ▪ Use of AI systems by public authorities for the evaluation or classification of the trustworthiness of natural persons leading to detrimental or unfavourable treatment of certain persons/groups;	Cease operation, remove from the market.

---

[3] Pursuant to the available information included in the press releases of the Council of the EU, European Parliament and European Commission dated on 09.12.2023.

- Use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes (subject to exceptions);
- Use of AI systems for untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases;
- Use of AI emotion recognition systems for use in workplace or educational institutions.

HIGH RISK LEVEL[4]

Permissibility: Authorized subject to a set of requirements, obligations and an ex-ante conformity assessment

Subject to oversight by competent authorities

Use of AI including: - biometric identification, categorization and emotion recognition systems; - management and operation of critical infrastructure (such as in the fields of water, gas and electricity); - medical devices; - systems to determine access to educational institutions or for employment management; - access to and enjoyment of essential private services and public services and benefits; - certain systems used for law enforcement, border control management, administration of justice and democratic processes.	High-risk AI systems must, among others: - register on an EU database[5] before placement on the market; - deploy a risk management system; - observe data quality standards; - comply with requirements for technical documentation and record keeping; - ensure transparency and provide information to users; - provide the possibility for human oversight while in use; - ensure accuracy, robustness and cybersecurity in the system design and development.

LIMITED/LOW RISK LEVEL
Permissibility: Authorised

- chatbots; - certain emotion recognition and biometric categorization systems; - systems generating visual and audio 'deepfake' content.	Transparency obligations: - Users who are natural persons must, as a principle, be informed that they are interacting with an AI system and, if applicable, that such system is an emotion recognition system or a biometric categorisation system; - Users of AI systems generating content that appreciably resembles existing persons, places etc and would falsely appear to be authentic or truthful ('deep fake'), must, under certain exceptions, disclose that the content has been artificially generated. Adoption of codes of conduct to voluntarily apply the legal requirements for high-risk AI systems is encouraged.

MINIMAL/ NO RISK LEVEL
Permissibility: Authorised

All AI systems not classified in the above categories, for example: - spam filters; - AI-enabled video games.	No additional legal obligations. Voluntary adoption of codes of conduct is encouraged.

---

[4] Classification according to Article 6 and the annexes of the EU AI Act.
[5] To be set by the EU in collaboration with Member States.

BERNITSAS briefing

2. The criteria for the classification of AI systems are provided by the Act and its annexes. It remains to be seen in practice whether and to what extent these criteria provide the legal certainty and clarity needed for companies' compliance.

3. In addition, specific cases of general-purpose AI (GPAI) systems as well as foundation models are addressed following a tiered approach depending on the systematic risk they entail, imposing relevant compliance obligations to providers of such models.

F. Penalties

1. Infringement of the Act may result in the imposition of fines. The amount of the fines may vary depending on the type of infringement and the infringing entity's size:

TYPE OF INFRINGEMENT	FINES THRESHOLD
Engagement to prohibited practices or non-compliance with data requirements.	Up to €35m or 7% of the total worldwide annual turnover of the preceding financial year (whichever is higher).
Non-compliance with any other requirement or obligation imposed by the Act.	Up to €15m or 3% of the total worldwide annual turnover of the preceding financial year (whichever is higher).
	Up to €7.5m or 1.5% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

2. In case of SMEs or startups, the above fines thresholds shall be adjusted proportionately to be the lowest[6].

G. What Should Companies Do?

1. Although the definitive text of the AI Act remains to be seen, companies are strongly advised to take proactive steps and prepare well in advance to ensure full and timely compliance with the Act. They should start by mapping their AI systems, assessing the level of risk that these systems present and understanding the respective framework they must comply with.

2. Depending on the classification of each system, companies should therefore plan, among others, for the following:

   a. understand their position in the AI value chain (ie whether developer, buyer etc) and the way they may be developing and using AI tools and systems (even within the company);

   b. proceed to a risk assessment of the AI systems concerned and classify them under the AI Act;

   c. remove all AI systems prohibited by the Act;

   d. identify the applicable obligations for high and limited risk systems;

   e. conduct a gap analysis;

   f. design and take the necessary steps for compliance; and

   g. closely follow legal developments (finalization and coming into force of the Act, decisions by the competent Authorities etc).

H. Other Legal Implications

1. Besides regulatory compliance, companies (providers, users etc) should take into consideration several legal issues that the development and use of AI gives rise to. Some of these relate to the following:

   a. use of data for both training of AI models and the production of results;

   b. privacy and personal data protection;

   c. intellectual property rights;

   d. eventual criminal liability; and

   e. sector specific legal issues

2. Companies should consider ways to mitigate legal risk; appropriate contracting and carefully drawn policies are useful tools in this direction.

I. Next Steps

1. Following the political agreement reached at the EU institutions' level last month, work is currently underway to refine the outstanding technical details and generate a final consolidated text.

2. Once finalized, the EU AI Act will need to be formally adopted by the European Parliament and the Council before being published in the Official Journal. It will then enter into force 20 days after publication in the Official Journal, with a direct effect in EU Member

---

[6] See Council's press release 986/23 of 09.12.2023.

BERNITSAS briefing

States.

3. The AI Act will in general become applicable after a transition period of two years after its entry into force. Different applicability periods will be provided for specific cases (for example, 6 months for prohibited practices). During the transitional period, the

European Commission will launch an AI Pact, whereby AI developers from Europe will voluntarily commit to implementing key obligations of the AI Act ahead of their coming into force.

Contacts

Dr Anastasia Mallerou
Counsel
E amallerou@bernitsaslaw.com

Tania Patsalia
Senior Associate
E tpatsalia@bernitsaslaw.com

Fotini Karra, Senior Associate and Ioniki Poulaki, Associate contributed to this Briefing.