

**C L I F F O R D**

**C H A N C E**

**FINAL NEGOTIATIONS CAN BEGIN AFTER EUROPEAN  
PARLIAMENT VOTE ON THE EU AI ACT**

## CONTENTS

1. Overview	3
2. Addressing emerging and developing hot topics	4
3. Revisiting and narrowing critical concepts	6
4. Taking a stricter stance on certain AI uses and practices	7
5. Adapting the enforcement framework	8
6. And more...	9
7. Looking forward	9
8. What should companies be doing?	10

## FINAL NEGOTIATIONS CAN BEGIN AFTER EUROPEAN PARLIAMENT VOTE ON THE EU AI ACT

On 14 June 2023, the European Parliament voted to adopt its negotiating position on the proposed EU regulation on AI (“**AI Act**”). This is another major step towards the adoption of the proposed AI Act, undoubtedly one of the most important and anticipated pieces of legislation of these past few years.

Parliament has made a number of significant changes to the European Commission’s original proposal. In terms of strategic orientations, the Parliament appears to be seeking to: (i) address emerging or developing hot topics, including generative AI and foundation models, and core ethical principles; (ii) revisit or narrow down some critical concepts, such as the definition of an AI system and what qualifies as a high-risk AI system; and (iii) take a stricter position on some AI uses and practices, including a broader ban on the hotly debated use of AI systems for remote biometric identification in public spaces.

Now, the EU institutions need to discuss, agree a common position and adopt a final text. So begin the trilogues, and there’s work ahead to reconcile the different positions. There is an increasing sense of urgency regarding the need to adopt an appropriate framework to regulate AI – and the rest of the world is watching closely.

In this article, we examine some of the key changes introduced by the European Parliament.

### 1. Overview

The AI Act is a landmark piece of legislation which seeks to regulate the placing on the market, putting into service and use of AI systems (see our briefing: [The future of AI regulation in Europe and its global impact](#)). Following years of work at the EU level, the European Commission shared the initial proposal for the AI Act in April 2021, with the Council of the EU then adopting its ‘general approach’ in December 2022 (see our article: [The EU AI Act: concerns and criticism](#)). Following the Parliament’s vote on 14 June 2023, trilogue negotiations between the Commission, Parliament and Council have now at last begun with the aim of agreeing a final, common text.

Parliament has amended the Commission’s proposal substantially. Key changes include:

- Addressing emerging or developing hot topics that were not addressed by the Commission (or only in a limited fashion), including through specific requirements to regulate ‘foundation models’ and ‘generative AI’ and through the introduction of general principles presented as applying to all AI systems;

- Revisiting or narrowing some critical concepts, such as the definition of an AI system, as well as the categorisation of, and obligations relating to, high-risk AI systems;
- Taking a stricter position and expanding the list of prohibited AI uses and practices, including a more general ban on AI systems for remote biometric identification;
- Developing the AI Act enforcement and governance, and proposing an independent European AI Office; and
- Other changes including, notably, on the scope of the AI Act and its territorial reach.

## 2. Addressing emerging and developing hot topics

### Regulating general purpose AI, foundation models and generative AI

#### General purpose AI and foundation models

The Council's general approach introduced the concept of 'general purpose AI system'.

The Parliament retains the concept, redefined as "*an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed*". Further, and in response to advances in the sophistication of AI systems, the Parliament now also introduces the concept of 'foundation models' and a number of specific requirements for these:

- A 'foundation model' is defined as an "*AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks*". A new recital illustrates how the concepts of 'AI system', 'general purpose AI system' and 'foundation model' interact: "*AI systems with specific intended purpose or general purpose AI systems can be an implementation of a foundation model, which means that each foundation model can be reused in countless downstream AI or general purpose AI systems*".
- Providers of foundation models would be subject to specific requirements, such as conducting risk assessments and mitigating reasonably foreseeable risks, establishing appropriate data governance measures, and registering the foundation model in an EU database. They would also be subject to obligations regarding the design and development of the system, including in relation to appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity, as well as environmental impact, and to draw up technical documentation and intelligible instructions for use.

#### Generative AI

The Parliament's text adds further obligations for providers of foundation models used in 'generative AI' (meaning "*foundation models used in AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video*") and those "*who specialise a foundation model into a generative AI system*". Such providers would have to comply with certain transparency obligations, including: (i) informing individuals where content is generated by an AI system; (ii) training, designing and developing the foundation model in such a way as to ensure

adequate safeguards against the generation of content that violates EU law; and (iii) making publicly available documentation summarising the use of training data protected under copyright law.

(For more on generative AI, see our paper: [\*Generative AI – the big questions.\*](#))

### **General core principles for all AI systems?**

There are six ‘general principles’ that all operators would be required to make best efforts to adhere to when developing and using any AI system or foundation model (*i.e.*, not limited to high-risk systems) to promote a “*coherent human-centric European approach to ethical and trustworthy AI*”:

- *human agency and oversight*: AI systems are required to be developed to serve people, respect human dignity and personal autonomy, and be appropriately controlled and overseen by humans;
- *technical robustness and safety*: minimising unintended and unexpected harm as well as ensuring robustness and resilience of the AI system in case of unintended problems;
- *privacy and data governance*: compliance with existing privacy and data protection laws and meeting high standards of quality and integrity;
- *transparency*: allowing appropriate traceability and explainability, making humans aware when they communicate or interact with an AI system, and informing users of the capabilities and limitations of that AI system and affected persons about their rights;
- *diversity, non-discrimination and fairness*: promoting equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases;
- *social and environmental well-being*: promoting the use of AI in a sustainable and environmentally-friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy.

The Parliament is explicitly reflecting and putting the emphasis (back) on some key ethical principles that have been at the heart of discussions around AI for years. If truly made to apply to all AI systems, this could be an important change to the scope and the risk-based approach of the AI Act. However, the proposed language casts doubt on how far these provisions are actually intended to go. This is something that will certainly be discussed in trilogues and we can expect to be revisited.

Further, and while the Commission’s and the Council’s positions already include some references, environmental considerations are given more prominence in the Parliament’s text.

### 3. Revisiting and narrowing critical concepts

#### The definition of AI system

Following a very broad definition proposed by the Commission (see our article: *The new EU regulation on artificial intelligence: 'AI system' = any software?*), both the Council and the Parliament have sought to rework the definition of 'AI system' which sits at the heart of the AI Act.

As part of the definition, the original text proposed by the Commission notably included an annex detailing the techniques and approaches used to develop an AI system, and the Council's general approach incorporated part of this detail directly into the definition itself. The Parliament has not included these references at all. In the Parliament's text, an AI system means "*a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments*".

This definition more closely aligns with that used by the OECD.

Although the Parliament's trimmed definition is more technology-neutral, it remains broad and the discussions on this topic illustrate the complexity of defining what is at the core of the AI Act, *i.e.*, the very notion of an AI system.

#### New conditions for AI systems to qualify as high-risk?

While the Commission proposed to automatically categorise as 'high-risk' all systems falling in certain critical areas and use cases, both the Council and Parliament have suggested introducing additional conditions. For the Parliament, an AI system should no longer automatically qualify as high-risk simply because it is listed in Annex III; it would also have to present a significant risk of harm to health, safety and fundamental rights – or, in some cases, to the environment. The Commission would be responsible for issuing guidelines in this respect, and a specific process would apply where the provider considers that its system does not pose such a risk.

The Parliament has also proposed significant changes to the list of stand-alone high-risk AI systems in Annex III, including adding some and moving others to prohibited practices. For example, the Parliament includes in the list under Annex III: (i) AI systems intended to be used to make or materially influence decisions on eligibility for health and life insurance (the Council had also suggested that certain systems used for assessment and rating purposes in life and health insurance be added); (ii) AI systems intended to be used for biometric identification of natural persons, with the exception of systems that are prohibited; (iii) AI systems intended to be used by very large online platforms (also known as VLOPs) under the Digital Services Act in connection with their recommender systems; and (iv) certain AI systems used for influencing the outcome of, or voting behaviour in, an election or referendum.

## **4. Taking a stricter stance on certain AI uses and practices**

### **An expansion of the prohibited practices**

Parliament has extended the list of AI practices which are prohibited under the AI Act.

Remote biometric identification systems, such as facial recognition systems, have been hotly debated throughout the legislative process so far – right up to the last minute as regards the plenary vote. In the Commission's initial proposal, the use of AI systems for real-time remote biometric identification in publicly accessible spaces for law enforcement purposes was prohibited, with some exceptions. Parliament has expanded this prohibition, banning: (i) the use of 'real-time' remote biometric identification systems in publicly accessible spaces; as well as (ii) the putting into service or use of AI systems for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, with a narrow exception in the second case linked to specific and particularly serious crime and subject to a pre-judicial authorisation.

As the Parliament was voting in favour of a wide ban on remote biometric identification systems in public spaces, developments were taking place at the Member State level. For instance, on 12 June and following other recent legislation on algorithmic video surveillance adopted in connection with the Paris 2024 Olympics and Paralympics, the French senate passed a bill to allow the experimentation of biometric recognition technology in public spaces in specific cases. While this bill still needs to make its way through the legislative process and to be debated, it marks another interesting development at the Member State level, taking place in parallel to – and intended to apply in advance of – the EU-wide developments.

Other prohibitions proposed by the Parliament include the placing on the market, putting into service or use of an AI system for:

- Predictive policing based on profiling, location or past criminal behaviour;
- Emotion recognition systems used in law enforcement, border management, the workplace or educational institutions; and
- The creation or expansion of facial recognition databases using indiscriminate scraping of biometric data from social media or CCTV footage.

### **Enhanced compliance obligations for high-risk AI systems**

Parliament has expanded various compliance obligations relating to the use and deployment of AI. Notably, it has introduced a requirement for deployers (referred to as 'users' in the Commission's initial proposal) of certain high-risk AI systems to carry out a fundamental rights impact assessment prior to putting the relevant high-risk AI system into use, and possibly also during the use if the relevant criteria are no longer met. The assessment would cover, among other things, the system's intended purpose, the scope of its use, the categories of persons likely to be affected, the

check that the use of the system is compliant with relevant EU and national laws on fundamental rights, the reasonably foreseeable impact on fundamental rights of using the system, and specific risks of harm likely to impact marginalised people or vulnerable groups. There would also need to be a detailed plan as to how the harms and negative impact on fundamental rights will be mitigated; and if a detailed plan to mitigate the risks outlined in the course of the fundamental rights impact assessment cannot be identified, the deployer would have to refrain from putting the high-risk AI system into use.

The new requirements would also entail a consultation process with the competent authority and relevant stakeholders, and, for certain entities, there would be a requirement to publish the summary of the assessment results.

Other changes include, in relation to training, validation and testing datasets, a requirement for (i) appropriate measures to detect, prevent and mitigate possible biases and (ii) transparency regarding the original purpose of data collection.

Conversely, the Parliament has sought to address some of the criticism directed at the Commission's initial proposal as regards obligations for high-risk AI systems. This includes seeking to further frame obligations around data and data governance, notably the widely-criticized requirement for datasets to be error-free and complete – something which the Council's general approach also looked at – and further clarifying the allocation of responsibilities between provider and deployer where the data is actually held by the deployer.

## 5. Adapting the enforcement framework

### Penalties

The Parliament's text provides for an increase in the possible maximum fine for the most serious breaches. More specifically, it contemplates fines of up to EUR 40 million or 7% of the total worldwide turnover for the preceding financial year of the offender, whichever is the higher, in case of non-compliance with the prohibited AI practices.

A waterfall of lower (but still significant) maximum fine tiers continues to be envisaged for different categories of other offences under the AI Act, with some of the maximum amounts being reduced in the Parliament text compared with the Commission's initial proposal.

### Governance

Amongst other things, the Parliament proposes an independent AI office with its own legal personality in place of the European Artificial Intelligence Board proposed by the Commission (which was mainly modelled on the example of the European Data Protection Board under the GDPR). It would maintain a similar role and powers including in relation to monitoring the implementation of the AI Act, providing guidance, fostering cooperation between national authorities and coordinating joint investigations – and more, *e.g.*, also promoting AI literacy. The AI office would be accountable to the Council and the Parliament.



## 6. And more...

There are various other changes in the Parliament's proposal, for instance on such things as: the scope of the AI Act, including to also seek to prevent prohibited practices from being "exported" outside of the EU by providers or distributors located in the EU; and the introduction of rights for affected persons to report infringements to the competent national supervisory authority, and to lodge complaints against providers and deployers of AI systems, which are encouraged to provide internal complaint mechanisms.

## 7. Looking forward

### When will the AI Act actually apply?

Parliament and Commission both propose a transition period of two years, following the entry into force of the AI Act, before the majority of its provisions would apply (and the Council has proposed to extend this to three years). That said, the idea of an earlier implementation timeframe, reduced by six months, was mentioned by the co-rapporteurs in the context of discussions around the plenary vote for some systems such as foundation models and generative AI.

### Next steps

Following the Parliament's vote, trilogue discussions between the Council, the Parliament and the Commission have now commenced. It is difficult to predict how long the process will take before a political agreement on the AI Act can be reached but conceivably it could be before the end of 2023 or early in 2024, and there is pressure on the EU institutions to work fast on this. It is reported that several meetings have been scheduled in the coming months with the objective of finalising the AI Act. In any event, the European elections of June 2024 act as a natural deadline. If agreement is not reached before then, there may be a significant delay to the AI Act entering into force.

Interestingly with respect to the trilogues, some MEPs – the EPP Shadows – have reportedly now launched a short public consultation on the AI Act to help shape their strategy for the trilogues.

More generally, there is a growing sense that an appropriate framework to regulate AI needs to be adopted and to start applying rapidly, and this may be reflected in the trilogues. Also, given the pace of technological developments compared with the time required for legally binding rules to be agreed and to become applicable, various initiatives and measures are being discussed under the steer of the EU to anticipate upcoming 'hard law' on a voluntary basis. This includes, for instance, the AI Code of Conduct, which aims to establish a set of non-legally binding AI standards for stakeholders, and the AI Pact, which is intended as a commitment in terms of early compliance with the future AI Act by businesses.

Once enacted, the AI Act will be one piece of a broader regulatory landscape expected for AI, alongside laws such as the GDPR, the proposed AI Liability Directive and the proposed revision of the Product Liability Directive.

## **8. What should companies be doing?**

- Define your AI and tech strategy and governance, building on and seeking to leverage existing control frameworks.
- Map your existing and expected development and use of AI.
- Monitor the key AI regulatory, policy and market developments.
- Assess the impact of the AI Act and other key frameworks and laws around the world on your AI projects and plans.
- Consider participating in initiatives that are being developed to onboard industry, such as the AI Pact and the AI Code of Conduct.

# C L I F F O R D C H A N C E

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to [nomorecontact@cliffordchance.com](mailto:nomorecontact@cliffordchance.com) or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.