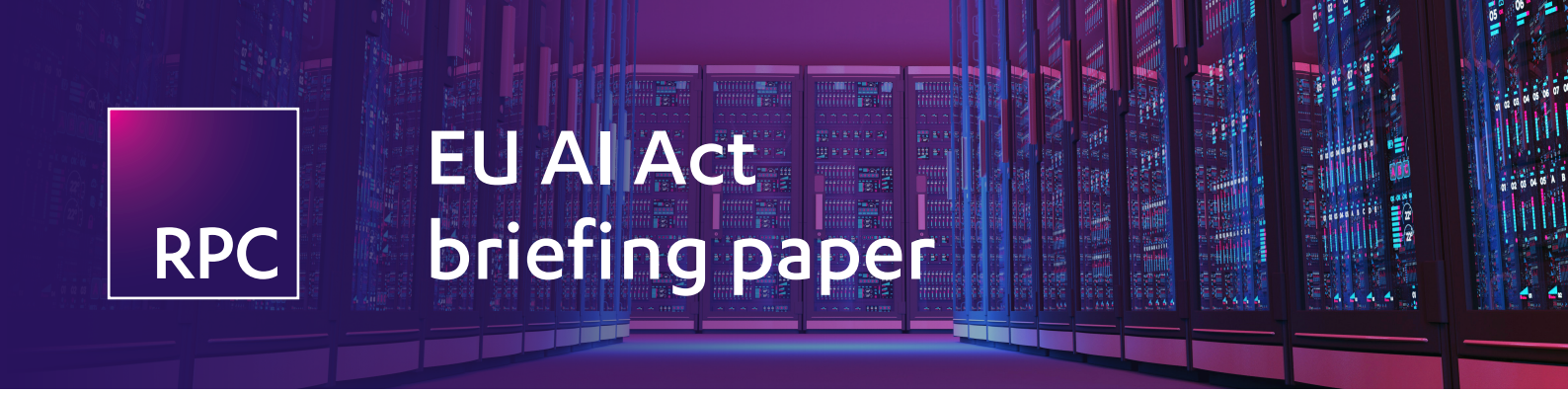

EU AI Act briefing paper

The EU's regulatory approach to the use of AI systems across the EU.

Brief timeline

- **February 2020** – Commission White Paper on Artificial Intelligence: A European approach to excellence and trust, 2020 proposing AI Act
- **April 2021** – EU Commission's Proposal for a Regulation laying down harmonised rules on AI
- **December 2022** – the Council unanimously adopted its General Approach
- **14 June 2023** – EP plenary session approved its negotiating mandate based on the Committee Report. **There were numerous proposed amendments in the Parliament text adopted on 14 June 2023**. The EP, Council and Commission negotiators can now start informal trialogue negotiations with the aim of reaching an agreement on the final text of the Regulation by the end of the year/early next year.
  - Procedure file
  - Adopted text (14.06.2023)
- **Next steps** – the proposed Regulation must be adopted under the ordinary legislative procedure, which means that following trialogue negotiations, both the EP and the Council, being co-legislators, will have to adopt the same final text before the Regulation can be formally adopted. It's possible this might happen this year or early next year. Once it becomes law it will trigger a two year grace period for compliance. Until then it will be subject to change.

Summary

The AI Act is based on a risk framework. The intention is to achieve proportionality by setting the regulation according to the potential risk the AI can generate to health, safety, fundamental rights or the environment. AI systems with an unacceptable level of risk to people's safety would therefore be prohibited.

The legal framework laid down in the AI Act will apply to both public and private actors inside and outside the EU as long as the AI system is placed on the EU market or its use affects people located in the EU. It covers all entities within the AI value chain from providers through importers and distributors to deployers.

Definition of AI

Unlike other jurisdictions like the UK, the AI Act provides (Art 3(3)) for a definition of an AI system:

> *'...a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.'* [latest definition from amended adopted text, 14 June 2023]

The definition of an AI system has narrowed with the latest (June) amendments.

Scope

It applies to providers, deployers, importers and distributors, product manufacturers and authorised representatives of providers of AI systems and affected persons that are located in the Union and whose health, safety or fundamental rights are adversely impacted by the use of an AI system that is placed on the market or put into service within the Union (Art 2).

General principles applicable to all AI systems

On 14 June, six general principles were added of: human agency and oversight, robustness and safety, privacy and data governance, transparency, diversity, fairness, and social and environmental well-being as relevant to all AI systems, these are not otherwise regulated under the EU AI Act (Art 4a).

There are also new requirements for providers and deployers/users of AI systems to ensure a sufficient level of AI literacy for staff and other persons dealing with the operation and use of their AI systems (Art 4b).

Risk-based approach

The AI Act takes a risk-based approach. Unacceptable risks are prohibited while those considered high risk are permitted on the EU market only when they comply with certain mandatory requirements. Providers of "non-high-risk" AI systems are to be encouraged to create codes of conduct intended to foster the voluntary application of the requirements applicable to high-risk AI systems, adapted in light of the intended purpose of the systems and the lower risk involved (recital 80).

Prohibited practices

The framework applies to AI systems and foundation models and (after outlining exemptions in Art 2 such as AI systems used for military purposes or AI R&D) **prohibits** certain AI practices (Art 5) including the placing on the market, putting into service or use of an AI system:

- that deploys subliminal techniques that materially distort behaviour causing significant harm
- exploits any of the vulnerabilities of a person or a specific group of persons, including characteristics or social or economic situation age, physical or mental ability with the objective or to the effect of materially distorting the behaviour of that person in a manner that causes or is likely to cause that person or another person significant harm
- or use of biometric categorisation systems that categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics
- for the social scoring evaluation or classification of natural persons
- for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics
- that creates or expands facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage
- that infers emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions
- that provides analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless they are subject to a pre-judicial authorisation in accordance with Union law and strictly necessary for the targeted search connected to a specific serious criminal offence.

"High risk" AI systems

AI systems that create adverse impact on people's safety, their fundamental rights or the environment.

These are categorised as:

- AI systems intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation law listed in Annex II (eg Machinery Directive 2006/42/EC; Safety of Toys Directive 2009/48/EC; Medical Devices Regulation (EU) 2017/745 etc) (Art 6(1))
- the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment related to risks for health and safety, with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation law listed in Annex II (Art 6(1))
- AI systems falling under one or more of the critical areas and use cases referred to in Annex III (including biometrics, critical digital infrastructure, employment and recruitment tools, access to essential services, law enforcement, migration and border control and judicial and democratic processes) where they pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Where an AI system falls under Annex III point 2 (critical infrastructure), it is considered to be high-risk if it poses a significant risk of harm to the environment (Art 6(2))

The AI Act specifies in Chapter 2 requirements for High-Risk AI Systems (risk management, data governance, technical documentation, record keeping, transparency obligations, human oversight, accuracy, robustness and cybersecurity). Chapter 3 specifies who is subject to each of those requirements and how.

On 14 June, AI systems used to influence voters and the outcome of elections and in recommender systems used by social media platforms (with over 45 million users) were added to the high-risk list.

New requirements for providers of foundation models

The 14 June amendments have introduced new requirements for providers of foundation models. Under Art 28 b a provider of a foundation model would have to assess and mitigate possible risks (to health, safety, fundamental rights, the environment, democracy and rule of law) and register their models in the EU database before their release on the EU market.

Generative AI systems based on such models would have to comply with transparency requirements (disclosing that the content was AI-generated, also helping distinguish so-called deep-fake images from real ones) and ensure safeguards against generating illegal content. Sufficiently detailed summaries of copyright protected data used for their training would also have to be made publicly available.

Recent geopolitical points

Ahead of diplomatic discussions on the AI Act, EU governments, led by Spain, have been considering the key issues to focus on for discussion and negotiation with the EP, including:

- the requirement (potentially very challenging) for AI developers to document and publicly share a detailed summary of the use of copyright protected training data
- the EP's (14 June amendments) new requirements facing providers of foundation models
- the proposed tougher pre deployment tests, facing providers of high risk AI systems, to consider an AI system's intended purpose and "reasonably foreseeable misuse"
- that, based on self assessment, AI systems are to be considered, with some narrow exceptions, high risk by default unless they "exceptionally do not pose a significant risk of harm to the protected legal interests"
- the tripling of maximum fines for breaches of the AU Act
- the AI Act coming into force much sooner than expected.

Talks resume between Spain on behalf of EU governments, the European Commission and parliamentary negotiators on 2 and 3 October.

Contacts

Helen Armstrong
Partner
+44 7912 519 732
helen.armstrong@rpc.co.uk

Charles Buckworth
Partner
T +44 20 3060 6641
M +44 7842 243 256
charles.buckworth@rpc.co.uk

rpc.co.uk