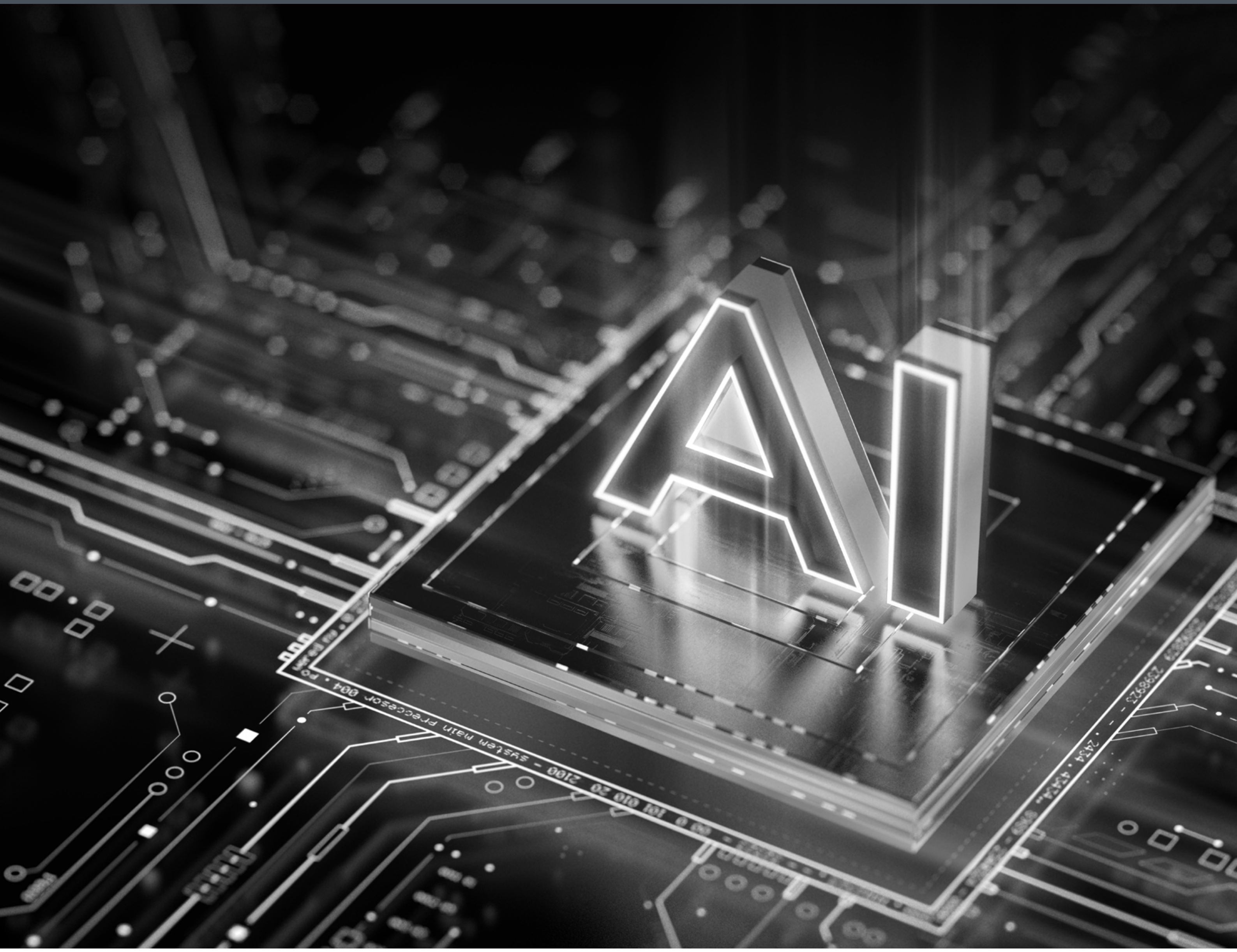
HFW

EU, COMPETITION AND REGULATORY | APRIL 2024



EUROPEAN PARLIAMENT APPROVES LANDMARK ARTIFICIAL INTELLIGENCE ACT

On 13 March 2024, the European Parliament formally approved the Artificial Intelligence Act (the AI Act).[1]

This represents another important step in the AI Act's entry into force, following a provisional agreement on the text being reached between the EU Council, the European Parliament and the European Commission (the **Commission**) on 8 December 2023[2], and the publication of the final compromise text on 26 January 2024.[3] First proposed in April 2021 by the Commission, the AI Act is expected to become one of the first, toughest and most

[1] European Parliament. *Artificial Intelligence Act: MEPs adopt landmark law.* Available at: Artificial Intelligence Act: MEPs adopt landmark law | News | European Parliament (europa.eu)

[2] We published a briefing in December 2023 detailing the negotiations leading up to the provisional agreement. Available at: Regulating AI - The EU agrees on landmark AI act

[3] European Council. *Public Register (5662/24) (26 January 2024).* Available at: pdf (europa.eu)

comprehensive regimes on artificial intelligence (**AI**) in the world.[4]

The AI Act seeks to ensure that AI systems which are used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly.[5] Its goal is to boost innovation and establish Europe as a leader in the field, whilst ensuring that there are adequate protections in place for fundamental rights, democracy, the rule of law and environmental sustainability.[6]

The AI Act will be applicable not only to providers of AI systems, but also to companies that use AI systems. Since it will apply to companies providing or using AI in the EU, the AI Act, as in the case of the General Data Protection Regulation (**GDPR**)[7], will have far-reaching extraterritorial impacts and carry implications for companies registered abroad conducting business in the EU.

The AI Act still requires a final lawyer-linguist check, and will need to be formally endorsed by the EU Council before it can enter into force. It will enter into force 20 days after its publication in the EU's Official Journal, and be fully applicable 24 months after its entry into force, except for certain provisions discussed further below which will apply respectively six, 12, and 36 months after its entry into force.[8] With this timeline in mind, the first prohibitions under the AI Act are not expected to become applicable until late 2024 at the earliest.

Definition

The AI Act seeks to enshrine in EU law a technology-neutral, uniform definition of 'AI system', wide enough to apply to present and future technological developments:

'An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'.[9]

Whilst many stakeholders welcomed the establishment of a legal definition, several expressed concerns in the consultation phase that, as drafted, the definition was too broad and would cover far more than what is currently subjectively understood as AI (including simple search, sorting, and routing algorithms, for example, software that sifts through job applications). There was apprehension that an overly broad definition could mean legal uncertainty for developers and operators, and could ultimately lead to over-regulation.[10]

In response, the European Parliamentary Research Service stated that the definition is not intended to apply to simpler traditional software systems or programming approaches. The Commission is expected to publish more detailed guidelines in due course.[11]

Risk-based approach

The AI Act establishes a risk-based approach to AI regulation, separating AI systems into multiple risk categories, each necessitating a different level of legal intervention. Four risk categories are identified, as described below.

Unacceptable risk

The following AI systems present an *'unacceptable risk'* and are prohibited because they pose a threat to people's safety, livelihoods and rights:

- AI systems using subliminal, manipulative or deceptive techniques to distort people's or a group of people's behaviour and impair informed decision-making, leading to significant harm;
- AI systems exploiting vulnerabilities due to age, disability, or social or economic situations, causing significant harm;
- Biometric categorisation systems inferring race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation (except for lawful labelling or filtering for law enforcement purposes);
- AI systems evaluating or classifying individuals or groups based on social behaviour or personal characteristics, leading to detrimental or disproportionate treatment in unrelated contexts or unjustified or disproportionate to their behaviour;
- 'Real-time' remote biometric identification in public spaces for law enforcement (except for specific necessary objectives such as searching for victims of abduction, sexual exploitation or missing persons, preventing certain substantial and imminent threats to safety, or identifying suspects in serious crimes);
- AI systems assessing the risk of individuals committing criminal offences based solely on profiling or personality traits and characteristics (except when supporting human assessments based on objective, verifiable facts linked to a criminal activity);
- AI systems creating or expanding facial recognition databases through untargeted scraping from the internet or CCTV footage;
- AI systems inferring emotions in workplaces or educational institutions, except for medical or safety reasons.[12]

[4] European Parliament. *Artificial intelligence act: Briefing*. Available at: Artificial intelligence act (europa.eu)

[5] European Parliament. *EU AI Act: first regulation on artificial intelligence*. Available at: EU AI Act: first regulation on artificial intelligence | Topics | European Parliament (europa.eu)

[6] European Parliament. *Artificial Intelligence Act: MEPs adopt landmark law*. Available at: Artificial Intelligence Act: MEPs adopt landmark law | News | European Parliament (europa.eu)

[7] Regulation (EU) 2016/679 (General Data Protection Regulation). Available at: Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu)

[8] Ibid.

[9] European Parliament. *Artificial intelligence act*: Briefing. Available at: Artificial intelligence act (europa.eu)

[10] Ibid.

[11] Ibid.

[12] Ibid.

> **"AI systems that are 'high-risk' are those that can potentially have a detrimental impact on people's health, safety, or fundamental rights. They are permissible, but must fulfil several requirements and obligations before they can gain access to the EU market."**

These prohibited systems will have to be phased out within six months of the AI Act entering into force.[13]

High risk

AI systems that are *'high-risk'* are those that can potentially have a detrimental impact on people's health, safety, or fundamental rights. They are permissible, but must fulfil several requirements and obligations before they can gain access to the EU market.

The AI Act identifies a number of *'high-risk'* use cases including:

- non-banned biometrics;
- critical infrastructure;
- education and vocational training;
- employment, workers management and access to self-employment;
- access to and enjoyment of essential public and private services (for example, healthcare, emergency first response, life insurance, and evaluation of creditworthiness);
- law enforcement;
- migration, asylum and border control management; and
- administration of justice and democratic processes.[14]

AI systems are always considered 'high-risk' if they profile individuals, i.e., automated processing of personal data to assess various aspects of a person's life, such as work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movement.[15]

All *'high-risk'* AI systems will be assessed before being placed on the market and throughout their life cycle.[16] They will need to comply with a range of requirements, including risk management, data governance, record-keeping, human oversight, and cybersecurity. In some cases, including those which involve deployers that are bodies governed by public law or private operators providing public services, a fundamental rights impact assessment will need to be conducted to ensure the systems are compliant with EU law.[17]

Obligations concerning *'high-risk'* AI systems will become fully applicable 36 months after the AI Act enters into force.[18]

Transparency risk

Certain AI systems present specific risks of impersonation and deception, particularly those that are built to interact with natural persons or generate content. Such systems are subject to the following information and transparency requirements:

- Users must be made aware if they are interacting with a chatbot;
- When publishing image, audio or video content that has been generated or manipulated by AI systems (i.e., deepfakes), deployers must disclose that the content has been artificially generated or manipulated (except in very limited cases, for example, when used to prevent criminal offences);
- If AI systems are capable of generating large quantities of synthetic content, providers must implement reliable techniques and methods (for example, watermarks) to show clearly that the content has been generated by an AI system and not a human;
- Employers who use AI systems in the workplace must inform their employees.[19]

In cases where a deepfake is generated for *"evidently"* artistic, creative or satirical work, the requirement to flag remains, but it may be done in an *"appropriate manner that does not hamper the display or enjoyment of the work"*.[20]

[13] Ibid.

[14] Annex III EU AI Act. Available at: Annex III: High-Risk AI Systems Referred to in Article 6(2) | EU Artificial Intelligence Act

[15] European Parliament. *Artificial intelligence act*: Briefing. Available at: Artificial intelligence act (europa.eu)

[16] European Parliament. *EU AI Act: first regulation on artificial intelligence.* Available at: EU AI Act: first regulation on artificial intelligence | Topics | European Parliament (europa.eu)

[17] European Parliament. *Artificial intelligence act: Briefing.* Available at: Artificial intelligence act (europa.eu)

[18] European Parliament. *EU AI Act: first regulation on artificial intelligence.* Available at: EU AI Act: first regulation on artificial intelligence | Topics | European Parliament (europa.eu)

[19] European Parliament. *Artificial intelligence act: Briefing.* Available at: Artificial intelligence act (europa.eu)

[20] Article 52(3) EU AI Act. Available at: Article 52: Transparency Obligations for Providers and Users of Certain AI Systems and GPAI Models | EU Artificial Intelligence Act

Low or minimal risk

AI systems which present minimal risk to people (for example, spam filters) will not be subject to obligations under the AI Act, but remain subject to currently applicable legislation, such as the GDPR.[21]

General-purpose AI

The AI Act also imposes specific rules on general-purpose AI (**GPAI**), which includes generative AI (for example, ChatGPT). The AI Act follows a two-tiered approach:

1. All GPAI model providers will have to ensure that they are compliant with EU copyright law and must publish detailed summaries of the content they use to train the GPAI models; and
2. Providers of GPAI models that pose a *"systemic risk"* to public health, safety, public security, fundamental rights, or society as a whole due to their *"high-impact capabilities"* (i.e., models trained using a total computing power in excess of 10^25 FLOPs) must notify the Commission of their status and will be required constantly to assess and mitigate the risks posed to ensure cybersecurity protection.[22]

Rules on GPAI will be fully applicable 12 months after entry into force of the AI Act.[23]

Sandboxing

The AI Act also puts into place measures to strengthen investment into AI systems. National authorities must now establish at least one AI *"regulatory sandbox"* with the aim of developing and testing nascent AI systems before their placement on the market or entry into service. These regulatory sandboxes will provide real-world conditions in a controlled environment, accelerating innovation with the benefit of strict regulatory oversight.[24]

Enforcement

A number of national and EU-level authorities will be responsible for implementation and enforcement. At the national level, Member States must establish at least one *"market surveillance authority"* and at least one *"notifying authority"* responsible for the application and implementation of the AI Act.

Notifying authorities will be responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of *"conformity assessment bodies"* (i.e., bodies that perform third-party conformity assessment activities, including testing, certification and inspection) and for their monitoring. Notifying authorities will notify conformity assessment bodies to the Commission and the other Member States.

At the EU level, the authorities responsible for implementing the AI Act include the Commission, the AI Board, the AI Office (which will develop codes of practice in support of the AI Act within nine months of its entry into force), the EU standardisation bodies (CEN and CENELEC), and an advisory forum and scientific panel of experts.[25]

The AI Act provides for a range of fines for non-compliance:

- €7.5m or 1.5% of a company's total worldwide turnover – whichever is higher – for giving incorrect information to regulators;
- €15m or 3% of worldwide turnover – whichever is higher – for breaching certain provisions of the AI Act, such as transparency obligations;
- €35m or 7% of turnover – whichever is higher – for deploying or developing banned AI tools.

Depending on the legal system of the Member States, administrative fines may be imposed by competent national courts or other bodies, such as national market surveillance authorities, as applicable in those Member States.

In each of the three breach categories above, fines imposed on small and medium-sized enterprises (**SMEs**) and start-ups will represent the lower (rather than the higher) of the two relevant figures.[26]

UK and other approaches to AI regulation

While the EU is set to adopt prescriptive legislative measures for AI regulation, President Biden has signed an Executive Order to promote *"Safe, Secure, and Trustworthy Artificial Intelligence"* in the US,[27] and China has issued guidelines to the effect that *"regulators will exercise classified and grading supervision over generative AI services"*.[28]

The UK Government has also recognised the importance of AI regulation and is seeking to establish the UK as a world leader in this sector. In November 2023, it hosted the inaugural global AI Safety Summit, attended by the EU and US amongst other AI leaders. On 6 February 2024, following a lengthy consultation period, the UK's Department for Science, Innovation & Technology (**DSIT**) published its highly anticipated *"pro-innovation approach"* to AI regulation.

The DSIT framework established a cross-sector and outcome-based approach to regulating AI, underpinned by five core principles:

[21] European Parliament. *Artificial intelligence act: Briefing.* Available at: Artificial intelligence act (europa.eu)

[22] Ibid.

[23] European Parliament. *Artificial Intelligence Act: MEPs adopt landmark law.* Available at: Artificial Intelligence Act: MEPs adopt landmark law | News | European Parliament (europa.eu)

[24] European Parliament. *Artificial intelligence act: Briefing.* Available at: Artificial intelligence act (europa.eu)

[25] Ibid.

[26] Article 71 EU AI Act. Available at: Article 71: Penalties | EU Artificial Intelligence Act

[27] On 30 October 2023, President Biden signed an Executive Order on Safe, Secure, and Trustworthy AI (available at: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House) placing wide-ranging safety obligations on AI developers, including a requirement for AI developers to perform safety tests and notify the government of the results before introducing any new products to the market.

[28] The State Council of the People's Republic of China. *China moves to support generative AI, regulate applications.* Available at: China moves to support generative AI, regulate applications (www.gov.cn)

- Safety, security and robustness;
- Appropriate transparency and explainability;
- Fairness;
- Accountability and governance; and
- Contestability and redress.[29]

Its aim is to boost innovation without compromising safety, by applying existing technology-neutral regulatory principles to AI. The UK Government has acknowledged that legislative action will eventually be required to address AI-related harms and ensure public safety (particularly with regard to GPAI systems), but maintains that to take such action now would be premature, since it does not yet fully understand the risks and appropriate mitigations as the technology is evolving so rapidly.[30]

Following the publication of its framework, DSIT has been in contact with a selection of leading UK regulators[31], requesting that they publish their strategic approach to AI regulation by 30 April 2024. Their plans will include the following:

- An outline of the measures to align their AI plans with the framework's principles;
- An analysis of AI-related risks within their regulated sectors;
- An explanation of their existing capacity to manage AI-related risks; and
- A plan of activities for the next 12 months.[32]

On 1 April 2024, following commitments made at the AI Safety Summit in November 2023, the UK and US signed a landmark bilateral agreement on AI safety, laying out plans to pool technical knowledge and capabilities for the purpose of co-operative AI testing.[33]

Next steps

The AI Act and the UK's AI regulatory framework are early stages in the global push towards AI regulation. Effectively implementing these regimes will present significant challenges to come, as will achieving the correct balance between fostering innovation and preserving safety. Future international cooperation in the field will also be very important.

However, the fact that the UK has opted for a soft law approach while the EU has implemented more prescriptive legislative measures shows that there is potential for divergence in this rapidly changing area. If the UK is to be a market leader in AI, its approach must secure international recognition and confidence.

Businesses should always keep in the forefront of their minds that the risk profile of any AI tool will always be impacted by the purpose of the tool: an AI tool used for basic customer insights will likely overcome data protection concerns more easily as the potential for harm to data subjects is lower. AI tools used for analysing specific customer behaviours and subsequent decisions will require more careful consideration of the associated risk. It will also be important to keep up to date with the direction of travel and development of AI tools and the evolving legislative and regulatory landscape, as well as tracking the risk appetite of customers and clients to the opportunities such AI tools present.

For further information, please contact:

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

SARAH HUNT
Partner, Geneva
T +41 22 322 4816)
E sarah.hunt@hfw.com

GEORGES RACINE
Partner, Geneva
T +41 22 322 4812)
E georges.racine@hfw.com

SARA ABHARI
Associate, Geneva
T +41 22 322 4818
E sara.abhari@hfw.com

Sam Rietbergen, Trainee Solicitor, London assisted in the preparation of this briefing.

[29] Department for Science, Innovation & Technology. *A pro-innovation approach to AI regulation: government response*. Available at: A pro-innovation approach to AI regulation: government response - GOV.UK (www.gov.uk)

[30] Ibid.

[31] The Government has written to the Office of Communications (Ofcom); Information Commissioner's Office (ICO); Financial Conduct Authority (FCA); Competition and Markets Authority (CMA); Equality and Human Rights Commission (EHRC); Medicines and Healthcare products Regulatory Agency (MHRA); Office for Standards in Education, Children's Services and Skills (Ofsted); Legal Services Board (LSB); Office for Nuclear Regulation (ONR); Office of Qualifications and Examinations Regulation (Ofqual); Health and Safety Executive (HSE); Bank of England; and Office of Gas and Electricity Markets (Ofgem). The Office for Product Safety and Standards (OPSS), which sits within the Department for Business and Trade, has also been asked to produce an update.

[32] Department for Science, Innovation & Technology. *A pro-innovation approach to AI regulation*: government response. Available at: A pro-innovation approach to AI regulation: government response - GOV.UK (www.gov.uk)

[33] Department for Science, Innovation & Technology. *UK & United States announce partnership on science of AI safety*. Available at: UK & United States announce partnership on science of AI safety - GOV.UK (www.gov.uk)

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, Competition and Regulatory capabilities, please visit hfw.com/EU-Competition-and-Regulatory.

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice. Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please email hfwenquiries@hfw.com

Americas | Europe | Middle East | Asia Pacific