Charles
Russell
Speechlys

The EU AI Act

A Beginner's Guide for UK and International Businesses Using AI

July 2024

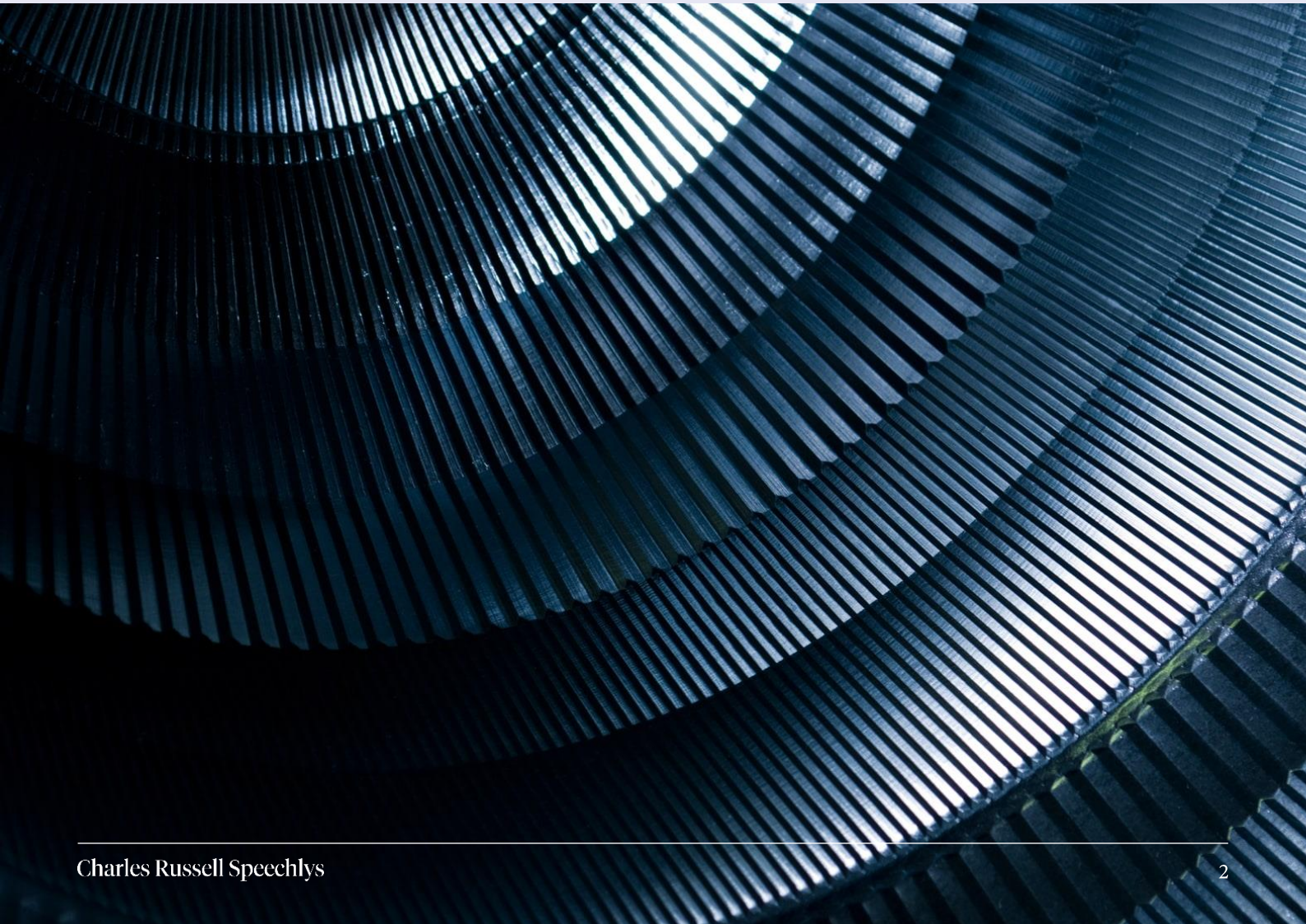
Introduction

After years of negotiations, the EU proposal for a Regulation laying down harmonised rules on artificial intelligence (the AI Act) has finally been agreed and was published in the Official Journal on 12 July 2024. It will enter into force 20 days later on 1 August 2024.

Following on from our AI Business Guide, this guide seeks to outline the implications of the new AI Act for businesses that are using AI, and may therefore be subject to the AI Act's provisions.

Most importantly, we will tell you what practical steps you need to take to comply with the new obligations, given the requirement that all persons in the AI supply chain (including those placing AI systems on the market, putting into service, and using AI systems) must comply with the AI Act to varying degrees, as well as the significant fines that are being introduced for those who fail to do so.

This guide focuses on users of AI, known as "deployers" under the AI Act. Deployers are defined in Article 3 to include a natural or legal person using an AI system under its authority except where it is used in the course of a personal non-professional activity. Our guide does not focus on the obligations of providers, importers or distributors of AI systems.



Key questions for users of AI

Does the EU AI Act apply to UK businesses?

The AI Act clearly applies to businesses that use AI and are located or established within the EU, but just like the EU General Data Protection Regulation (GDPR), the AI Act has extra-territorial effect (as set out in Article 2). This means that it also applies to organisations whose place of establishment or location is outside of the EU where the output produced by the AI system is used in the EU. The recitals to the AI Act give the example of an operator in the EU obtaining services from a business using AI outside the EU, which would be classified as high-risk under the AI Act.

It is also possible that some UK businesses, as well as international businesses, will seek to understand the approach that the AI Act takes to risk assessment and regulation of AI as a benchmark for their internal assessments of AI deployment. This is a relatively common approach for international businesses. There is a risk of gold plating, but a consistent evaluation of risk across a business, as well as a consistent approach to governance and risk management up to and including Board level, is increasingly necessary for businesses to meet their corporate governance and cyber risk management responsibilities.

Are there any exceptions?

Yes, certain AI systems are excluded, including AI systems that are:

- solely for scientific research and development;
- for personal, non-professional activities;
- for research, testing and development of AI systems or models prior to being put on the market/into service (i.e. in a controlled environment such as a laboratory or other simulated environment); or
- released under free and open-source licences, unless they are "prohibited" or "high-risk" AI systems or are designed to interact directly with natural persons.

What AI is covered by the EU AI Act?

AI is defined in the AI Act as "a machine-based system that is 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". The emphasis on autonomy and inference takes it beyond predetermined automation processes. We are expecting further guidelines regarding this definition within the next six months.

The AI Act addresses specific categories of AI:

Prohibited	High-Risk	Limited Risk	Minimal Risk	General Purpose AI
AI that presents an unacceptable risk to EU citizens.	AI that creates a high risk to the health and safety or fundamental rights of EU citizens.	Risks associated with lack of transparency about AI usage.	Generally simple tasks with no interaction with EU citizens	General purpose AI systems (GPAI) have a broad range of uses (Chat GPT, Siri, Google Assistant, Alexa and Google Translate). They are trained on a large amount of data and can competently perform a wide range of tasks, regardless of the way the model is placed on the market. GPAI systems can also be integrated into a variety of downstream systems or applications.

Your obligations

We will address the obligations in relation to the different types of AI below.

What are the timeframes to comply with the EU AI Act?

Whilst the AI Act will come into force on 1 August 2024, different provisions will start to apply at different times:

- most provisions of the AI Act will apply 24 months after entry into force (2 August 2026);
- provisions relating to prohibited AI systems will apply after 6 months (2 February 2025);
- obligations on employers relating to AI literacy will apply after 6 months (2 February 2025);
- obligations on providers of GPAI after will apply after 12 months, as will provisions relating to penalties (2 August 2025);
- provisions relating to high-risk AI systems under Annex I (AI systems forming a product or safety component) will apply after 36 months (2 August 2027).

The EU Commission has launched the AI Pact, a scheme under which businesses are encouraged to commit (on a voluntary basis) to comply with certain obligations of the AI Act before the regulatory deadlines.

What is the penalty and enforcement regime?

Non-compliance with the AI Act could lead to significant fines for users of AI:

- prohibited AI infringements: up to the greater of 7% of global annual turnover or EUR35m;
- high-risk and transparency infringements: up to the greater of 3% of global annual turnover or EUR15m;
- the supply of incorrect information: up to the greater of 1.5% of global annual turnover or EUR7.5m;
- for SMEs, including start-ups, the fines are capped at the lower of the percentage of global turnover or the fixed amount.

The European Commission established the EU AI Office on 29 May 2024. The AI Office operates within the Commission to support the implementation and management of the AI Act. The intention is that it will also work to foster research and innovation in trustworthy AI and position the EU as a leader in international discussions. The Office aims to ensure the coherent implementation of the AI Act. It will do this by supporting the governance bodies in Member States. The AI Office will also directly enforce the rules for GPAI models.

The AI Office is preparing guidelines on the AI system definition and on the prohibitions, both due six months after the entry into force of the AI Act. The Office is also getting ready to coordinate the drawing up of codes of practice for the obligations for GPAI models, due 9 months after entry into force.

The EU AI Board will work alongside the AI Office. It is potentially similar to the European Data Protection Board under the GDPR. The AI Board comprises representatives from each Member State and will advise and assist the Member States with the consistent and effective implementation of the AI Act. The first meeting of the upcoming AI Board took place on 19 June 2024 to set the groundwork for the formal entry into force of the AI Act.

Each EU Member State will need to appoint a "Market Surveillance Authority" (MSA). MSAs will enforce the EU AI Act on a national level.

How does the EU AI Act regulate AI?

As mentioned above, the AI Act takes a risk-based approach to regulation. It is possible for an AI system to fall within more than one category. Obligations are set out in relation to each category below.

General Purpose AI

The AI Act imposes specific obligations on the providers of GPAI models and additional obligations on providers of GPAI models with systemic risk. This is to address concerns that some models could carry systemic risks if they are very capable or widely used. For example, powerful models could cause serious accidents or be misused for far-reaching cyber-attacks. For the purpose of this guide, it is important to note that business users of GPAI will be subject to the rules set out below.

Prohibited AI

Some types of AI which present an unacceptable risk to EU citizens are completely prohibited. For example, AI systems that deploy subliminal, manipulative or deceptive techniques which materially distort a person's behaviour and are likely to cause significant harm, and AI systems that evaluate or classify people based on their social behaviour or personality characteristics, leading to detrimental or unfavourable treatment. There is a detailed list of prohibited AI in Article 5.

> ### Practical Tip
>
> Most organisations now have a Responsible AI policy (if you don't yet, consider getting one!). If you fall within the jurisdiction of the AI Act, you should now amend this policy to make sure that your list of "prohibited AI uses" reflects the "banned" AI under the EU AI Act.
>
> The reality is that it is unlikely that your organisation knowingly engages in these banned activities in any event, but the prohibitions are broadly stated, and the categories of prohibited AI should be considered and reflected in your policy so that it's clear that you are ensuring consistency with the AI Act. Even if you do not currently fall within the AI Act's territorial reach, businesses may take the view that the EU is leading the way in best practice and compliance with its key provisions should form part of responsible AI governance.
>
> However, as noted above, this is a nuanced decision and may not be suitable for all businesses either from a cost or governance perspective.

High-Risk AI

Most of the obligations in the AI Act apply to AI that is "high-risk." An AI system is high-risk if it is a safety component or a product covered by EU legislation listed in Annex 1 of the AI Act; and is required to undergo a third-party conformity assessment pursuant to that legislation.

In addition, Annex III to the AI Act lists AI systems that fall into the high-risk category. There are certain derogations from this list in specified circumstances which lower the significant risk (set out in Article 6 (3)). The Commission may update this list by adopting delegated acts and will also publish guidelines with practical examples of high-risk and non-high risk use cases. There will be a database of high-risk systems, so it will be possible to check this database before deploying a specific AI system.

Whilst many of the high-risk areas will not apply to most organisations, some areas will be relevant to a lot of organisations. For example, AI systems will be considered to be high-risk if they are intended to:

- be used for recruitment or selection, notably to place targeted job advertisements, to analyse and filter job applications and to evaluate candidates; or
- make decisions about promotions, termination, allocate tasks based on individual behaviours, personal traits or characteristics, and monitor and evaluate performance and behaviour.

Given the increasing number of AI-powered tools on the market designed to make the sourcing and hiring of employees easier, HR teams will need to be cognisant that the requirements of the AI Act relating to high-risk AI may be triggered more often than not. This is particularly given that, although most of the obligations apply to the providers of high-risk AI systems, there are also obligations on deployers of high-risk AI systems (see below).

Financial institutions also need to be aware that AI systems intended to evaluate creditworthiness or establish credit score will also be high-risk, as will AI systems that are intended to be used for risk assessment and pricing in relation to life and health insurance.

If you are considering deploying an AI system, you will need to establish if it is a high-risk AI system and perform some initial analysis for these purposes. Deployers of high-risk AI systems have direct obligations under Article 26 of the AI Act, which include:

- taking appropriate technical and organisational measures to ensure you use such systems in accordance with the accompanying instructions for their use;
- assigning human oversight to the AI system to someone who has the requisite competence, training and authority, as well as the necessary support;
- monitoring the operation of the high-risk AI system, including informing the provider or distributor of the AI system and the relevant MSA if certain risks present (i.e. present health, safety or fundamental rights risks), or if there is a "serious incident", and suspend use;
- ensuring that input data that the deployer has control over is relevant and sufficiently representative in the view of the intended purpose of the high-risk AI system;
- keeping the logs automatically generated by the high-risk AI system if the logs are under their control for at least 6 months;
- informing employees' representatives and the affected employees that they will be subject to the system;
- using the information provided by the provider to carry out a Data Protection Impact Assessment.

It is important to note that in certain circumstances deployers of high-risk AI systems may become providers (as defined in the AI Act) of a high-risk system and have additional associated obligations. These include deployers who apply a trade mark to a high-risk system already on the market, make substantial modifications to a high-risk system or make modification to an AI system (including GPAI), rendering it high-risk (Article 25).

Practical Tip

Consider who the most appropriate person is within your organisation to have oversight over high-risk AI systems and write this in your Responsible AI policy. The AI governance profession is still developing, but data privacy professionals and their professional associations are taking the helm in this area given the similarities and overlap between the two fields. So, perhaps your Data Protection Officer may be the most appropriate person to oversee compliance, or otherwise someone with the necessary technical skills and appropriate seniority to understand the operation of the AI system in your business.

In the UK, cyber is a board level responsibility. However, there are also general duties on directors in the Companies Act 2006 to promote the success of the company, including giving regard to the likely consequences of a decision. There will be an increasing obligation on Boards to ensure they identify, understand and mitigate risks to the business, and this will include the deployment and use of AI. This cannot simply be delegated.

Make sure that teams involved in commissioning or deploying these types of AI systems understand that they are "high-risk" and that they should not engage with providers of these systems without full consideration (and sign-off) of the legal ramifications. It is also worth giving careful consideration to any customisation of third-party AI systems. As with prohibited AI, make sure that your Responsible AI policy is updated to specify what types of AI systems are "high-risk".

Transparency Obligations: Article 50

Risks associated with lack of transparency in AI usage are considered to be limited risk. Certain AI systems are subject to transparency obligations, including those used or intended to be used:

- to interact directly with EU citizens (for example, chatbots);
- to generate synthetic audio, image, video or text content (including GPAI);
- to generate or manipulates images, audio or video content as “deep fakes”;
- for text generation or manipulation published to inform the public on matters of public interest.

These systems require the provision of specific information to individuals in a clear and distinguishable manner. This includes informing individuals that they are interacting with AI and disclosing that content has been artificially generated or manipulated. The AI Office will facilitate the drawing up of codes of practice to support compliance. It is important to note that these obligations are in addition to any obligations that are imposed if a system is also considered to be high-risk.

Practical Tip

Although users of AI may not be subject to the same obligations as providers, they will need to think about the increased obligations that are being imposed when procuring an AI system. Contracts will look to ensure that parties are clear about their roles in the AI supply chain and that they can and will comply with the various obligations. They may also need to address potential changes in regulation during the contractual relationship.

The standard EU Commission model clauses drafted for use by public organisations procuring AI systems provide an indication of the issues that private businesses should be looking to address in their contracts, including data governance, transparency and design. Bodies such as the Society for Computers and Law are also looking to publish guidance and sample clauses to assist with the contractual implications of the AI Act.

Minimal Risk/All AI Systems

Users must ensure that their staff have a sufficient and appropriate level of AI literacy when using AI systems on their behalf and considering persons on whom the AI systems are to be used (Article 4). They are also encouraged to implement voluntary codes of conduct (Article 95).

Practical Tip

Much day-to-day use of AI will fall within the limited / minimal risk category. However, businesses should ensure that appropriate AI policies are created and managed internally and that transparency notices are published. Internal training on the use and deployment of AI is essential and particular focus should be on ensuring safe use and avoiding ingesting data into models that may infringe the intellectual property rights of third parties. All businesses must also ensure that governance is embedded in the business to manage AI deployment and use in a safe environment.

Charles Russell Speechlys

Contact us

If you have any questions please contact:

Janine Regan
Legal Director

+44 (0)20 7427 1074
janine.regan@crsblaw.com

Louise Zafer
Knowledge Development Lawyer

+44 (0)20 7203 8948
louise.zafer@crsblaw.com