Freshfields Bruckhaus Deringer

The EU's proposed AI Regulation

What you need to know

Technological advances in the field of artificial intelligence have brought about sweeping economic and societal benefits, with an exponential boom in the development and deployment of AI systems across sectors. AI sits at the heart of the global trend towards digitalisation and its various applications have huge potential to improve the ways in which businesses run and in which we, as consumers, interact with them and with each other.

However, with new technological benefits come risks and regulation. On 21 April 2021, the European Commission published its draft legislative proposal on artificial intelligence (the **AI Regulation**). The AI Regulation attempts to strike a balance between addressing perceived risks linked to AI, on the one hand, and not unduly constraining or hindering technological development or otherwise increasing the cost of placing AI solutions on the market, on the other. Some commentators have already suggested that it is more successful at the former than the latter.

Although the AI Regulation will not come into force until it has passed through the European legislative process, the significant regulatory requirements in the proposed text cannot be ignored. The AI Regulation will play a key role in shaping how AI is developed in the EU and will likely also serve as a blueprint for other regulatory authorities around the world contemplating similar regulation. It could also provide another opportunity to test the new and emerging relationship between the EU and the US on technology and data issues.

The AI Regulation encompasses a wide-ranging set of rules seeking to regulate the pervasive use of AI across a spectrum of industries and social activities, with rule breakers facing the possibility of fines of up to 6% of global turnover. It is a culmination of three years of work, during which the Commission undertook extensive consultations with industry and wider society, receiving more than 1,200 responses worldwide on its February 2020 White Paper alone.

At its core, the AI Regulation proposes a sliding scale of rules based on risk: the higher the perceived risk, the stricter the rule. This, the Commission believes, will allow legal intervention to be tailored to those situations where it thinks there is justified cause for concern or where such concern can reasonably be anticipated in the near future.

We outline below which businesses are affected by the AI Regulation, what they need to know and how they should be approaching compliance in the future.

Who and what is subject to the AI Regulation?

The AI Regulation has a wide reach:

- ***Actors***. The AI Regulation will apply to various participants across the AI value chain, covering both public and private actors inside and outside the EU as long as the AI system is placed on the EU market or the output produced by the system (such as content, predictions, recommendations, or decisions) is in the EU. Strict requirements may apply inter alia to providers, users, end-product manufacturers, importers or distributors, depending on the risk associated with the AI system.
- ***Broad-brush definition of AI***. An AI system is defined as software that is developed with machine learning, logic- and knowledge-based or statistical approaches which can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

The remit of the AI Regulation goes beyond modern machine learning systems that learn to make decisions themselves, also capturing systems that operate according to hard coded rules, which have long been embedded in a wide variety of applications (from flight control to pacemakers to industrial settings). The Commission's expansive approach means virtually all systems that currently do, or which may in future, use AI would fall within scope – from personalised pricing, advertising and feed algorithms, to connected IoT systems, self-driving cars, or applications used to support recruitment and other business processes.

A sliding scale based on risk

The AI Regulation focuses on when, where and how AI is developed, marketed, and used. Every application and use case of AI will fall into one of four different risk categories: **unacceptable, high, limited** and **minimal**, with differing degrees of regulation applying to each. The higher the risk, the stricter the requirements.

The AI Regulation also contains future-proofing provisions allowing for additions and/or expansions to these categories, and the examples contained within them, to cover emerging uses and applications of AI.

'Unacceptable risk' – prohibited

There is an outright prohibition on certain AI systems which the Commission deems to pose an unacceptable level of risk, ie which are assumed to be particularly harmful and to contradict values of respect for human dignity, freedom, equality, democracy and the rule of law and EU fundamental rights. This is an exhaustive list which, in summary, focuses on:

- AI systems that distort human behaviour in a manner causing physical or psychological harm by deploying subliminal techniques or by exploiting vulnerabilities due to the person's age or physical or mental disability.
- AI-based social scoring systems deployed by public authorities leading to the detriment of individuals or groups of people.
- AI systems used for real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement, subject to a number of exceptions.

While the latter two categories are focussed on public authorities and law enforcement, the first category is more relevant to private actors' own interactions with end-users. Certain AI applications could be said to involve 'deploying subliminal techniques' to influence human behaviour. The limiting factor set by the AI Regulation is the causation of physical or psychological harm, but this is not explicitly defined in the regulation. If that remains the case in the final regulation, what amounts to psychological harm may be a key battleground in any future AI disputes.

'High risk' – strictly regulated

High-risk AI systems are those which affect human health and safety, or which involve the use of intrusive data analytics and profiling that could affect fundamental rights. Such systems will need to undergo a conformity assessment procedure to verify that they comply with a set of specifically designed high-risk requirements (explained below), following which a written declaration of conformity must be drawn up, a CE mark applied and the AI system registered in a new EU database to be set up by the Commission.

High-risk AI systems are split into two categories:

- ***Safety products/components.*** This covers AI systems which are used as safety components in products (or are themselves products) that are already subject to existing conformity assessment systems under specific EU harmonisation legislation. For example, existing EU regulations require cars, medical devices and industrial machinery to be assessed for conformity with various essential safety requirements before they can be placed on the market. Once the AI Regulation comes into force (along with any relevant secondary legislation, eg implementing acts specific to automated vehicles), these existing conformity assessments will also include compliance with the high-risk requirements described below. This would cover, for example, the use of machine learning in an autonomous vehicle or an AI-enabled pacemaker.
- ***Specific uses of AI in sensitive sectors with fundamental rights implications.*** This covers AI systems which are not used in situations that are already subject to EU harmonisation legislation, as above, and which fall into one of eight areas listed in Annex 3 to the regulation.

High-risk applications (Annex 3)

1. AI used for **biometric identification and categorisation of natural persons**
2. AI used as safety components in the **management and operation of critical infrastructure**, such as the supply of utilities
3. AI used for determining access to, and assessments in, **educational and vocational training**
4. AI used in **employment, workers management and access to self-employment**, including the use in recruitment, task allocation or monitoring and evaluating performance
5. AI used to evaluate the creditworthiness of individuals or their credit score, or in certain other manners that determines **access to and enjoyment of essential private services and public services and benefits**
6. AI used in **law enforcement** for individual risk assessments or as polygraphs
7. AI used for assessing security risks in **migration, asylum and border control management**
8. AI used to assist a judicial authority in the **administration of justice and democratic processes**

Products or services which fall into these use cases will be subject to self-assessment conformity obligations to confirm compliance with the high-risk requirements described below, with the exception of systems for biometric identification and categorisation of natural persons, which will be subject to conformity assessment by an external testing body.

Because these high-risk requirements are wide-ranging (see below), conformity assessments of any kind will impose significant burdens on those who develop, market or use AI applications falling into either category. The impact may vary by sector and use case. Systems for the management of critical infrastructure are already tightly regulated and controlled, and those responsible for them will be used to operating within a complex regulatory framework. In contrast, providers and users of biometric scanners or recruitment software may find these changes more demanding. The AI Regulation seems particularly keen to tighten protections around algorithmic bias and discrimination in the work place, and performance management algorithms – such as those found to be discriminatory to certain categories of riders in a recent ruling by an Italian tribunal concerning an algorithm used by a food delivery platform – would be treated as high-risk applications.

At the same time, AI developers will welcome the Commission's stance that only self-assessment conformity is required for most high-risk AI systems, saving them from having to disclose their algorithms and underlying training data to external testing bodies for review, thereby ensuring that intellectual property protections and trade secrets for those assets are not compromised.

'Limited risk' – enhanced transparency

The AI Regulation identifies three categories of AI systems which, while not necessarily 'high-risk', will need to fulfil requirements in terms of transparency:

1. AI systems that interact with natural persons will need to be designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and context.
2. Emotion recognition or biometric categorisation systems must inform end-users that they are exposed to such a system.
3. AI systems that generate or manipulate content to resemble existing persons, objects, places or other entities or events, so that the content would falsely appear to a person to be authentic (ie a 'deep fake'), must disclose that the content has been artificially generated or manipulated.

These applications do not, however, need to comply with the high-risk requirements (below) or undergo conformity assessment, unless they separately constitute high-risk applications (eg an AI system with which employees interact in order to obtain access to vocational training).

'Minimal risk' – no additional restrictions

The EU expects that the 'vast majority' of AI technology will fall into the minimal-risk category, which is free to develop and use with no restrictions on top of any relevant existing legislation (this category is not formally listed in the legislative proposal but is detailed in the Commission's Q&As published alongside the proposed AI Regulation). No conformity assessment is required for such technology. Examples would include email spam filters and mapping products used for route planning.

At the same time, the Commission and the newly formed European Artificial Intelligence Board (see below) will encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application of the mandatory requirements for high-risk AI systems even for those AI systems that do not fall within the high-risk category.

High-risk requirements

High-risk AI systems must comply with several mandatory requirements before the system can be placed on the market or put into service, or before its output can be used in the EU. Conformity assessment (as described above) is intended to certify that the system in question meets these requirements:

1. **Risk management systems** must be established, implemented, documented, maintained and regularly updated. The risk management system must identify and analyse foreseeable risks associated with the AI and eliminate or reduce those risks to the extent possible and otherwise implement control measures in relation to those risks.
2. **Data and data governance**. High-risk AI systems which involve training models with data must use training, validation and testing data sets which are subject to appropriate data governance and management practices, are relevant, representative, free of errors and complete, and take into account the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the AI system is intended to be used.
3. **Technical documentation**, containing as a minimum the information detailed in Annex IV, including a detailed description of the elements of the AI system and the process of its development, must be drawn up before the AI systems are placed on the market or put into service, and must be kept up-to-date.

4. **Record keeping**. High-risk AI systems must have logging capabilities ensuring traceability of the AI system's functioning throughout its lifecycle, at a level appropriate to its intended purpose.
5. **Transparency and provision of information to users**. The operation of high-risk AI systems must be (i) sufficiently transparent to enable users to interpret the AI system's output and use it appropriately; and (ii) accompanied by instructions for use, including any known and foreseeable circumstances that may lead to risks to health and safety or fundamental rights, human oversight measures, and the expected lifetime of the high-risk AI system. The information must be concise, complete, correct and clear, and must be relevant, accessible and comprehensible to users.
6. **Human oversight**. High-risk AI systems must be capable of being overseen by natural persons, with the aim of preventing or minimising risks to health, safety or fundamental rights. The provider is to identify and build (where possible) oversight measures into the AI system. The designated individual should fully understand the capacities and limitations of the AI system and be able to monitor its operation and output for signs of anomalies, dysfunctions and unexpected performance. Humans should be able to intervene and stop the system.
7. **Accuracy, robustness and cybersecurity.** High-risk AI systems must, in light of their intended purpose, be appropriately accurate, and the accuracy metrics must be declared in the accompanying instructions of use. The systems must also be appropriately robust and resilient to errors, faults or inconsistencies and resilient to third parties intending to exploit system vulnerabilities, including data poisoning and adversarial examples.

These high-risk requirements will be onerous to comply with. Potential issues include:

- The requirement that data sets be 'representative' does not sit easily with GDPR requirements regarding sensitive personal data. Similarly, a provider of a high-risk AI system is allowed to process the GDPR special categories of personal data for the purposes of ensuring bias monitoring, detection and correction in those systems, subject to certain safeguards. But minimal detail is provided as to what those safeguards would encompass.
- The requirement that data used to train AI systems be 'free of errors and complete' may well be unachievable in practice, given the scale of the data sets used in machine learning.
- The requirement, in certain circumstances, for a designated individual to be able to 'fully understand' the operation of a complex AI system, sets a very high bar; this is unlikely to be an attractive role for anyone to take on.
- Traceability requirements may pose problems for certain deep learning AI systems, where it is difficult to clearly explain and trace how the system is functioning.

On whom do these obligations fall?

A **Provider** is anyone who develops an AI system, or has it developed with a view to putting it on the market or into service under its own name or trademark. Providers of high-risk AI systems have primary responsibility for ensuring compliance with the AI Regulation. They must:

- ensure that the AI system complies with the high-risk requirements
- manage the conformity assessment procedures and inform national competent authorities of any non-compliance
- put in place a post-market monitoring system to collect, document and analyse data throughout the lifetime of the AI system and to evaluate the AI system's continuous compliance
- a third party will also be treated as a provider if, for example, it places on the market or puts into service an AI-enabled product under its own name or brand, or makes a substantial modification to an existing high-risk AI system

A **User** is anyone deploying an AI system under its authority, but does not include personal and non-professional uses (eg everyday consumers). Users have more limited obligations than providers, but still have various monitoring and information obligations:

- use the AI systems in accordance with the instructions of use
- ensure that input data is relevant in view of the intended purpose of the AI system
- monitor the operation of the AI system on the basis of the instructions of use
- inform the provider or distributor of any risk to health and safety or fundamental rights
- keep automatically generated logs to the extent that such logs are under their control

Manufacturers of products which are already regulated under EU sectoral legislation (cars, medical devices etc) and which use high-risk AI, are subject to the same obligations as providers. There are also obligations on **importers** and **distributors** of high-risk AI systems.

Governance and penalties

The AI Regulation proposes the establishment of a new European Artificial Intelligence Board composed of representatives from the Member States and the Commission to assist with implementation. Its intended role seems to be similar to that of the European Data Protection Board (EDPB), as regards GDPR.

The AI Regulation provides for a significant set of tiered fines, up to:

€30m or 6%of total worldwide annual turnover
for non-compliance with the prohibition on unacceptable-risk AI systems or the data governance requirements

€20m or 4%of total worldwide annual turnover
for non-compliance with any other requirement or obligation

€10m or 2%of total worldwide annual turnover
for supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities, in reply to a request

Looking ahead

The AI Regulation will apply (with limited exceptions) to AI systems that are placed on the market, put into service, or high-risk AI systems that have significantly changed, two years after the AI Regulation enters into force. An AI system's inherent adaptation on the basis of its machine learning application does not constitute significant change.

However, the AI Regulation is still a draft, and it will need to pass through the European legislative process – this includes a review by the European Parliament, which has previously voiced the need for broad regulation, as well as the Member States. Given the degree of interest shown in the AI Regulation even before its publication, that legislative process is likely to be protracted. We expect inter-institutional negotiations to finalise the text will take between 18 and 24 months, and the regulation could theoretically apply as from early/mid 2024.

We expect considerable debate in the European Parliament as to which committee takes the lead on the proposal, given that many have prepared reports to guide the future legislation. MEPs are likely to seek to toughen the proposal, including likely pushback on the exceptions provided to law enforcement to deploy prohibited uses and the fact that quality management and conformity assessment procedures are only needed for high-risk AI systems. In addition, there is broad scepticism with regard to the creation of another body (the European Artificial Intelligence Board) that could wield material power in deciding what gets added to or taken out of the high-risk and the prohibitions lists (especially when many consider that the European Data Protection Board could perform this function).

Beyond the AI Regulation, wide-ranging though it is, the EU is also considering how other aspects of emerging technologies such as AI should be regulated. For example, it remains to be seen whether proposals will follow to amend the rules governing businesses' liability to consumers for harm caused by AI-enabled products.

What are the top points I should be thinking of today if…

I'm a provider or user of AI

- Get ready for the new regulation by assessing the likely impact of the proposal on your business and by developing mature AI governance frameworks.
- Engage with the EU institutions as the proposed regulation is examined and amended: the AI Regulation is still at an early stage of the legislative process and it is likely that Member States in Council and MEPs will be actively seeking input from stakeholders. This could be done individually, or via trade associations, a number of which have already been actively working on the Commission's AI work streams. These include DIGITALEUROPE, DOT Europe, MedTech Europe, EuroCommerce and AmCham EU, to name a few.
- Monitor the development of this regulation, and related changes in areas such as liability, in the months ahead.

I'm investing in AI

- Assess which risk category any target AI systems would fall into and whether there is a risk that these systems shift between risk categories with future technological advances or regulatory amendments.
- Understand the extent to which a target business complies (or can easily be made compliant) with likely future regulatory requirements, in the same way that preparedness for GDPR was assessed in the past. Consider, in particular, whether AI systems are so deeply integrated into applications that they will be difficult to adapt to fit with future regulation.
- The EU believes development and commercialisation of AI will be driven by public trust. Assess whether the target is at a level where it could promote and explain the trustworthiness of its AI.
- Diligence whether any target AI systems are built on third party component AI systems, models or datasets – and test whether the business has appropriate licences to use them.
- Consider the global direction of regulatory travel: assess where the target operates its AI systems and consider whether other jurisdictions will pass similarly strict regulation. EU officials say Japan and Canada are already taking a close look at its proposal.

Key contacts

Natalie Pettinger Kearney
Deputy Head of EU Regulatory & Public Affairs
T +32 2 504 7184
E natalie.pettingerkearney@freshfields.com

Giles Pratt
Partner
T +44 20 7716 4339
E giles.pratt@freshfields.com

Andrew Austin
Partner
T +44 20 7716 4048
E andrew.austin@freshfields.com

Christoph Werkmeister
Partner
T +49 211 49 79 189
E christoph.werkmeister@freshfields.com

Sascha Schubert
Partner
T +32 2 504 7039
E sascha.schubert@freshfields.com

Ben Cohen
Associate
T +44 20 7427 3192
E ben.cohen@freshfields.com

freshfields.com

This material is provided by the international law firm Freshfields Bruckhaus Deringer LLP (a limited liability partnership organised under the laws of England and Wales authorised and regulated by the Solicitors Regulation Authority (SRA no. 484861)) and associated entities and undertakings carrying on business under, or including, the name Freshfields Bruckhaus Deringer in a number of jurisdictions, together referred to in the material as 'Freshfields'. For further regulatory information please refer to www.freshfields.com/support/legal-notice.

Freshfields Bruckhaus Deringer has offices in Austria, Bahrain, Belgium, China, England, France, Germany, Hong Kong, Italy, Japan, the Netherlands, Russia, Singapore, Spain, the United Arab Emirates, the United States of America and Vietnam.

This material is for general information only and is not intended to provide legal advice.