Key provisions of the Draft AI Regulation

24 May 2021

On 21 April 2021, the European Commission published its proposal for the Artificial Intelligence Regulation (the Draft AI Regulation).

It is the world's first concrete proposal for regulating artificial intelligence (AI). The Draft AI Regulation is likely to profoundly affect the debate on AI and ultimately the way that companies, both small-scale startups and large tech giants and their clients, as well as governments and law enforcement can use AI.

An earlier draft version was leaked a week before the official publication date, but there are significant changes in the final proposal which were not present in this earlier version, including with respect to fines.

This newest proposal is only one of several initiatives by the EU in the context of its Digital Strategy. Over the last few years, the EU has positioned itself as global leader in regulating the digital sector, including through the General Data Protection Regulation (the GDPR), the proposed Data Governance Act and the proposed Digital Services Act. The GDPR has quickly become the global gold standard that other nations look to as blueprint. It is expected that the Draft AI Regulation may play a similar role.

This article provides an overview of the key provisions of the Draft AI Regulation.

What is an AI system?

An AI system is any software that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with, provided that the software was developed using one or more of the following techniques:

- machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; or
- statistical approaches, Bayesian estimation, search and optimization methods.

This definition is purposively broad to be as technology neutral and future-proof as possible.

Scope of application

With regard to its territorial scope of application, the focal point is whether the impact of the AI system occurs within the EU, regardless of the location of the provider or user. This could lead to a very broad extraterritorial application of the Draft AI Regulation, reaching far beyond the borders of the EU. The Draft AI Regulation envisages that it will apply to:

- providers that first supply commercially (whether or not free of charge) or put an AI system into service in the EU (putting into service involves making it available for use by a "user" or for use by the provider itself), regardless of whether the providers are located inside or outside the EU;
- users of AI located in the EU; and
- providers and users located outside the EU, if the output produced by the system is used in the EU.

The provider is defined as the person who has developed the AI system or has had it developed for it. It is, however, important to note that if another person in the distribution chain (importer, distributor, user) (i) puts an AI system on the market under its own name or trademark, (ii) modifies the intended purpose of an existing AI system, or (iii) makes substantial modifications to the AI system, this person takes on the obligations of a "provider" under the Draft AI Regulation. In the case of (ii) or (iii) the original provider is no longer considered a "provider". Branding may therefore have an impact on a party's legal obligations and should be considered carefully.

Note that the term "user" does not have its intuitive meaning of a natural person using an AI system. It refers to an entity or person under whose authority the AI system is operated, except where the AI system is used in the course of a "personal non-professional activity". For example, if company A implements a chatbot on its website developed by Company B, Company A is the user and Company B is the provider. The visitor to the website who chats with the chatbot is not considered a user under the Draft AI Regulation.

The Draft AI Regulation does not apply to AI systems that are exclusively developed or used for military purposes, or to public authorities of third countries or international organizations using AI systems under international agreements for law enforcement/judicial co-operation.

Risk-based Approach

Instead of opting for a blanket regulation covering all AI systems, the European Commission has used a risk-based approach based on three tiers: (i) unacceptable risk, (ii) high risk, (iii) low risk.

The use of unacceptable-risk AI systems is simply banned.

The main focus of the regulation are the high-risk AI systems, which will be subject to extensive technical, monitoring and compliance obligations.

Certain systems in the low-risk category are subject to transparency obligations. The low-risk category is encouraged to self-regulate by implementing codes of conduct for instance by adopting some of the requirements that are imposed on high-risk AI systems.

Unacceptable-risk AI systems

The following AI systems are prohibited by the Draft AI Regulation:

- Distorting human behaviour: AI systems materially distorting a person's behaviour in a manner that causes or is likely to cause physical or psychological harm to that person or another person, by deploying subliminal techniques to distort a person's behaviour or by exploiting vulnerabilities of a group of persons due to their age or physical or mental disability.
- Social scoring by public authorities: AI systems for social scoring by public authorities or on their behalf that leads to the detrimental or unfavourable treatment of certain persons or groups in certain circumstances. Social scoring is the practice of evaluating or classifying the trustworthiness of natural persons over a certain period, based on their social behaviour or characteristics.
- Real-time remote biometric identification: AI systems used for real-time remote biometric identification in publicly accessible spaces, eg facial recognition systems, for the purposes of law enforcement is in principle prohibited. There are however some exceptions to this position relating to law enforcement, such as use in the context of a targeted search for victims of crime, such as missing children.

High-risk AI systems

The Draft AI Regulation qualifies two groups of AI systems as high-risk: (1) the AI is (a part of) a product that is already subject to certain EU safety regulations (as listed in an Annex to the Draft AI Regulation) and (2) AI systems designated by the European Commission as high risk:

1. AI systems that are products or safety components of products that (i) are covered by EU legislation set out in the table below, and (ii) are subject to a third party ex-ante conformity assessment under that legislation.

- **Medical devices**
- **In vitro medical devices**
- **Radio equipment**
- **Lifts**
- **Toys**
- **Personal protective equipment**
- **Machinery**
- **Marine equipment**

- **Appliances burning gaseous fuels**
- **Motor vehicles and trailers**
- **Two- or three-wheel vehicles and quadricycles**
- **Equipment and protective systems for use in potentially explosive atmospheres**
- **Civil aviation security**
- **Pressure equipment**
- **Agricultural and forestry vehicles**
- **Unmanned aircrafts**
- **Cableway installations**
- **Recreational crafts and personal watercrafts**
- **Rail system**

2. AI systems designated by the European Commission as being high-risk. These AI systems are listed in Annex III of the Draft AI Regulation. This list may be updated at any time. The table includes a selection of the AI systems that are most relevant for the private sector:

Key obligations for providers of high-risk AI systems:

- Risk management system: providers must establish and document a continuous risk management system, including the identification and evaluation of risks. The risk management system must ensure that such risks are eliminated or reduced to the extent possible through adequate design and development. Providers are to implement risk mitigation and control measures for risks that cannot be eliminated.
- High quality data sets: the AI systems must be trained, validated and tested by “high-quality” data sets that are relevant, representative, free of errors, and complete. In addition “sensitive personal data” (eg data relating to race/ethnicity/religion/philosophical beliefs/political options/ health) *is* permitted to be used to the extent “strictly necessary” to monitor, detect and correct bias. This provision on data and data governance is given great weight by the Draft AI Regulation as breach of it is subject to the highest level of penalties.
- Technical Documentation: The provider is obliged to create and keep up to date technical documentation that proves the system’s conformity and compliance with the Draft AI Regulation to regulators.
- Information to users: Users must be able to sufficiently understand how a high-risk AI system works to enable them to interpret and use its output, including by being informed on the characteristics, capabilities and limitations of performance of the high-risk AI system.
- Quality management system and logs: the provider must implement a quality management system, which includes technical standards and a regulatory compliance strategy and design automatic logging

capabilities.

- Human oversight: high-risk AI systems must be designed in such a way that they can be effectively overseen by competent natural persons. These persons should fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation. This oversight must include the ability to disregard, override or interrupt the AI system.
- Robustness, accuracy, and cybersecurity: high-risk AI systems must be designed and developed in such a way that they achieve an appropriate level of accuracy and resilience against errors and attempts by unauthorized third parties to alter the system.
- Conformity assessment: the provider must perform a conformity assessment of the high-risk AI system to demonstrate its conformity with the requirements of the Draft AI Regulation before the AI system can be used or put on the EU market. In most cases, this may be done by way of a self-assessment where the provider itself issues a declaration of conformity after internal control. The declaration must be updated whenever modifications are made. AI used for remote biometric identification and public infrastructure networks is subject to a third party conformity assessment every five years or any lesser period identified by the third party. In addition, a CE marking must be visibly affixed.
- Registration: standalone high-risk AI systems must be registered in a publicly accessible EU-wide database established by the European Commission.
- Monitoring: providers must implement proportionate post-marketing monitoring to evaluate continuous compliance of the AI system by collecting and analysing performance data. Providers are also required to inform national authorities about serious incidents or the malfunctioning of the AI system as soon as they become aware thereof, as well as any recalls or withdrawals of the AI system.

Providers that are credit institutions under Directive 2013/36/EU (CRD IV) are entitled to discharge some of these obligations through compliance with requirements that are already imposed on them under other EU regulation.

Key obligations for users of high-risk AI systems: Users must use the AI system in accordance with the instructions indicated by the provider, implement the human oversight measures indicated by the provider, ensure that the input data is relevant for the intended purpose, monitor the operation for incidents or risks (eg as to health and safety or to fundamental rights and freedoms), interrupt the system in the case of incidents or suspend its use if they consider that use *may* result in such a risk and keep the logs generated by the AI system. They are also required to carry out a data protection impact assessment under the GDPR.

Key obligations for importers of high-risk AI systems: Before placing a high-risk AI system on the market, importers must ensure that the conformity assessment has been carried out, that the documentation obligations have been complied with and that the CE conformity marking is applied.

Key obligations for distributors of high-risk AI systems: Distributors must, among other obligations, verify that the high-risk AI system bears the required CE conformity marking and is accompanied by the required documentation and instructions for use. A distributor is also required to verify that a provider and importer has complied with the obligations set out in the Draft AI Regulation.

Low-risk AI systems

For certain low-risk AI systems, the Draft AI Regulation introduces some transparency obligations. These transparency obligations are currently intended only to apply to (i) AI systems that interact with humans, like chatbots, unless it is obvious from the circumstances and the context of use that it is an AI system, (ii) emotion recognition or biometric categorization systems and (iii) so-called deepfakes. There are some limited exceptions to the transparency obligations, for instance, in some cases for law enforcement purposes.

Low risk AI systems that do not fall under the above-mentioned transparency obligations are essentially unregulated.

Regulatory sandboxes

National supervisory authorities may establish AI regulatory sandboxing schemes to provide a controlled environment that facilitates the development, testing and validation of AI under direct supervision and regulatory oversight before the systems are placed on the market or put into service. The objectives of these regulatory sandboxes are to (i) enhance legal certainty for innovators and ensure compliance of the AI system with the Draft AI Regulation, and (ii) increase the national competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI.

Fines

Similar to the GDPR and the proposed Digital Services Act, the Draft AI Regulation provides for substantial fines in the event of non-compliance as well as other remedies, such as requiring the withdrawal of the AI system. A hierarchy of fines applies depending on the severity of the infringement, which are:

- up to the higher of EUR 30 million and 6% of the total worldwide annual turnover for breaching the prohibition on unacceptable-risk AI system or infringing the data governance provisions for high-risk AI systems;
- up to the higher of EUR 20 million and 4% of the total worldwide annual turnover for non-compliance of AI systems with any other requirement under the Draft AI Regulation; and
- up to the higher of EUR 10 million and 2% of the total worldwide annual turnover for supplying incorrect, incomplete, or false information to notified bodies and national authorities.

Supervision and enforcement mechanism

The Draft AI Regulation introduces a dual system where national authorities at the Member State level supervise the application and enforce the Draft AI Regulation and where a cooperation mechanism applies the rules at the EU level to try to ensure the consistent application of the Draft AI Regulation. Each Member State is required to designate a national competent authority. At EU level, the Draft AI Regulation creates a European Artificial Intelligence Board, composed of representatives from the national supervisory authorities and the European Commission, which will be tasked with facilitating cooperation of national supervisory authorities and providing guidance on its various aspects.

This governance model is similar to the GDPR, where there is a large diversity between the enforcement activities of the different national data protection authorities. The European Commission now proposes to chair the European Artificial Intelligence Board, which demonstrates that it wishes to be closely involved in the enforcement of the Draft AI Regulation.

What's next?

The European Commission stresses that it has been careful to adopt a risk based approach to its regulation of AI systems under the Draft AI Regulation. However, the requirements in the Draft AI Regulation for high-risk AI systems are detailed and onerous, backed up heavy penalties. Taking into account the manner in which the more advanced AI systems work, some obligations in the Draft AI Regulation, such as the human oversight obligation, will force providers to fundamentally reconsider how AI is designed and developed. These detailed obligations will, in any case, require significant compliance costs.

The European Commission will need to reach an agreement with the European Parliament and the Council of the European Union before this text is adopted. It could still take several years before the Draft AI Regulation becomes law. While the text may still undergo changes, it is clear that this draft signals the start of a more engaged and high stakes debate over the coming years.

Over the next few weeks, we will share our further thoughts on specific aspects of the Draft AI Regulation. In the meantime, please contact us if you would like to discuss any impact that the Draft AI Regulation might have on your business.