Prevent the AI Act from taking you by surprise: how to limit the risks

By Reinier W.L. Russell, of Russell Advocaten B.V.

Almost all companies now use some form of artificial intelligence (AI). This means they may be subject to the prohibitions and regulations set out in the European AI Act, even if they are not located in the European Union (EU). How can a business ensure that they comply with these rules?

AI is becoming increasingly prevalent in society. The healthcare sector, education, the legal sector, and the business community all use it. The applications of AI within these sectors vary, but they all have in common that they bring both advantages and disadvantages. AI will contribute to innovation and efficiency within various sectors, at the same time, it poses potential risks to the protection of fundamental human rights, as every application of AI raises ethical, privacy, and security issues.

Companies need to be aware of this. For this reason, since February 2, 2025, the EU has required organizations that use AI to ensure sufficient AI literacy. They must provide their staff, and others who manage AI systems on their behalf, with sufficient AI knowledge. This obligation is part of the European AI Act, which was adopted in 2024 and will enter into force on August 2, 2026. Some important parts have already come into force, while other regulations will be enforced at a later date. (Those differences are called out below.)

The AI Act

The European AI Act is the first piece of legislation specifically for artificial intelligence. The regulation aims to safeguard two interests: the protection of human rights and measures to stimulate innovation. The law contains rules on the design, implementation, and use of AI systems within the EU.

The AI Act affects the use of AI within the EU and worldwide. This regulation applies to providers of AI systems and their representatives, importers and distributors, and companies and organizations that use AI (the deployers). Companies that (intend to) place AI systems on the European market, or that have their AI systems process data from EU citizens, will therefore need to take the new AI Act into account. Different rules apply to each of them.

What the regulation entails

Risk categories

The European Commission has opted for a risk-based approach, whereby AI systems are divided according to risk levels. These risk levels determine the requirements that the related AI system must meet. The system distinguishes between four main groups:

1. **Unacceptable risk**
   AI systems that pose an unacceptable risk to safety, fundamental rights, or EU values have been strictly prohibited since February 2, 2025. Examples include social credit scores and behavior manipulation systems. These systems may not be placed on the market. Biometric identification systems also fall under this category in principle. However, the AI Act makes an exception for cases where these are deemed necessary for the functioning of the democratic rule of law. An example of this is their use to identify perpetrators of criminal offences.
2. **High risk**
   AI systems that, due to their intended purpose and context, may pose significant risks to health, safety, or fundamental rights are subject to strict regulation. Examples include systems used in education, for personnel selection, or by

public services. These systems must meet strict requirements in terms of transparency, accountability, and data management. The regulation for this will come into force on August 2, 2027.

3. **Limited risk**
   AI systems that pose limited risks to users and the public are mainly subject to transparency obligations, such as informing the public that they are interacting with AI-generated content. This is mandatory for chatbots and deepfakes, for example.
4. **Minimal risk**
   AI systems that pose minimal or no risk to safety or fundamental rights do not have to comply with specific regulations under the AI Act. These include spam filters.

General Purpose AI (GPAI) models

Depending on the risk assessment, different rules apply, but the AI Act also contains specific regulations for GPAI models. This includes the well-known ChatGPT. Such AI models must provide documentation, comply with copyright laws, and publish summaries of the training data. Models that pose a systemic risk have additional obligations, such as reporting incidents and ensuring cybersecurity. These rules have been in effect since August 2, 2025.

Legal pitfalls

In addition to the specific obligations that apply to each category, the European Commission also recommends general safeguards for the use of AI. To avoid legal and financial risks, companies must be aware of the risk group to which their AI system belongs and the obligations that this entails. The most important considerations are briefly outlined below:

- **Compliance and liability:** Companies must ensure compliance with the European AI Act. This means, among other things, keeping documentation on how their AI works, performing risk analyses, and identifying possible biases.
- **Transparency and control:** The AI Act emphasizes transparency and traceability of AI decisions, especially in high-risk applications. This requires companies to be able to clearly explain how their AI systems function and make decisions.
- **Human intervention:** Article 22 of the GDPR requires human intervention if the use of AI relates to natural persons.
- **AI literacy:** Organizations using AI must provide their staff and others who manage AI systems on their behalf with sufficient AI knowledge.

Penalties for non-compliance with the AI Act

Penalties may be imposed for non-compliance with the European AI Act. The amount of the penalty depends on both the risk category of the AI system and the severity of the violation. AI practices that are explicitly prohibited due to unacceptable risks are subject to a fine of up to 35 million EUR or, for companies, up to 7 percent of global annual turnover. Violations of the rules for the use of high-risk AI systems and those for general-purpose AI models are punishable by a fine of up to 15 million EUR or, for companies, 3 percent of global annual turnover. Providing incorrect or misleading information to the authorities is punishable by a fine of up to 7.5 million EUR or, for companies, 1 perfect of global annual turnover.

Avoiding legal pitfalls

To ensure compliance and avoid penalties, companies must consider the following:

- **Risk management:** Evaluate the risks of AI systems and keep track of which compliance requirements apply.
- **Transparency and accountability:** Maintain detailed documentation on the operation and use of AI systems within the company.
- **Training and awareness:** Train staff in the use of AI applications, particularly with regard to ethics, regulations, and the protection of personal data. This is essential in order to meet the requirement of “AI literacy.”
- **Compliance with the GDPR:** Comply with the requirements set out in the GDPR at all times.

Practical tip

AI is not solely the responsibility of the IT department; clear rules must also be established from an HR perspective. Russell Advocaten drafts AI policies for its clients that can be added to an employee handbook, code of conduct, or other instructional tools.

IT/ICT lawyer

Have questions about the new AI regulations, or would like to avoid legal pitfalls? We are happy to assist with this or other questions about IT/ICT and law. Please contact Reinier W.L. Russell, of Russell Advocaten B.V.