# Fit for the AI Act

On Friday, Feb. 2, 2024, the EU member states unanimously voted to accept the AI Act. The final text is formally published in July 2024, and this means that, by August 2026, everyone operating within the EU will have to comply with all the parts of this regulation.

A great success for Europe! Or is it?

Maybe that answer depends on who you are; what your role is in the research, development, use of 'AI' systems. But maybe not – it may affect us all. Let us remember two facts.

- First, AI systems have a very short time to market. Since they scale so well, it is often possible that systems that are developed in research environment – not intended for market use – can be immediately deployed in real applications, sometimes with some retraining involved.
- Second, research labs are not intended to nor good at delivering certifiable, high-quality end products. Instead, they aim at proof of concepts, to be then taken into the value chain by other departments. So, the wild-west approach to putting AI systems on the market that has been common in recent years leads to problems. Search for 'AI scandal' or some such in your browser, and you'll get an idea. (But beware: some of those scandals may be fake!)

Instead, we need to strive towards 'quality' AI systems. And put safeguards in place, just as they exist for other software and hardware. No electric appliances can be sold in Europe without a CE mark – it prevents you from being electrocuted when plugging it in. That's a good thing, isn't it? Even for the producers and importers, as it saves them from costly litigation, and increases trust. And since all companies are subject to the regulation, the cost is comparable for everyone.

Back to AI. The AI Act gives us a set of rules on how AI systems, in certain applications, need a level of transparency to ensure that (a) we end up with a certain level of quality, and (b) if it still goes wrong, it's easier to repair, and it's easier to determine who needs to repair it.

This law, which will be in force from the second quarter of 2024, requires everyone who is involved in developing AI, deploying AI, providing AI etc. to become active.

Parts of its regulation already activates from 6 months after it becomes in force. Meaning, around January 2025.

What does this mean for you? Which steps will you have to take immediately? What should you not do? This document, while not to be mistaken for legal advice, and not aiming to be complete, tries to point out some things for you to look out for.

## AI Act principles

There are two important principles of the AI Act.

**one** The AI Act uses a 'risk-based approach' which means it looks at how risky an AI application could be and sets rules based on that risk. It assesses the potential harm or that an AI system might pose to individuals or society and categorises their risk as minimal, limited, high, or unacceptable. The more dangerous an AI could be to people or society, the stricter the rules it must follow. For example, AI applications considered a high risk would be subject to stricter compliance requirements, such as transparency, data quality.

**two** The AI Act is 'horizontal' meaning that the regulation applies broadly across various sectors and applications, not just being focussed on one specific type of business or technology. This makes sure that the foundational principles of AI regulation, such as safety, transparency, and accountability, are uniformly applied to all AI systems, no matter where or how the AI is used.

Be aware that the definition of AI in the regulation is so broad that it almost includes any piece of software[1] – but then, of course, only comes into effect when the application of that software falls in the said risk categories.

## Does it affect you?

As a legal entity: Yes. From the above it is clear that any company which uses, makes, or sells software or hardware is potentially affected. It will also affect research institutions, either through the way they interact with their personnel, or how they work with third parties.

As an individual, the AI Act lays a foundation for protecting your rights. Combined with the

[1] The official definition (Title I, Article 3) reads: (1) 'Al 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;

upcoming AI Liability Directive, it provides a strong instrument to defend your rights if you are adversely affected by a machine.

## When and how must you act?

Most of the regulations of the AI Act will 'apply' 24 months after the regulation is 'in force'. I.e., August 2026. Let's look at the two most important categories: prohibited AI, and high-risk AI.

**prohibited AI – your AI inventory**

Not all of the AI act gives you two years of time: the regulation on prohibited AI will apply already after 6 months. These include subliminal techniques, exploiting vulnerabilities of individuals, social scoring, real-time remote biometric identification, and a few others (Title II, Article 5).

Now, hopefully, your company is not involved in any of these applications. The regulation – through the upcoming AI Liability Directive – does not implement a reverse burden of proof, but it *does* presume causality, even without proof. This makes burden of proof easier for potential victims as to how or why an AI system reached a certain harmful output.

Therefore, it is imperative that you can show that you are not involved in any of these prohibited applications of AI, within 6 months of the regulation coming into force; i.e., from early 2025. To be able to do that, you are well advised to have an inventory of your 'AI systems' by that time, to rule out any possible negative effects.

**high-risk AI – your obligations**

For the next category, high-risk AI systems, there are many obligations. If an AI is high-risk AI is determined based on the application areas and the potential impact on fundamental rights and safety. Application areas include critical infrastructure, education and employment, law enforcement, healthcare, and public services. If the systems you put on the market or use can fall in these categories, you have obligations including:

- implementing a *risk management* system to identify and mitigate risks;
- *data governance*: Ensuring high-quality datasets to minimize risks and biases;
- end-to-end *documentation* of the software as well as the data;
- *transparency*: Providing clear information to users about the system's capabilities and limitations;

- implementing measures to ensure the system's *accuracy*, *robustness*, and *cybersecurity*;
- compliance with privacy and data protection regulations of your systems (i.e., not just of the data used);
- *monitoring*;
- *human oversight*: ensuring human intervention and oversight to minimize risks;
- *conformity assessment*: undergoing assessment procedures to verify compliance with the AI Act.

Not all these points are run-of-the-mill: e.g. data documentation is technically challenging; robustness etc. is not always given; it is not completely clear how AI systems may impact data privacy; and monitoring as well as human oversight at a scalable level is hard.

This means that, at this moment, while you should start making your AI governance structure in good order, you cannot yet fill it in and make your systems compliant with the AI Act. Some unclarities remain.

**What if I purchase an 'AI system'?**

The AI Act differentiates between different parties, in particular: providers (that includes those who develop an AI system and put it on the market), deployers (who use it), authorised representatives, importers (of AI systems into the EU), distributors (beyond the previous mentioned, who make the AI system available in the EU), and operators (all of the above). Each have their rules to adhere to:

- Providers (those who develop AI systems): They must conduct thorough risk assessments, ensure data quality, implement robust and accurate record-keeping, and ensure transparency and provision of information to users. They're also required to ensure their AI can be overseen by humans, to prevent or minimise risks.
- Suppliers (those who supply AI components but may not be the original developers): They need to ensure that their components, when integrated into AI systems, do not compromise the overall compliance of the system with the AI Act's requirements.
- Importers (those who bring AI systems into a market area, like the EU): They must check that the AI systems they import comply with the AI Act, including all documentation, safety, and transparency requirements.
- Deployers (organisations or individuals who use AI systems in their operations): They are responsible for using the AI in accordance with the manufacturer's instructions, including any requirements for human oversight, and ensuring the system is used in a

way that continues to comply with the AI Act.

This means that, for instance, if you are just the 'user' of an AI system – a deployer – you can just be as liable as the organisation that designed and programmed it. Remember, the AI Act is all about how AI is *used*.

## What should you *not* do?

Don't run off and get your audit. While you will find many companies offering their AI auditing services, since there are no agreed-upon AI standards[2] yet that cover the AI Act, the audit you can get today may or (more likely) may not cover the AI Act. Be aware that methods to implement the AI Act, and mitigate the impact of AI systems, is still under development. And the same holds for methods for AI-Act aligned auditing and testing, which are core parts of compliance.

## What *should* you do?

Don't panic. And don't ignore. Depending on the size of your organisation, it can certainly pay off to set up a small unit of legal, organisational and technical experts to implement the AI Act. For smaller organisations, setting up such teams may be challenging, and finding one expert who can cover all these areas will be almost impossible.

But either way, your organisation should start today by getting familiar with the requirements of the AI Act, ideally by having one or more dedicated people analysing its contents and evaluating how it affects your business. Your next step of action is to create an inventory of AI-related software that your entity makes, sells, buys, or use. And this is challenging for larger organisations: not all software may be inventoried; and what exactly is 'AI' and who determines 'high-risk' is not set in stone, so cross-department alignment is required.

The next deadline, after 12 months, comes with regulations to general-purpose AI (Chapter V). We won't dive into that here; in short, there are broad transparency requirements for GPAI, such as disclosing information about the training data, the design and development process, and potential risks.

[2]These standards are being developed by CEN/CENELEC. More at https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:2916257&cs=11D701467243B7C63DEF4702C86E0138A

The major challenge is preparing for high-risk AI systems. Applied from August 2026, these have many requirements as mentioned above: risk management, data governance, technical documentation, transparency, human oversight, accuracy, robustness, cybersecurity, and conformity assessment.

There is not yet a clear go-to place for getting outside help. AI Act startups, legal firms, AI suppliers, and consulting firms still need to prove their worth, and it's rare to find those who can consult you with the breadth needed.

So, it is key to start getting informed now. If you can build up a team, do. If not, get in touch with us. Since you are not alone in this challenge. You can team up with your peers in etami, to jointly learn how to improve your AI system processes. Indeed, etami has defined Fields of Action (FoA) that align with challenges in the AI Act. Join those, and you will be able to change a legislative burden into an improved value stream process for AI.

**Caveat: We strive for accuracy but make mistakes. BDVA is not liable for any damages resulting from following our advice. This information should not be considered legal advice. For legal matters, please consult a qualified attorney.**

*Published in 2024 by etami, a task force in BDVA. Visit https://etami.org or https://bdva.eu for more information.*