NADOVO

# EU AI ACT COMPLIANCE FOR SMES

A Practical Guide

**Jochen Stier**

Edition: February 2026

# TABLE OF CONTENTS

# 1. WHY AI COMPLIANCE NOW?

Artificial intelligence is no longer a topic for the future. It is the present: in every company, in every industry, in the tools that employees use every day. At the same time, the European Union has adopted the world's first comprehensive AI regulation with the AI Act. The deadlines are running, the penalties are severe, and most small and mid-sized businesses have not yet started to prepare.

This chapter explains why waiting is the riskiest of all strategies.

## AI Is Already Here, Whether You Want It or Not

In conversations with managing directors of small and mid-sized businesses, the same sentence often comes up: "We don't really use AI." This sentence is almost always wrong.

The reality looks different. Most companies already use AI systems, often without having consciously decided to do so. Microsoft 365 contains Copilot functions that are based on large language models. CRM systems such as Salesforce or HubSpot use AI for lead scoring and forecasting. Accounting software classifies receipts automatically. ERP systems optimise order quantities with the help of machine learning. Even spam detection in your email inbox is an AI system.

On top of that comes a second layer: AI features that are embedded into existing software without much announcement. A software update, and suddenly the system suggests texts, recognises patterns or prioritises tasks. The provider has integrated AI. The company that uses the software becomes the deployer of an AI system, often without knowing it.

So the question is not whether a company uses AI. The question is how much AI is already in use and whether management has an overview of it.

> **In practice:** A simple test creates clarity. Pose this question in a meeting of department heads: "Which of our software systems use AI or machine learning?" Compare the answers with the actual product descriptions of the solutions in use. In most cases, the discrepancy is considerable.

## Shadow AI: The Underestimated Risk

Alongside the "official" use of AI, there is a phenomenon that is significantly more dangerous for companies: shadow AI. This refers to the use of AI tools by employees without the knowledge, approval or control of the company.

The scenarios are as everyday as they are risky. A sales employee has ChatGPT draft a quotation and pastes customer data, pricing terms and contractual conditions into the input field. An HR officer uses an AI translation tool to translate an employment contract into English, including the personal data of the employee. A developer has code fragments analysed by an AI assistant and in doing so transfers proprietary business logic to an external service.

What these situations have in common: personal data or trade secrets leave the company without a legal basis having been examined, without a data processing agreement having been concluded, and without it even being documented that this processing is taking place. This is no minor matter; it is a serious data protection problem under the GDPR. And the EU AI Act adds a further compliance dimension.

Anyone who lived through the shadow IT debate in the 2010s knows the pattern: employees bypass official IT channels because the official solutions are too slow, too cumbersome or simply not available. Shadow AI follows the same logic, with one crucial difference. Shadow IT was usually about productivity tools or cloud storage. Shadow AI is about systems that generate content, prepare decisions and transfer data to external models. The risk potential is significantly higher.

The consequence is clear: without an inventory of the AI systems in use, including the unofficial ones, and without binding usage policies, no company can manage its AI risks. The first step in any AI compliance strategy is therefore transparency about the status quo.

## The Clock Is Ticking: Deadlines and Consequences

The EU AI Act (Regulation (EU) 2024/1689) entered into force on 1 August 2024. Since then, a staggered timetable has been running that activates different obligations at different points in time.

**What already applies:**

Since 2 February 2025, the prohibitions of certain AI practices have been in effect. These include, among other things, social scoring, manipulative techniques that exploit the

vulnerabilities of persons, and certain forms of biometric real-time remote identification. Also since 2 February 2025, the obligation regarding AI literacy (Article 4) has applied: companies must ensure that staff who operate or oversee AI systems possess sufficient knowledge.

> **EU AI Act:** Art. 4: Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf.

**What is still to come:**

Since 2 August 2025, the obligations for providers of general-purpose AI models (GPAI), that is, the providers of large language models, have applied. From **2 August 2026**, the EU AI Act will be applicable in its full breadth. This concerns in particular the comprehensive obligations for high-risk AI systems under Annex III: risk management, data governance, technical documentation, human oversight, transparency and reporting obligations.

**The penalties are severe:**

The EU AI Act provides for a three-tier system of fines. For breaches of the prohibited AI practices, fines of up to €35 million or 7% of worldwide annual turnover, whichever is higher, may be imposed. For other breaches of the regulation, the upper limit is €15 million or 3% of turnover. Even providing incorrect or incomplete information to authorities can be sanctioned with up to €7.5 million or 1% of turnover.

> **EU AI Act:** Art. 99: For SMEs and start-ups, the regulation provides for proportionate upper limits. This does not change the fact that fines can also be a threat to the existence of small and mid-sized businesses.

It is not just about money. Market surveillance authorities can prohibit the use of non-compliant AI systems or order their withdrawal from the market. For a company that depends on a particular AI system in its business operations, such an order can be more severe than a fine.

## Compliance as an Opportunity, Not Just a Duty

So far, this may sound as if AI compliance is primarily a burden. Fines, deadlines, obligations. That is one side. The other side is often overlooked.

**Trust as a competitive advantage.** Customers, business partners and public-sector clients are increasingly asking: how does the company handle AI? Are there policies? Is its use documented? Companies that can answer these questions credibly have an advantage, whether in tenders, supplier audits or customer conversations. Demonstrable AI governance is becoming a quality marker, much like ISO certifications or GDPR compliance already are.

**Better decisions through transparency.** A complete AI inventory and a systematic risk classification provide management with something many companies lack: a clear overview of their own AI landscape. Which systems are in use? For what purpose? With what risk? This knowledge improves not only compliance but also the strategic steering of AI use as a whole.

**Preparation for what is coming.** The EU AI Act is the first comprehensive AI regulation, but it does not stand alone. The originally planned AI Liability Directive was withdrawn in 2025. Liability questions for AI-related damages will instead be addressed through the revised Product Liability Directive, which applies from December 2026 and explicitly includes software and AI systems. Sector-specific requirements will follow. Insurers will price AI risks into their policies. Anyone who builds a solid compliance foundation today will not have to start from scratch tomorrow when the next wave of regulation arrives.

**No rocket science.** AI compliance does not require a multi-million budget or a team of AI specialists, but rather structure, an overview and the willingness to tackle the topic systematically. Most small and mid-sized businesses have proven with the GDPR that they can handle regulatory requirements. AI compliance builds on much of that experience.

> **In practice:** The most important first step costs nothing but time: create an inventory of the AI systems in use. Without this inventory, it is unclear what needs to be regulated. With this inventory, the foundation for everything else is in place. Chapter 8 shows how to implement this in the first week.

The EU AI Act is no surprise. It was negotiated for years, discussed publicly and finally adopted in June 2024. The deadlines are known. The supervisory structures in Germany

are to be established with the planned KI-MIG. What is still missing in many companies is internal preparation.

This guide provides the foundation for that. The following chapters explain what the EU AI Act actually regulates, which role a company plays, how AI systems are to be classified and what obligations arise. At the end stands a concrete roadmap for the first four weeks.

# 2. THE EU AI ACT AT A GLANCE

The EU AI Act is the world's first comprehensive regulation of artificial intelligence. It applies to every company that uses AI systems in the European Union, regardless of where the software provider is based. This chapter gives a compact overview: what the regulation governs, how it is structured, which deadlines apply, what national implementation looks like in Germany, and how the AI Act fits into the existing regulatory landscape.

## What Does the EU AI Act Regulate?

Regulation (EU) 2024/1689 pursues a clear goal: the safe, trustworthy and human-centred use of AI in the European Union. It defines under what conditions AI systems may be developed, made available and used, and it sets out limits that must not be crossed.

**The scope is deliberately broad.** The EU AI Act covers all AI systems that are placed on the market, put into service or used within the EU. This also applies if the provider is based outside the EU, as long as the output of the system is intended for persons in the EU. Many companies will already be familiar with this extraterritorial effect from the GDPR: it is not the location of the provider that is decisive, but the place where the system has effect.

**What does not fall under the AI Act:** purely military AI applications are excluded. Likewise, AI systems used exclusively for personal, non-professional purposes. Research and development also enjoy exemptions under certain conditions, but only as long as the systems are not placed on the market or put into service.

For small and mid-sized businesses in the DACH region, this means: anyone who uses AI software that in some way takes decisions, generates content or affects persons is highly likely to fall within the scope of this regulation.

## Structure of the Regulation

The EU AI Act comprises 13 chapters with 113 articles and 13 annexes. That sounds like a lot, and it is. The good news: not all parts are equally relevant in practice. The following overview shows where the most important content can be found.

| Chapter | Content | Relevance for SMEs |
|---|---|---|
| **Chapter I** (Art. 1-4) | General provisions, definitions, scope, AI literacy | High: this is where the basic terms are defined |
| **Chapter II** (Art. 5) | Prohibited AI practices | High: in force since 2 February 2025 |
| **Chapter III** (Art. 6-49) | High-risk AI systems: classification, requirements, obligations for providers and deployers | Core: decisive for everyone who deploys high-risk systems |
| **Chapter IV** (Art. 50) | Transparency obligations for certain AI systems | Relevant for chatbots, generative AI, emotion recognition |
| **Chapter V** (Art. 51-56) | General-purpose AI models | Primarily for GPAI providers, SMEs as users indirectly affected |
| **Chapter VII** (Art. 64-68) | Governance: AI Office, AI Board, national authorities | Relevant for the supervisory structure |
| **Chapter IX** (Art. 72-94) | Post-market monitoring, market surveillance | Relevant for reporting obligations and post-market monitoring |
| **Chapter X-XII** (Art. 95-101) | Codes of conduct, penalties | Relevant for the framework of fines |

Two annexes deserve particular attention.

**Annex I** lists the harmonised EU product regulations. If a product is already subject to an EU conformity assessment, for example as machinery, a medical device or a toy, and contains an AI component as a safety element, the AI system automatically counts as high-risk.

**Annex III** defines eight areas of application in which AI systems are classified as high-risk: from biometric identification, through HR management, to the administration of justice. This annex is the central test basis for SMEs and is dealt with in detail in Chapter 4.

> **In practice:** It is not necessary to read all 113 articles. The pragmatic way in: Article 5 (prohibitions), Article 6 (high-risk classification), Article 26 (deployer obligations) and Article 50 (transparency obligations). Together with Annex III, these passages cover the bulk of what is operationally relevant for SMEs.

## Timeline: What Applies When?

The EU AI Act does not take effect all at once but in stages. This gives companies time to prepare, but only if they actually use that time.

| Date | What applies? | Status |
|---|---|---|
| **1 August 2024** | Regulation entered into force | Completed |
| **2 February 2025** | Prohibited AI practices (Art. 5); AI literacy obligation (Art. 4) | **Already in force** |
| **2 August 2025** | Obligations for GPAI models (Art. 51-56); governance structures (AI Office, AI Board) | **Already in force** |
| **2 August 2026** | Full application: high-risk AI systems under Annex III, deployer obligations, transparency obligations, penalties | **Approx. 6 months to go** |
| **2 August 2027** | High-risk systems as a safety component in regulated products (Annex I) | Outstanding |

For most SMEs, **2 August 2026** is the decisive cut-off date. From that date, the comprehensive obligations for high-risk systems will apply in full: risk management, documentation, human oversight, reporting obligations and the possibility of regulatory sanctions.

Two obligations, however, already apply now. The prohibitions of certain AI practices have been in force since 2 February 2025. Anyone who carries out social scoring or uses manipulative AI techniques is already acting unlawfully. And the AI literacy obligation under Article 4 already requires that employees who operate or oversee AI systems possess sufficient knowledge.

> **In practice:** The first thing to check is whether the obligations that already apply are being met. Are there AI applications in the company that could fall under the prohibition list? Do employees have sufficient AI literacy? These two points are not future music; they apply now.

## National Implementation: The KI-MIG

As an EU regulation, the EU AI Act applies directly in all member states. Unlike a directive, it does not first need to be transposed into national law. What does need to be regulated nationally, however, is the question of which authorities are responsible for supervision, how fines are enforced and how cooperation between authorities is organised.

In Germany, the **AI Market Surveillance and Innovation Promotion Act (KI-MIG)** is intended to close this gap. The Federal Cabinet adopted the government draft on 11 February 2026. National supervisory structures should actually have been in place by 2 August 2025. The early federal election delayed the process. The draft is currently going through the parliamentary procedure in the Bundestag and Bundesrat.

### Competent authorities: a hybrid approach

Germany is opting for a distributed supervisory structure that respects existing competences.

The **Bundesnetzagentur (BNetzA)** will become the central market surveillance authority for the private sector. It is the main point of contact for companies that are not already subject to sector-specific supervision. For the financial sector, **BaFin** remains responsible, in particular for high-risk AI systems in banks, insurers and financial services. Likewise, the existing **product supervisory authorities** retain their competence. Anyone who has so far worked with the competent authority for medical devices or machine safety keeps that point of contact.

For SMEs, this hybrid approach means: in most cases, the BNetzA is the right address. Only if the company operates in a regulated sector with its own supervisory authority does the existing competence remain in place.

### KoKIVO and BNetzA support services

At the BNetzA, the establishment of the **Coordination and Competence Centre for the AI Regulation (KoKIVO)** is planned. It is intended to bundle AI expertise and make

it available to other authorities. For companies, the BNetzA already offers an **AI Service Desk**, which is specifically aimed at small and medium-sized businesses and start-ups. This is complemented by the **AI Compliance Compass**, an interactive tool for an initial assessment of one's own affectedness.

**AI regulatory sandboxes: testing with regulatory support**

The EU AI Act (Art. 57) requires every member state to establish at least one **AI regulatory sandbox** by 2 August 2026. In Germany, the BNetzA is to take on this task. In these controlled test environments, companies can develop innovative AI applications under regulatory guidance and check them for conformity. The regulatory requirements apply without restriction; the advantage lies in the technical advice and increased legal certainty. SMEs and start-ups based in the EU receive priority and free access (Art. 62).

**No German special path**

One detail of the draft law deserves particular emphasis: **the government draft of the KI-MIG dispenses with additional national requirements beyond the EU AI Act.** The Federal Ministry for Digital and State Modernisation (BMDS) explicitly emphasises an innovation-friendly implementation. Anyone who fulfils the EU regulation should thereby also fulfil German requirements. The draft provides for no national gold-plating and no tightened special rules, even though the EU AI Act allows member states stricter national rules in individual areas such as biometric real-time identification.

This sets the AI field apart from some other regulatory areas in which German implementing laws have erected additional hurdles. For SMEs, this is an important message of relief: the compliance requirements are intended to be limited to what is prescribed at European level.

> **EU AI Act / KI-MIG:** In practice this means: the EU AI Act is the benchmark. Anyone who fulfils its requirements is compliant in Germany. The BNetzA's AI Service Desk is available as a point of contact for questions.

## Distinction from Other Frameworks

The EU AI Act does not stand alone. It is part of a growing regulatory ecosystem in which different sets of rules complement one another.

**EU AI Act and GDPR** are complementary. The GDPR governs the protection of personal data; the EU AI Act regulates the use of AI systems. Both often apply at the same time because most AI systems process personal data. The AI Act expressly clarifies in Article 2

that the rights of data subjects under the GDPR remain unaffected. Chapter 6 deals in detail with how companies can implement both regulations together.

**The EU AI Act and product safety law** overlap where AI systems are deployed as a safety component in regulated products. If a product, such as a machine, a medical device or a lift, falls under an EU harmonisation rule from Annex I, and the conformity assessment requires a notified body, the AI safety component counts as a high-risk AI system (Art. 6(1)). The existing CE marking then also covers the AI Act requirements: a single conformity assessment encompasses both sets of rules (Art. 43(3)).

**The AI Liability Directive** was originally planned as a complement to the AI Act in order to regulate civil liability for AI-related damages. However, the European Commission withdrew the draft in 2025. Liability questions for AI-related damages will instead be addressed through the revised Product Liability Directive, which applies from December 2026 and explicitly includes software and AI systems. The AI Act itself, with its fines and market surveillance powers, follows a public-law approach. The Product Liability Directive complements it with private-law damages.

**International frameworks** such as the OECD AI Principles, the NIST AI Risk Management Framework (AI RMF) and the ISO/IEC 42001 standard for AI management systems provide complementary impulses. They are not legally binding but offer proven methods for risk management and governance that can help with implementing the EU AI Act. Companies operating internationally benefit from aligning their compliance strategy with these recognised frameworks.

> **In practice:** The most important takeaway for practice: the EU AI Act does not replace existing frameworks but complements them. Companies that already have GDPR processes, a data protection management system or a CE conformity assessment are not starting from scratch. These are building blocks on which AI compliance can be built.

# 3. DOES THIS APPLY TO ME?

The EU AI Act does not regulate AI technology as such, but the roles that organisations play in the AI ecosystem. The central question is therefore not: "Do we use AI?" but: "In what role do we use AI?" The answer determines which obligations apply. This chapter explains the three main roles, shows how to determine your own role and makes clear why most SMEs are to be classified as deployers, but not all.

## The Three Roles in the EU AI Act

The EU AI Act distinguishes three central roles, each entailing different obligations. The definitions are found in Article 3 of the regulation.

**Provider** is anyone who develops an AI system or has it developed and places it on the market or puts it into service under their own name or trade mark. The provider role is the most obligation-intensive: providers bear responsibility for conformity assessment, CE marking, technical documentation and the entire risk management of their system. In simple language: whoever builds the system bears the main responsibility.

**Deployer** is anyone who uses an AI system under their own responsibility. The deployer has not developed the system themselves but obtained it from a provider and uses it in their own business operations. The obligations are less extensive than those of the provider, but by no means negligible: human oversight, transparency towards affected persons, monitoring of the system in operation and, for high-risk systems, a fundamental rights impact assessment. In simple language: whoever uses the system bears the responsibility for its proper deployment.

**Distributor** is anyone who makes an AI system of a provider available on the EU market without significantly modifying it. Typical distributors are software resellers or system houses that distribute AI solutions of other manufacturers. The obligations essentially come down to ensuring that the system bears the CE marking and that the required documentation is enclosed. In simple language: whoever resells the system must check that everything is in order.

The EU AI Act also recognises further roles such as the importer (who brings a system from a third country into the EU) and the authorised representative (who represents a non-EU provider in the EU). For most SMEs, these roles are not relevant, since they typically act as deployers.

> **EU AI Act:** Art. 3(3): 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trade mark, whether for payment or free of charge.

| Role | Brief description | Scope of obligations | Typical SME scenario |
|---|---|---|---|
| **Provider** | Develops or has developed; places on the market under own name | High: conformity, CE, documentation, risk management | Rather atypical, but possible with own AI development |
| **Deployer** | Uses an AI system under own responsibility | Medium: oversight, transparency, monitoring | The standard case for SMEs |
| **Distributor** | Makes an AI system available on the EU market | Low: checking conformity and documentation | IT service providers, system houses |

## Decision Tree: Which Role Do I Have?

You can determine your own role with a few questions. The following decision tree leads systematically to the result.

**Question 1: Is an AI system developed in-house by the company or its development commissioned by it, and is it made available under its own name?** If yes: provider. The full provider obligations apply, including conformity assessment and technical documentation.

**Question 2: Is an AI system from an external provider used in your own business operations?** If yes: deployer. The deployer obligations under Article 26 apply, the scope of which depends on the risk class of the system.

**Question 3: Are AI systems of other providers distributed or resold without being significantly modified?** If yes: distributor. The obligations are limited to conformity checks and the correct passing on of documentation.

**Question 4: Do several of these descriptions apply?** Then there are multiple roles. A company can simultaneously be the provider of its own AI system and the deployer of purchased AI solutions. In that case, the obligations of the respective role apply to each system.

An example illustrates the multiple-role situation: a mid-sized IT service provider has developed its own AI-supported ticketing system and sells it to customers. For this system, the company is a provider. At the same time, it uses Microsoft Copilot for internal purposes and AI-based accounting software. For these systems, it is a deployer. Both roles exist side by side, and the respective obligations apply to each system.

> **In practice:** As a first step, it is advisable to draw up a list of all AI systems used in the company and answer the question for each system: did we develop this system ourselves or significantly modify it? In most cases, the answer will be "no". That makes the role clear: deployer.

## The Typical SME Situation: Mostly Deployer

The reality in most small and medium-sized businesses is clear: AI systems are bought and used, not developed in-house. A craft business that uses AI-supported quotation calculation is a deployer. A tax firm that uses AI-based document analysis is a deployer. A logistics company that uses AI-optimised route planning is a deployer. A machine builder that uses AI-based quality control in its production is a deployer.

Being a deployer does not mean that there are no obligations. The deployer obligations under Article 26 are manageable but real. The intensity of the obligations depends crucially on the risk class of the system in use.

**Obligations by risk class: the use case decides**

A central principle of the EU AI Act is often misunderstood in practice: it is not the AI system itself that determines the risk class, but the specific use case. The same system can fall into different risk classes depending on the deployment context. The decisive unit is therefore the AI process, that is, the combination of AI system and area of application.

An example makes this tangible: a company uses an AI-supported text analysis tool. In marketing, it generates product descriptions and social media posts. That is minimal risk; there are no specific obligations beyond AI literacy under Article 4. The same tool is used in the HR department to pre-sort applications and evaluate candidates. This use case falls under Annex III No. 4 (employment and HR management) and is therefore a high-risk AI process. One system, two areas of application, two completely different compliance requirements.

For high-risk AI processes, deployers must, among other things, ensure that the system is used in accordance with the provider's instructions for use, that adequate human oversight is in place, that input data is appropriate to the intended purpose and that relevant incidents are reported. Certain deployers, in particular public authorities, must additionally carry out a fundamental rights impact assessment.

For AI processes with limited risk, transparency obligations apply above all: persons interacting with a chatbot must be informed of this, and AI-generated content must be labelled as such.

For AI processes with minimal risk, no specific obligations under the EU AI Act apply. The AI literacy obligation under Article 4, however, applies to all risk classes.

This process-based view has an immediate practical consequence: a complete AI inventory alone is not enough. Only when each AI system is mapped to its specific areas of application can the risk class be determined and the actual compliance effort identified. The NADOVO Framework captures exactly this step systematically in the DEFINE phase.

> **In practice:** Being a deployer is not a free pass. What is decisive is not the role alone, but the combination of role and risk class. A deployer of a high-risk system has significantly more obligations than a deployer of a system with minimal risk. Risk classification is therefore the next logical step after determining the role and is dealt with in detail in Chapter 4.

## When Does a Deployer Become a Provider?

Article 25 of the EU AI Act contains a provision that deserves particular attention: the role shift. Under certain circumstances, a deployer can become a provider, with all the obligations that go with it.

**Three scenarios trigger the role shift:**

**Scenario 1: Substantial modification of the system.** Anyone who modifies an AI system to such an extent that it no longer corresponds to the original system of the provider becomes a provider themselves. An example: a company buys a pre-trained language model and continues to train it with its own industry data (fine-tuning) in order to use it for specific tasks such as automated creditworthiness checks. The fine-tuning substantially changes the behaviour of the model. The company becomes the provider of this modified system.

**Scenario 2: Making available under your own name.** Anyone who takes an AI system from another provider and places it on the market under their own name or brand becomes a provider, even without technical modification. The classic white-label model: the technology comes from a third party, but to the outside world, the company appears as the provider.

**Scenario 3: Change of intended purpose.** Anyone who uses an AI system for a purpose other than that intended by the original provider becomes a provider. This is particularly the case if the change of purpose results in a different risk class. An example: an AI system that was developed for customer analysis in marketing (minimal risk) is instead used for the assessment of credit applications (high risk). The change of purpose makes the company the provider of the system in this new context of use.

**The consequences are considerable.** Anyone who becomes a provider takes on the full provider obligations: conformity assessment, technical documentation, CE marking, risk management, post-market monitoring. These are obligations that require considerable resources and expertise.

> **EU AI Act:** Art. 25(1): Any natural or legal person shall be considered to be a provider of a high-risk AI system and shall be subject to the obligations of the provider if they substantially modify a high-risk AI system that has already been placed on the market or put into service.

The good news: normal configuration and parameterisation within the settings provided by the provider does not trigger a role shift. Anyone who uses a CRM system with integrated AI features and adjusts the standard settings remains a deployer. The threshold for "substantial modification" is set deliberately high.

> **In practice:** A simple safeguard helps to avoid an unintended role shift: before any adaptation of an AI solution that goes beyond the standard configuration, check whether the threshold of substantial modification is being crossed. Particular caution is required with fine-tuning, in-house training with company data or use for purposes that were not envisaged. In case of doubt, it is worth consulting the provider of the system, who should have documented which adjustments lie within the intended framework.

# 4. RISK CLASSIFICATION

The EU AI Act follows a risk-based approach. That means: not every AI system is treated the same way. The intensity of regulation is geared to the risk that an AI system poses to the health, safety and fundamental rights of persons. This chapter explains the four risk levels, shows how the use case determines the risk class, and provides a practical method for classifying your own AI systems.

## The Four Risk Levels

The EU AI Act divides AI systems into four risk levels. The higher the risk, the stricter the requirements.

**Unacceptable risk: prohibited.** Certain AI applications are completely banned. Article 5 defines the prohibited practices, which have applied since 2 February 2025. They include, among others:

- Social scoring by public authorities: the evaluation of persons on the basis of their social behaviour with adverse consequences.
- Manipulation through subliminal techniques: AI systems that influence the behaviour of persons in a way they cannot recognise and that causes them harm.
- Exploitation of vulnerabilities: AI systems that specifically exploit weaknesses of certain groups, for example on the basis of age, disability or social situation.
- Biometric real-time remote identification in public spaces: with narrowly defined exceptions for law enforcement.
- Emotion recognition in the workplace and in educational institutions: with exceptions for medical or safety-relevant purposes.

For SMEs, the prohibition list is a clear red line. Most companies will not deploy any of these systems. Nevertheless, it is worth checking, because some prohibitions are broader than they appear at first sight. An AI system that analyses the emotions of employees working from home in order to measure their productivity, for example, falls under the prohibition of emotion recognition in the workplace.

**High risk: strict regulation.** High-risk AI systems are subject to the most comprehensive requirements of the EU AI Act. There are two routes by which an AI system is classified as high-risk.

The first route runs via **Annex I**: if a product is already subject to an EU conformity assessment (for example as machinery, a medical device or a lift) and contains an AI component as a safety element, the AI system automatically counts as high-risk. The obligations from the AI Act then complement the existing product safety requirements.

The second route runs via **Annex III**: this defines eight areas of application in which AI systems count as high-risk. It is the more relevant test for most SMEs and is dealt with in detail in the section "Annex I and Annex III".

The obligations for high-risk systems include, among other things, risk management, data governance, technical documentation, transparency, human oversight and post-market monitoring. For providers, conformity assessment and CE marking apply additionally. Chapter 5 deals with the obligations in detail.

**Limited risk: transparency obligations.** AI systems with limited risk are subject to specific transparency obligations under Article 50. Three categories fall under this:

- AI systems that interact directly with persons (for example chatbots): the affected persons must be informed that they are communicating with an AI system.
- AI systems that generate synthetic content (text, image, audio, video): the providers of these systems must mark the outputs in a machine-readable way as AI-generated (Art. 50(2)).
- Emotion recognition and biometric categorisation systems (insofar as not prohibited): the affected persons must be informed about the deployment.

The transparency obligations under Art. 50 are more nuanced than is often presented. The labelling obligation under Art. 50(2) applies to the providers of the AI systems, not to the companies that use these systems as a tool. What is relevant for companies is above all Art. 50(4): anyone who publishes AI-generated texts on matters of public interest must disclose the AI involvement. However, a practically relevant exception applies: if the content has been subject to human review with editorial responsibility, this obligation does not apply. A company that uses AI to produce a technical report, reviews its content and publishes it under its own name is therefore not subject to the labelling obligation under Art. 50(4).

Deepfakes and synthetic media (image, audio, video) that depict real persons or events, by contrast, must always be labelled as AI-generated (Art. 50(4)).

> **In practice:** Independent of the legal obligation, voluntary transparency about the use of AI tools can be a sign of responsible practice, especially for companies that position themselves in the field of AI compliance.

**Minimal risk: no specific obligations.** The vast majority of AI systems fall into this category. Spam filters, spell checkers, simple recommendation systems or AI-supported search functions are not subject to any specific obligations under the EU AI Act. The legislator does recommend voluntary codes of conduct, but does not prescribe anything.

Two qualifications nevertheless apply. First: the AI literacy obligation under Article 4 applies to all AI systems, regardless of the risk class. Second: the GDPR and other existing rules continue to apply independently of the AI Act.

## The Core Principle: The Use Case Determines the Risk Class

This is the most important insight of the entire guide: it is not the technology that determines the risk class, but the use case. The same AI model can fall into different risk classes depending on the purpose of use. The decisive unit is the **AI process**: the combination of AI system (asset) and specific area of application.

A large language model (LLM) illustrates the principle. If it is used to create marketing texts, it is a system with minimal risk. If the same model is used for the automated preselection of job applications, it falls under Annex III No. 4 (employment and HR management) and becomes a high-risk system. If it is configured in such a way that it manipulates the behaviour of persons in a subliminal manner, its use is prohibited.

A further example: image recognition. The same technology used to classify product photos in e-commerce is minimal risk. The same technology used for the biometric identification of persons is high risk or, depending on the context, even prohibited.

And another example from everyday SME life: an AI chatbot. Used in customer service, it is subject to transparency obligations (limited risk). If the same chatbot is used for initial medical advice in a doctor's practice, it may be classified as a high-risk system.

> **In practice:** Blanket classifications such as "our AI system is not high-risk" fall short. Every individual use case must be assessed separately. A company that uses the same AI tool in three different departments for three different purposes may have to take three different risk classes into account.

## Annex I and Annex III: What Is in Them?

**Annex I** lists the harmonised EU product regulations that require third-party conformity assessment. The logic is simple: if a product is already regulated (as machinery, a lift, a medical device, a toy, recreational craft, cableway and others) and contains an AI component as a safety element, then the AI component automatically counts as high-risk. For SMEs that manufacture regulated products with AI components, Annex I is the relevant test point. Full application of the obligations for Annex I systems begins on 2 August 2027.

**Annex III** is the central test basis for most SMEs. It defines eight areas of application in which AI systems are classified as high-risk. The following overview shows the areas with typical application examples.

| No. | Area | Typical applications | SME relevance |
|---|---|---|---|
| 1 | Biometric identification and categorisation | Facial recognition, biometric access controls | Medium: relevant for biometric time-recording systems |
| 2 | Critical infrastructure | AI control of electricity, gas and water networks, traffic management systems | Low for most SMEs |
| 3 | Education and vocational training | Automated exam assessment, decisions on access to educational institutions | Low to medium: relevant for education providers |
| 4 | Employment and HR management | AI-supported applicant screening, automated performance evaluation, dismissal decisions | **High**: affects many SMEs |
| 5 | Access to essential services | AI-based creditworthiness checks, insurance assessments, prioritisation of emergency services | High: relevant for financial services and insurers |
| 6 | Law enforcement | Risk assessment, lie detectors, predictive policing | Low for private-sector SMEs |
| 7 | Migration, asylum and border control | Risk assessment, document checks | Low for most SMEs |
| 8 | Administration of justice and democratic processes | AI-supported legal research with decision suggestions, electoral influence | Low to medium |

For most SMEs in the DACH region, areas 4 (employment) and 5 (essential services) are particularly relevant. Anyone who uses AI systems in HR or in lending should check carefully whether the specific use case falls under Annex III.

**Art. 6(3): The exception from the high-risk classification**

An AI system that falls within an Annex III area is not classified as high-risk if it does not pose a significant risk to health, safety or fundamental rights, in particular by not materially influencing the outcome of decision-making. The condition is that at least one of the following four conditions is fulfilled:

(a) The AI system is intended to perform a narrow procedural task.

(b) The AI system is intended to improve the result of a previously completed human activity.

(c) The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns without replacing or materially influencing the human assessment.

(d) The AI system is intended to perform a preparatory task for an assessment that is relevant for the purposes of the use cases listed in Annex III.

An example: an AI-supported tool that pre-sorts incoming applications in the HR department according to formal criteria (complete documents, minimum qualification), without carrying out a substantive evaluation or ranking of candidates, could be classified as a preparatory task under condition (d) and thus excluded from the high-risk classification.

The exception, however, has a clear limit: if an AI system carries out profiling of natural persons, it always counts as high-risk, regardless of whether one of the four conditions is fulfilled. As soon as a system systematically evaluates personality traits, behavioural patterns or personal preferences, the exception does not apply.

Important for providers: anyone who relies on the exception must document the assessment before the system is placed on the market or put into service (Art. 6(4)). On request by the competent authority, this documentation must be presented.

## Practical Check: Classifying Your Own Applications

Classifying your own AI systems into the risk levels is not rocket science, but it does require a systematic approach. The following step-by-step method leads to the result.

**Step 1: Describe the use case.** What does the AI actually do? For which persons does the result have consequences? What kind of decisions are prepared or taken? A precise description of the use case is the foundation for everything that follows.

**Step 2: Test against the prohibition list.** Does the use case fall under one of the prohibited practices in Article 5? If yes: stop immediately. The prohibitions have applied since 2 February 2025.

**Step 3: Test against Annex III.** Does the use case fall into one of the eight high-risk areas? If yes: does the exception under Article 6(3) possibly apply? If no exception applies, this is a high-risk system.

**Step 4: Test against Annex I.** Is the AI system a safety component in a regulated product? If yes: high risk.

**Step 5: Check transparency obligations.** Does the system interact directly with persons? Does it generate synthetic content? If yes: the transparency obligations under Article 50 apply (limited risk).

**Step 6: If no hit.** If the use case falls into none of the categories mentioned, it is a system with minimal risk. No specific obligations under the AI Act apply, but the general AI literacy obligation under Article 4 does.

The following table shows the classification of typical SME use cases.

| Use case | Risk class | Reasoning |
|---|---|---|
| AI-supported accounting software (receipt classification) | Minimal | No Annex III category, no direct effect on persons |
| Chatbot in customer service | Limited | Transparency obligation: customers must know that they are interacting with AI |
| AI-based applicant screening | **High** | Annex III No. 4: employment and HR management |
| AI-supported creditworthiness check | **High** | Annex III No. 5: access to essential services |
| AI-optimised route planning (logistics) | Minimal | No Annex III category, no safety-critical function |
| Generative AI for marketing texts | Limited | Transparency obligation: AI-generated content must be capable of being labelled |
| AI quality control as a safety element in machinery | **High** | Annex I: AI as a safety component in a regulated product |

> **In practice:** The NADOVO core formula sums up the principle: **Asset + use case = AI process, from which the risk class follows.** First identify the AI system (asset), then describe the specific area of application, derive the AI process from it and finally determine the risk class. Chapter 7 shows how the DISCOVER phase of the NADOVO Framework supports this systematic inventory and classification. Chapter 8 provides the concrete roadmap for the first four weeks.

# 5. OBLIGATIONS BY ROLE AND RISK CLASS

Chapter 3 clarified the roles, Chapter 4 the risk classes. Now the two come together: what specific obligations result from the combination of role and risk class? The focus is on deployer obligations, since most SMEs operate in this role. The provider obligations are dealt with in overview, because deployers should also know what they can and must expect from their AI suppliers.

## Provider Obligations at a Glance

Providers bear the main weight of regulation. They are responsible for ensuring that a high-risk AI system meets the requirements of the EU AI Act from development through market launch to ongoing surveillance.

The most important provider obligations for high-risk systems at a glance:

**Risk management (Art. 9):** the provider must establish a risk management system that covers the entire life cycle of the AI system. Risks must be identified, assessed and mitigated through suitable measures.

**Data governance (Art. 10):** training data must be of high quality, representative and checked for systematic bias. The data quality requirements also apply to test and validation data.

**Technical documentation (Art. 11):** comprehensive technical documentation must be drawn up and kept up to date. This documentation is the basis for the conformity assessment and must be accessible to the authorities on request.

**Automatic logging (Art. 12):** the AI system must be designed in such a way that relevant events are automatically recorded (logging). The logs make it possible to trace decisions and to detect risks in operation.

**Transparency and instructions for use (Art. 13):** the provider must make available clear, comprehensible information about the system, in particular instructions for use for the deployer. These must describe, among other things, the intended purpose, performance limits and the requirements for human oversight.

**Human oversight (Art. 14):** the system must be designed in such a way that effective human oversight is possible. The provider defines which oversight measures are req-

uired and ensures that the technical conditions for them are in place.

**Accuracy, robustness and cybersecurity (Art. 15):** the system must achieve an appropriate level of accuracy, robustness and cybersecurity and maintain these throughout its entire life cycle.

**Conformity assessment and CE marking (Art. 43):** before placing on the market, the provider must carry out a conformity assessment. Depending on the system, this may require an internal check or an assessment by a notified body. With a positive result, the CE marking is applied.

**Post-market monitoring (Art. 72):** after market launch, the provider must systematically monitor the system, collect performance data and take corrective measures where necessary.

> **In practice:** Even though SMEs are usually not providers themselves, it is worth knowing these obligations. They form the benchmark for supplier selection. When procuring AI systems, in particular high-risk systems, the following questions should be put to the provider: is a conformity assessment available? Is there technical documentation? Are instructions for use for deployer operation available? What does the provider state regarding data quality and bias testing? A provider who cannot answer these questions should not be the first choice.

## Deployer Obligations: What SMEs Really Have to Do

The obligations for deployers are less extensive than those of providers, but they are binding and require organisational preparation. The scope depends crucially on the risk class of the system in use.

**For high-risk systems (Art. 26):**

The deployer obligations for high-risk AI systems can be grouped into seven core areas.

**1. Use as intended.** The AI system must be used in accordance with the provider's instructions for use. That sounds self-evident, but it has regulatory significance: anyone who uses a system outside the intended purpose risks not only malfunctions but also a role shift to provider (as described in Chapter 3).

**2. Human oversight.** The deployer must ensure that competent personnel oversee the functioning of the AI system. The persons concerned must be able to understand the outputs of the system, to recognise signs of anomalies and to stop or override the syst-

em if necessary. This presupposes that employees are trained accordingly, which in turn is connected with the AI literacy obligation under Article 4.

**3. Input data.** Insofar as the deployer has control over the input data, they must ensure that it is appropriate to the intended purpose of the system and sufficiently representative.

**4. Monitoring and reporting.** The deployer must monitor the functioning of the system in ongoing operation. In the event of malfunctions, risks or serious incidents, there is a reporting obligation towards the provider and the competent market surveillance authorities.

**5. Retention of logs.** The logs automatically generated by the system must be retained for at least six months, unless other rules apply.

**6. Data protection impact assessment.** If the deployment of the high-risk system requires a data protection impact assessment (DPIA) under the GDPR, the deployer must carry it out. The EU AI Act expressly refers to this obligation in Article 26(9). Chapter 6 deals with the interplay between the AI Act and the GDPR in detail.

**7. Fundamental rights impact assessment.** The FRIA obligation under Article 27 has a narrowly defined addressee group: bodies governed by public law, private bodies that provide public services, and all deployers of AI systems for creditworthiness checks (Annex III No. 5(b)) and for risk assessment in life and health insurance (Annex III No. 5(c)). For most private SMEs, this obligation does not apply. The FRIA assesses the impact of the AI deployment on the fundamental rights of the persons affected.

> **EU AI Act:** Art. 26(1): Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure that they use such systems in accordance with the instructions for use accompanying the systems.

**For AI systems with limited risk:**

The obligations are limited to transparency. Persons interacting with an AI system (for example a chatbot) must be informed that they are communicating with an AI. AI-generated or manipulated content such as synthetic images, videos or texts must be capable of being labelled as such and must also be labelled when published.

**For AI systems with minimal risk:**

There are no specific obligations under the EU AI Act. Nevertheless, it is advisable also to keep these systems in the AI inventory and to set up internal usage policies. This

tes transparency and makes it easier to adapt if regulation evolves further or a system is to be used for a new use case with a higher risk class.

> **In practice:** The deployer obligations for high-risk systems are demanding, but they require above all organisation, not technology. The backbone consists of three elements: trained staff (AI literacy), documented processes (who oversees what, how are incidents reported) and a working line of communication with the provider of the system. Anyone who builds up these three elements has laid the essential foundations.

## Overview Table: Role × Risk Class

The following matrix sums up the most important obligations by role and risk class. It serves as a central reference for your own need for action.

| Risk class | Provider | Deployer | Distributor |
|---|---|---|---|
| **Unacceptable** | Prohibited | Prohibited | Prohibited |
| **High** | Risk management, data governance, technical documentation, logging, transparency, human oversight, accuracy/robustness/cybersecurity, conformity assessment, CE marking, post-market monitoring | Use as intended, human oversight, quality of input data, monitoring and reporting obligation, retention of logs, DPIA (where required by GDPR), FRIA where applicable | Check CE marking and documentation, ensure conformity in the supply chain |
| **Limited** | Ensure transparency, enable labelling of AI-generated content | Inform users of AI interaction, label AI-generated content | Pass on labelling obligations through the supply chain |
| **Minimal** | No specific obligations (voluntary codes of conduct recommended) | No specific obligations (voluntary codes of conduct recommended) | No specific obligations |

**For all risk classes:** the AI literacy obligation under Article 4 applies to anyone who operates or oversees AI systems, regardless of role or risk class.

## GPAI Models: What SMEs as Users Need to Know

Alongside the obligations for AI systems, the EU AI Act in Articles 51 to 56 also regulates the obligations for providers of general-purpose AI models (GPAI). What is meant are models that can competently perform a wide range of different tasks, often referred to in practice as foundation models: GPT, Claude, Gemini, Llama or Mistral.

**The four core obligations for all GPAI providers (Art. 53)**

Providers of GPAI models must, since 2 August 2025, fulfil the following obligations:

(a) Draw up and keep up to date the technical documentation of the model (Annex XI).

(b) Make information and documentation available to downstream providers that integrate the model into their AI systems (Annex XII).

(c) Implement a strategy for compliance with EU copyright law, in particular for observing reservations of rights under the Copyright Directive (EU) 2019/790.

(d) Draw up and publish a summary of the content used for training, following a template provided by the AI Office.

Open-source exception: models that are made available under a free and open-source licence and whose weights, architecture and information on use are publicly accessible are exempt from obligations (a) and (b). The copyright strategy (c) and the training data summary (d) also apply to open-source models. Where there is systemic risk, this exception does not apply.

**Additional obligations in the case of systemic risk (Art. 55)**

GPAI models with systemic risk, that is, models with particularly high capability or reach (Art. 51), are subject to tightened requirements: model evaluation and adversarial testing for the identification of systemic risks, observation and reporting of serious incidents to the AI Office, and ensuring an adequate level of cybersecurity.

**What does this mean for SMEs?**

The compliance burden for GPAI models lies with their providers, not with the companies that use AI systems built on top of them. The GPAI-specific obligations under Articles 53 to 55 apply to companies such as OpenAI (as the provider of the GPAI model GPT), not to the using company.

A distinction of roles is important here: OpenAI is the GPAI model provider. Microsoft integrates GPT into its own product (Copilot) and is thereby the provider of an AI system with its own obligations under Art. 16 et seq., but not the provider of the underlying GPAI model.

For companies, the question arises whether by deploying such AI systems they become a deployer within the meaning of the EU AI Act. Art. 3(4) defines a deployer as someone who uses an AI system "under their own authority". A company that licenses Microsoft Copilot and integrates it into its business processes is a deployer and is subject to the obligations under Art. 26. Occasional use of ChatGPT via the browser by individual employees, by contrast, does not without more establish a deployer role. What is decisive is whether the company organisationally takes responsibility for the deployment of the AI system.

Codes of practice as compliance evidence: until harmonised standards are published, GPAI providers can demonstrate compliance with their obligations by adhering to the codes of practice under Art. 56. The AI Office of the European Commission published the final Code of Practice on 10 July 2025; the Commission and the AI Board confirmed it on 2 August 2025 as an adequate compliance instrument. Adherence is voluntary, but it establishes a presumption of conformity. Active enforcement by the AI Office (requests for information, model access) starts from 2 August 2026.

For breaches of the GPAI obligations, fines of up to €15 million or 3% of worldwide annual turnover apply (Art. 101(1)).

> **In practice:** The thread remains unchanged: the use case determines the risk class. This applies in particular to GPAI-based systems. The GPAI model providers bear their own obligations; downstream AI system providers such as Microsoft bear theirs. But which obligations apply to the deploying company depends on what the system is actually used for and whether the company acts as a deployer.

# 6. INTERPLAY WITH THE GDPR

The EU AI Act does not stand alone. It enters a regulatory environment that has been shaped since 2018 by the General Data Protection Regulation (GDPR). Since most AI systems process personal data, both regulations often apply at the same time. The good news: existing GDPR processes form a solid basis for AI compliance. This chapter shows where the two frameworks overlap, where they complement each other and how SMEs can leverage synergies without building parallel structures.

## What Does the GDPR Regulate, What Does the EU AI Act?

The two regulations have different subject matters, but a broad common scope of application.

**The GDPR** governs the protection of personal data. It defines under what conditions personal data may be collected, processed and stored, what rights data subjects have, and what organisational and technical measures are required for data protection. The GDPR has been in force since May 2018, and most companies have by now established processes: records of processing activities, data protection impact assessments, data processing agreements, data protection officers.

**The EU AI Act** regulates the deployment of AI systems. It defines under what conditions AI systems may be developed, made available and operated, what risk levels exist and what obligations follow. The focus is not on the data alone but on the system and its use case: how does the AI take decisions? What risks arise from this for affected persons? Is human oversight ensured?

**Both regulations apply in parallel.** The EU AI Act expressly clarifies in Article 2(7) that the rights of data subjects under the GDPR remain unaffected. GDPR compliance does not replace AI Act compliance and vice versa. Anyone who uses an AI system that processes personal data must fulfil both regulations.

An example illustrates the interplay: AI-supported applicant screening processes CVs containing personal data (name, professional experience, qualifications). The GDPR requires a legal basis for the processing, transparency towards applicants and the right not to be subject to decisions based solely on automated processing. The EU AI Act classifies the system as high-risk (Annex III No. 4) and additionally requires human oversight, risk management, documentation and monitoring. Both sets of requirements must be fulfilled.

## Overlaps and Synergies

The GDPR and the EU AI Act pursue related goals: protecting natural persons from risks arising from automated processing and decision-making. At several points, the requirements overlap.

**Transparency.** The GDPR requires transparency in the processing of personal data (Articles 13 and 14 GDPR): data subjects must know what data is processed for what purpose. The EU AI Act requires transparency in the deployment of AI systems: persons must know that they are interacting with an AI (Article 50), and deployers of high-risk systems must inform affected persons about the AI deployment (Article 26(11)).

**Automated decisions.** Article 22 GDPR gives data subjects the right not to be subject to a decision based solely on automated processing that produces legal effects concerning them. Article 14 of the EU AI Act requires human oversight for high-risk AI systems. Both rules point in the same direction: people should not be entirely at the mercy of fully automated decisions.

**Accountability.** Both regulations require documentation and demonstrability. The GDPR calls it accountability (Article 5(2) GDPR): the controller must be able to demonstrate that the data protection principles are being complied with. The EU AI Act requires technical documentation, logging and the ability to demonstrate compliance to the authorities.

**Data quality.** The GDPR principle of accuracy (Article 5(1)(d)) requires that personal data be factually correct and up to date. The EU AI Act sets out in Article 10 requirements for the quality and representativeness of training, validation and test data. Both requirements can be addressed in a common data-quality process.

The following table shows the most important parallels.

| GDPR principle | Parallel in the EU AI Act | Synergy potential |
|---|---|---|
| Transparency (Art. 13/14) | Transparency obligations (Art. 50), information obligations (Art. 26) | Common information processes for data subjects |
| Automated decisions (Art. 22) | Human oversight (Art. 14) | Integrated concept for human oversight |
| Data accuracy (Art. 5(1)(d)) | Data governance (Art. 10) | Common data-quality management |
| Accountability (Art. 5(2)) | Documentation, logging, conformity | Extended compliance documentation |
| Data protection impact assessment (Art. 35) | Fundamental rights impact assessment (Art. 27), risk management (Art. 9) | Integrated assessment procedure |
| Processing on behalf (Art. 28) | Supplier due diligence, provider obligations | Extended vendor review |

> **In practice:** Companies that have set up their GDPR processes cleanly are not starting from scratch. The existing infrastructure of a data protection management system, records of processing, DPIA methodology and vendor management forms a foundation on which AI compliance can be built.

## DPIA and AI Risk Assessment: Leveraging Synergies

One of the largest synergies lies in the area of risk assessment. The GDPR knows the data protection impact assessment (DPIA), the EU AI Act knows the fundamental rights impact assessment (FRIA) and the risk management system under Article 9. The methodology of all three instruments is related: identify risks, assess them, define measures and document them.

**The DPIA (Article 35 GDPR)** is mandatory where data processing is likely to result in a high risk to the rights and freedoms of natural persons. With AI systems that process personal data, this is regularly the case.

**The fundamental rights impact assessment (FRIA) under Article 27 of the EU AI Act** has a narrowly defined addressee group. Bodies governed by public law and private bodies providing public services are obliged when they deploy Annex III high-risk AI

systems. In addition, the obligation applies to all deployers, that is, also purely private companies, of AI systems for the creditworthiness check of natural persons (Annex III No. 5(b)) and for the risk assessment in life and health insurance (Annex III No. 5(c)).

For most private SMEs, this means: the FRIA is not an immediate obligation, provided they do not provide public services and are not active in the areas of credit assessment or insurance. The FRIA assesses the impact of AI deployment on fundamental rights and thus goes beyond pure data protection: non-discrimination, equal treatment, access to essential services and human oversight are part of the scope of assessment.

**The risk management system (Article 9 of the EU AI Act)** is primarily a provider obligation. It must cover the entire life cycle of the AI system and systematically identify, assess and mitigate risks.

The differences lie in the focus: the DPIA looks at data protection risks, the FRIA at fundamental rights in a wider sense, the risk management system at systemic AI risks. But the methodology overlaps considerably.

The pragmatic recommendation is: build an integrated assessment procedure that covers all relevant perspectives in a modular process. Instead of producing three separate documents, the DPIA can serve as a starting point and be extended with AI-specific questions: which fundamental rights are affected? How is human oversight organised? What AI-specific risks exist, for example systematic bias, faulty outputs (hallucinations) or creeping changes in performance (drift)?

Such an integrated approach saves resources and at the same time delivers better results, because interactions between data protection and AI risks are not considered in isolation but in context.

The EU AI Act expressly supports this integrated approach: Art. 27(4) provides that the FRIA complements rather than replaces a DPIA already carried out under Art. 35 GDPR. Likewise, Art. 26(9) explicitly refers deployers of high-risk AI systems to the DPIA obligation. Linking the two instruments is therefore not only pragmatically sensible but also envisaged by the legislator.

## Practical Recommendations for SMEs

Five concrete steps help SMEs to leverage the synergies between the GDPR and the EU AI Act.

**1. Records of processing activities as a starting point for the AI inventory.** The records of processing activities under Article 30 GDPR already document which

l data is processed in the company and with which systems. This record can be used as a starting point for the AI inventory: which of the documented processing activities use AI components? Which additional AI systems are in use that have so far not been recorded in the records of processing activities because they do not process personal data?

**2. Involve the data protection officer.** The data protection officer (DPO) knows the GDPR processes, has experience with risk assessments and is networked with the relevant departments. It makes sense to locate AI compliance topics with the DPO or at least to coordinate closely with them, instead of building a parallel compliance structure.

**3. Extend existing processes, do not replace them.** Extend the data protection management system (DPMS) by AI-specific aspects, instead of creating a separate AI compliance system. This applies in particular to the risk-assessment methodology, vendor review and documentation.

**4. Check processing on behalf in the case of AI-as-a-service.** Many SMEs use AI as a cloud service (AI-as-a-service). In these cases, personal data is regularly transferred to the AI provider. This requires a data processing agreement under Article 28 GDPR. At the same time, the EU AI Act requires a check of whether the provider fulfils its obligations (CE marking, technical documentation, instructions for use). Both checks can be combined in an integrated vendor assessment.

**5. Clarify legal bases for AI-related data processing.** If company data is used for AI training or fine-tuning, the GDPR legal bases must be examined. This applies in particular where personal data is concerned. The usual legal bases (consent, legitimate interest, performance of a contract) also apply here, but require a specific check in the AI context.

> **In practice:** The additional effort for AI compliance is manageable for companies with established GDPR processes. The pattern is the same: inventory, risk assessment, documentation, ongoing monitoring. Anyone who has mastered the introduction of the GDPR has the organisational maturity to also implement the EU AI Act. The decisive step is to deliberately use the existing infrastructure as a springboard, instead of starting from scratch in parallel.

# 7. NADOVO FRAMEWORK: GETTING STARTED

The previous chapters have shown what the EU AI Act regulates, which roles and risk classes exist, what obligations follow, and how the interplay with the GDPR works. The decisive question now is: where to begin? This chapter introduces the NADOVO AI Compliance Framework as a structured approach that makes the complexity manageable.

## The Problem: Where to Begin?

113 articles, 13 annexes, multiple roles, four risk classes, staggered deadlines and a growing ecosystem of complementary frameworks. The wealth of information on the EU AI Act is considerable, and the sense of being overwhelmed that arises from it is understandable. In practice, four typical reaction patterns appear, all of which lead into a dead end.

**"We will wait and see what happens."** Waiting sounds like a low-risk strategy, but it is the opposite. The prohibitions and the AI literacy obligation have applied since 2 February 2025. The comprehensive high-risk obligations apply from 2 August 2026. Anyone who only starts then has no time left for careful implementation.

**"We will do everything at once."** Trying to handle the entire AI compliance in a single major project regularly leads to overload. The project becomes too complex, those involved lose the overview, and in the end, it fizzles out.

**"The data protection officer will do that on the side."** AI compliance does touch data protection (as Chapter 6 has shown), but it goes considerably beyond it. Risk management, technical assessment, supplier review and organisational measures require their own approach, even if the DPO is an important partner.

**"We will buy a tool."** Compliance software can support processes, but it does not replace an understanding of your own AI landscape. Anyone who does not know which AI systems are in use and what for cannot build sensible compliance even with the best tool.

What is missing is a structured, step-by-step approach that breaks the complexity down into manageable sections and defines a clear starting point.

## NADOVO as a Compliance Lifecycle

The NADOVO AI Compliance Framework is a practice-oriented lifecycle approach that delivers exactly this structure.

The basic idea: AI compliance is not a one-off project with a defined end point. It is a continuous cycle that adapts to change. New AI systems are added, existing ones are modified, regulatory requirements continue to evolve. A static compliance state does not exist.

The framework consists of five phases organised as a cycle. Four core phases form the operational cycle: DISCOVER, DEFINE, ASSESS and IMPLEMENT. They represent the two sides of compliance work: understanding (DISCOVER and DEFINE) and implementing (ASSESS and IMPLEMENT). The fifth phase, MONITOR, frames the entire cycle as continuous oversight and ensures that compliance remains current.

The lifecycle ensures that nothing is forgotten, that each phase builds on the previous one and that the results are regularly reviewed and updated.


The NADOVO Continuous Compliance Cycle

## The Five Phases at a Glance

### Phase 1: DISCOVER (Asset Management)

**What is done:** inventory of all AI systems in the company, including embedded AI features in existing software and unauthorised shadow AI.

**Core question:** which AI systems are in use, including those that nobody knew about so far?

**Result:** a complete AI register (AI inventory) that records all AI assets with their basic properties: name, provider, area of deployment, type of AI function, data affected.

The DISCOVER phase is the starting point of every AI compliance initiative. Without a complete inventory, the foundation for everything else is missing. Experience shows: in most companies, considerably more AI systems are in use than initially assumed. This is due to embedded AI features in standard software and to the uncontrolled use of external AI services by individual employees.

> **In practice:** Start with the top 10, not with the demand for completeness. Capture the most important and most obvious AI systems first, then expand systematically. An inventory that covers 80% is infinitely more valuable than an aspiration to perfection that is never put into practice.

### Phase 2: DEFINE (Process Management)

**What is done:** for each AI asset captured, define the specific use case, assign the role within the meaning of the EU AI Act (provider, deployer, distributor) and describe the related business process.

**Core question:** what is each system used for, and who is responsible?

**Result:** documented use cases with clear role assignment. Each AI asset is mapped to one or more business processes, and for each process the role of the company is documented.

The DEFINE phase applies the NADOVO core formula: **Asset + use case = AI process.** The AI system alone says nothing about the risk class. Only the specific use case, that is, the "what for", makes the classification possible. That is why every use case must be defined and documented individually.

### Phase 3: ASSESS (Risk Management)

**What is done:** assign each defined process to a risk class, evaluate the risks and prioritise the need for action.

**Core question:** which risk class follows from the use case?

**Result:** a complete risk classification of all AI processes and a prioritised action list. Systems with unacceptable risk must be stopped immediately. High-risk systems require comprehensive measures. Systems with limited risk need transparency measures. Systems with minimal risk need no specific measures.

The ASSESS phase uses the method described in Chapter 4: testing against the prohibition list (Article 5), against Annex III (high-risk areas), against Annex I (regulated products) and against the transparency obligations (Article 50).

### Phase 4: IMPLEMENT (Compliance Execution)

**What is done:** put in place the required measures, graded by risk class and role.

**Core question:** what specifically must be done to be compliant?

**Result:** implemented compliance measures. Depending on need, this comprises: documentation, human oversight, training, supplier contracts, process adjustments, transparency measures and reporting processes.

The IMPLEMENT phase translates the findings of the first three phases into concrete measures. The scope varies considerably: for a high-risk system as a deployer, considerably more measures are required than for a system with minimal risk. Chapter 5 has described the obligations by role and risk class in detail. The IMPLEMENT phase turns them into work packages.

> **In practice:** For high-risk systems, begin with the most important: organise human oversight and set up the documentation. These two measures are the most effective both regulatorily and operationally.

### Phase 5: MONITOR (Continuous Compliance)

**What is done:** ongoing monitoring of the implemented measures, updating of the AI inventory in the event of changes and regular review of compliance.

**Core question:** are the measures still working? Are there new AI systems, changed use cases or regulatory developments?

**Result:** a living compliance system that adapts to change instead of becoming outdated.

MONITOR is not a one-off phase but a permanent process. It ensures that the AI inventory remains current, that new AI systems run through the lifecycle before they are put into service, and that existing assessments are updated when changes occur.

> **In practice:** Schedule quarterly reviews. Run through the cycle anew with every material software change, every new AI tool and every changed use case. The AI inventory should be a living document, not a report drawn up once and then forgotten.

## The Core Formula

The NADOVO core formula condenses the basic principle of the EU AI Act into an operational instruction for action:

**Asset + use case = AI process, from which the risk class follows.**

A consistent example shows the formula in application.

**The asset:** Microsoft Azure OpenAI Service (GPT-4), used in a mid-sized service company.

**Use case 1:** the model is used for internal FAQ answering. Employees ask questions about internal processes; the system delivers answers based on company documentation. The process: knowledge management. The risk class: minimal. No personal decisions are concerned, no Annex III category applies.

**Use case 2:** the same model is used in the HR department for the automated pre-selection of applications. It analyses CVs and produces a ranking of candidates. The process: recruiting screening. The risk class: high. Annex III No. 4 (employment and HR management) applies. The full deployer obligations for high-risk systems take effect.

The same asset, different risk classes. The technology is identical. What changes is the use case. And the use case determines the risk class. This insight is the operational heart of NADOVO and at the same time the basic principle of the EU AI Act.

## Going Further

NADOVO is deliberately conceived as a framework, not as a rigid set of rules. It can be adapted to different company sizes and degrees of maturity. A start-up with three AI tools runs through the cycle faster than a mid-sized company with 50 AI applications, but the methodology remains the same.

This guide gives an overview of the five phases and their interconnections. For deeper implementation, the NADOVO Framework offers detailed templates, checklists and methodologies that operationalise the lifecycle step by step.

NADOVO sees itself as a pragmatic approach, not the only one. The framework is compatible with established standards such as ISO/IEC 42001 (AI management systems), the NIST AI Risk Management Framework and the OECD AI Principles. Companies that already work with one of these frameworks can use NADOVO as a complement that delivers the EU-AI-Act-specific compliance focus.

> **In practice:** Each company decides on the depth of implementation itself, depending on its risk situation and ambition. Some companies need a comprehensive AI governance system. Others get by with a clean inventory and documented risk classifications. NADOVO sets the direction. The next chapter delivers the concrete roadmap for the first four weeks.

# 8. FIRST STEPS: GET GOING RIGHT AWAY

Theory matters. But theory without implementation is worthless. This chapter delivers a concrete 4-week plan with which any SME can start immediately. The plan follows the first three phases of the NADOVO Framework (DISCOVER, DEFINE, ASSESS) in a condensed form that is sufficient for getting started.

## The First Four Weeks: The Roadmap

First, a realistic management of expectations: in four weeks, no company will be fully AI Act-compliant. That is not the goal either. The goal is a solid basis: an overview of your own AI landscape, clarity about roles and risk classes, a prioritised action list. That is more than most companies have today.

The plan does not require a full-time effort. Per week, four to eight hours of work are realistic, distributed across the responsible person and short consultations with departments. The resources are manageable. What is needed is the decision to begin.

## Week 1: Start the AI Inventory (DISCOVER)

**Goal:** identify and document the five to ten most important AI systems in the company.

**Approach:**

**1. Walk through the IT landscape.** Which software is in use in the company? Which of these systems has AI functions? Many standard applications now contain AI components: Microsoft 365 with Copilot, CRM systems with AI-supported lead scoring, accounting software with automated receipt classification, ERP systems with AI-based order optimisation.

**2. Survey the departments.** A targeted question for the heads of department: which AI tools or AI features are used in the department? This often reveals the shadow AI described in Chapter 1: employees independently using ChatGPT, Midjourney, DeepL or other AI services without the IT department knowing.

**3. Check cloud services.** Which SaaS solutions are in use, and which of them use AI in the background? A glance at the current product descriptions of the cloud services in

use often reveals AI features that did not yet exist at the time of the original procurement.

**4. Document the result.** A simple table is enough to start with:

| System name | Provider | Type (cloud/on-premise/internal) | Area of deployment | User group | Personal data? |
|---|---|---|---|---|---|
| Microsoft 365 Copilot | Microsoft | Cloud | Company-wide | All employees | Yes |
| HubSpot (AI scoring) | HubSpot | Cloud | Sales | Sales team | Yes |
| ChatGPT (Team) | OpenAI | Cloud | Various | Individual employees | Potentially |
| DATEV (AI receipt capture) | DATEV | Cloud | Accounting | Financial accounting | Yes |
| ... | ... | ... | ... | ... | ... |

> **In practice:** Perfection is not necessary. Start with what is known and add to it gradually. An inventory that captures 80% of AI systems is the basis for everything else. Without this inventory, AI compliance remains an abstract endeavour.

## Week 2: Determine Roles (DEFINE, Part 1)

**Goal:** for each identified AI system, clarify your own role within the meaning of the EU AI Act.

**Approach:**

For each system in the inventory, ask two questions:

**Question 1: was the system developed in-house or substantially modified by the company?** If no (which will be the case for most SMEs): the role is deployer.

**Question 2: is the system made available under your own name or trade mark?** If yes: the role is potentially provider, and the considerably more extensive provider obligations must be examined.

In practice, around 90% of SMEs will be classified as deployers for all their AI systems. That is a relieving finding, because the deployer obligations are more manageable than the provider obligations (as Chapter 5 has shown).

The inventory is extended by one column:

| System name | ... | Role |
|---|---|---|
| Microsoft 365 Copilot | ... | Deployer |
| HubSpot (AI scoring) | ... | Deployer |
| ChatGPT (Team) | ... | Deployer |
| In-house ticketing system with AI | ... | Provider |

Particular attention should be paid to cases in which AI systems are retrained, adjusted by fine-tuning or used for a purpose other than that envisaged by the provider. Here, the role shift described in Chapter 3 may apply.

## Week 3: Define and Classify Use Cases (DEFINE/ASSESS)

**Goal:** for each AI system, document the specific use case and determine the risk class.

**Approach:**

**Step 1: Describe the use case.** What does the AI do in the company? What decisions are taken or prepared? Which persons are affected?

**Step 2: Test against Article 5 (prohibitions).** Does the use case fall under a prohibited practice? If yes: stop immediately.

**Step 3: Test against Annex III (high risk).** Does the use case fall into one of the eight high-risk areas? Areas 4 (employment) and 5 (essential services) in particular are relevant for SMEs. If yes, additionally check whether the exception under Article 6(3) applies (see Chapter 4).

**Step 4: Check transparency obligations (Article 50).** Does the system interact directly with persons? Is synthetic content generated?

**Step 5: Assign the risk class.** Unacceptable, high, limited or minimal.

The NADOVO core formula comes into play here: **Asset + use case = AI process, from which the risk class follows.**

The inventory is extended again:

| System name | Role | Use case | Risk class |
|---|---|---|---|
| Microsoft 365 Copilot | Deployer | Text support, email summaries | Minimal |
| HubSpot (AI scoring) | Deployer | Lead prioritisation in sales | Minimal |
| ChatGPT (Team) | Deployer | Internal research, text creation | Limited (transparency) |
| AI applicant screening | Deployer | Pre-selection of applications | **High** (Annex III No. 4) |

> **In practice:** After Week 3, a clear picture is in place: which AI systems are in use, in which role the company acts and which risk class applies in each case. That is the basis for all further decisions.

## Week 4: Document Results and Plan Next Steps

**Goal:** consolidate the results so far, prioritise the need for action and plan further steps.

**Approach:**

**1. Finalise the inventory document.** Summarise the results of weeks 1 to 3 in a clean document and align it with management. This document is the company's AI register and the basis of all further compliance measures.

**2. Prioritise high-risk systems.** Are there AI systems that have been classified as high-risk? These require the most extensive measures and should be tackled first. Draw up an initial list of measures for each high-risk system: human oversight, documentation, reporting processes, supplier review.

**3. Implement quick wins.** Some measures can be put in place immediately: add a chatbot notice that draws customers' attention to the fact that they are interacting with an AI. Draw up an internal AI usage policy for employees that regulates which AI tools may be used and what data must not be entered into external AI systems.

**4. Clarify responsibilities.** Who in the company is responsible for AI compliance? Ideally, a person who coordinates the topics and acts as a central point of contact. This can be the data protection officer (with an extended mandate), an IT manager or a specifically appointed person.

**5. Draw up a timeline up to 2 August 2026.** Which measures must be in place by the cut-off date? What resources are required for them? A realistic milestone plan helps to keep the overview.

## How Things Continue

After four weeks, the basis is in place. The next steps lead into the IMPLEMENT and MONITOR phases of the NADOVO Framework.

**High-risk systems:** for each identified high-risk system, implement the detailed deployer obligations from Chapter 5. Organise human oversight, build up documentation, define reporting processes, review supplier contracts.

**Set up monitoring:** establish a process that ensures the AI inventory is updated with every material change. Schedule quarterly reviews.

**AI policy for employees:** develop a binding policy that regulates the use of AI tools in the company. This addresses both the shadow AI issue and the AI literacy obligation under Article 4.

**Supplier management:** define compliance requirements for AI providers. When procuring new AI systems, ask the questions from Chapter 5 (conformity assessment, technical documentation, instructions for use) as a matter of standard practice.

The NADOVO AI Compliance Framework offers detailed templates, checklists and methodologies for each of these tasks. The Bundesnetzagentur's AI Service Desk is available as a point of contact for specific questions.

> **In practice:** AI compliance is not a sprint but a continuous process. But the most important step has been taken: the overview is in place, the risk classes are known, and the need for action is prioritised. That is the foundation on which everything else builds. The deadlines are running, but anyone who starts now has sufficient time for careful implementation.

### Note on the creation of this guide

This guide was produced with the use of AI-supported writing tools. The technical conception, content structuring, quality assurance and editorial responsibility lie entirely with the author. All content has been reviewed and reflects the state of regulation at the time of publication.

This labelling is provided voluntarily in the spirit of the transparency obligations of the EU AI Act (Art. 50) and reflects the conviction that the responsible use of AI begins with openness.

## About this guide

This guide was prepared with the support of AI-assisted writing tools. The subject-matter design, structuring of content, quality assurance and editorial responsibility lie entirely with the author. All content has been reviewed and reflects the state of the regulation at the time of publication.

This disclosure is made voluntarily in the spirit of the transparency obligations of the EU AI Act (Art. 50) and reflects the conviction that responsible use of AI begins with openness.

## Legal notice

This guide is provided for general information only and does not constitute legal advice. Despite careful preparation, no warranty can be given as to completeness, accuracy or timeliness. For the implementation of regulatory requirements, qualified professional advice is recommended.

## Imprint and Copyright



**Contact**

CONTORO SOLUTIONS OÜ
E-Mail: info@contoro.solutions
Web: www.contoro.solutions
Web: www.nadovo.ai

**Edition:** February 2026