EU AI Act Jargon Buster

Every Term You Need to Know, in Plain English

A free guide from AI Act Advisors

The EU AI Act can feel overwhelming. This guide breaks down the jargon into plain English so SME business owners can understand their obligations. Whether you're using AI in hiring, customer service, or financial decisions – this reference document covers the key terms you need to know.

Colour coding:
■ Red = Prohibited AI (banned)
■ Orange = High-risk AI (strict compliance)
■ Blue = Limited risk (transparency required)
■ Green = Minimal risk (lightest obligations)

Last updated: February 18, 2026

A

AI System

What the Act considers "AI"

A software system that uses machine learning or logic-based approaches to generate predictions or decisions. In plain terms: tools that "learn" from data or follow rules to make decisions.

AI literacy

The Article 4 obligation to train staff

Article 4 requires businesses using high-risk AI systems to ensure their staff understand how the system works and its limitations. It's about keeping your team informed, not turning them into AI experts.

Annex III

The list of high-risk AI categories

This annex to the AI Act lists the specific uses that qualify as "high-risk" – including hiring systems, critical infrastructure, and law enforcement tools. It determines which systems need the most compliance work.

Article 14

Human oversight obligation

Requires humans to stay meaningfully involved in high-risk AI decisions. Not a token button-press – humans must have real ability to understand and override the system.

Article 26

Deployer obligations

Sets out what businesses using high-risk AI must do: monitor performance, keep records, report incidents, ensure human oversight. The main compliance checklist for SME users.

Article 27

Fundamental rights impact assessment

A deployer requirement to assess how high-risk AI might affect people's rights. Document potential harms and your mitigation measures.

Article 4

AI literacy obligation

Requires deployers of high-risk AI to ensure staff are trained on how the system works. SMEs must document this training and keep records.

Article 49

EU database for high-risk systems

A public register where high-risk AI systems are listed. Improves transparency and helps customers know what systems are being used.

Article 5

Prohibited practices

The complete ban on certain AI uses deemed "unacceptable risk" – real-time facial recognition, emotion recognition for policing, and manipulation tactics. No exceptions, no compliance path.

Article 50

Transparency obligations (limited risk)

For lower-risk systems: you must tell people when they're interacting with AI and disclose how it works. Basic honesty requirements.

Article 6

High-risk classification rules

Defines which systems are high-risk based on the intended use and impact on people's rights. Critical for SMEs to understand what category their AI falls into.

Article 99

Penalties

Sets the maximum fines under the AI Act – up to 6% of global turnover for serious breaches. Understanding compliance avoids these costs.

B

Biometric categorisation

Classifying people by physical traits

AI that automatically assigns people to categories (age, gender, ethnicity) based on biometric data. Often banned or heavily restricted due to discrimination risks.

C

CE marking

The compliance label for high-risk AI

A mark you place on high-risk AI systems to show they meet AI Act requirements. Similar to CE marks on other EU products – signals conformity to the regulator.

Codes of practice

Voluntary compliance frameworks

Optional industry standards that help you demonstrate good compliance practices. Useful for SMEs wanting to show extra diligence beyond minimum requirements.

Conformity assessment

The formal compliance check for high-risk systems

An independent review (typically by a notified body) that verifies your high-risk system meets all legal requirements. Mandatory for high-risk AI before placing on market.

D

Deep fake

AI-generated synthetic media

Video, audio, or images created or altered by AI to manipulate people. The Act requires labelling of synthetic media to prevent deception.

Deployer

Business that uses AI (most SMEs are this)

The organisation that actually uses an AI system in their operations. If you're using ChatGPT, predictive analytics, or recommendation engines for your business – you're a deployer.

E

EU database

The public register for high-risk systems

A transparency tool where providers register high-risk AI systems they've placed on the market. Lets customers verify what they're using.

Emotion recognition system

Detecting feelings via AI

AI that claims to identify emotions from facial expressions or voice. Often inaccurate and risky; heavily restricted or banned in many contexts.

F

Fundamental rights impact assessment

Article 27, for deployers of high-risk systems

A documented review of how your high-risk AI might violate people's rights (discrimination, privacy, autonomy). Identify and mitigate harms before deployment.

G

GDPR

Data protection (overlaps with AI Act)

The EU's general data protection regulation. Governs how you handle personal data – overlaps significantly with AI Act requirements since AI systems often process personal data.

General-Purpose AI (GPAI)

Models like ChatGPT, Claude

Large language models or other AI trained on broad data that can be adapted for many different uses. The Act has specific rules for GPAI providers about transparency and safety testing.

H

High-risk AI system

Annex III listed systems

AI systems that could significantly impact fundamental rights or critical functions – hiring tools, credit scoring, biometric ID. These trigger the most compliance obligations (conformity assessment, CE marking, human oversight).

Human oversight

Article 14, keeping humans in the loop

The requirement that humans remain meaningfully involved in decisions made by high-risk AI. Means they understand the system, monitor it, and can override or stop it if needed.

L

Limited risk

Transparency obligations (Article 50)

AI systems with some risk but not high-risk. You must disclose that AI is being used and explain how it works. Lighter compliance burden than high-risk systems.

M

MDR

Medical Device Regulation (healthcare AI)

EU rules for medical devices. Overlaps with AI Act for healthcare AI – you may need to comply with both. Healthcare AI is often high-risk.

Market surveillance authority

The national enforcement body

Your national regulator responsible for checking AI Act compliance and taking enforcement action. Each EU member state has one – contact them with concerns or for guidance.

Minimal risk

Most business AI, lightest obligations

AI systems that don't significantly impact rights or safety – recommendation engines, chatbots for customer service. Minimal compliance requirements, but you still can't use banned practices.

N

Notified body

Independent assessor for conformity assessments

A third-party organisation (government-accredited) that conducts conformity assessments for high-risk AI. You hire them to verify your system meets AI Act requirements.

O

Operator

Umbrella term for both providers and deployers

Any organisation involved in the AI value chain – either building it (provider) or using it (deployer). The Act imposes different obligations on each.

P

Placing on the market

Making AI available in the EU

When a provider first makes an AI system available for distribution or use – either selling it or offering it as a service. This triggers compliance obligations.

Post-market monitoring

Ongoing compliance after deployment

After you deploy high-risk AI, you must continuously monitor its performance, gather user feedback, and check for problems. Catch issues before they harm people.

Prohibited AI

The banned uses (Article 5)

AI systems deemed to pose "unacceptable risk" and are completely banned in the EU. Includes real-time facial recognition in public spaces, emotion recognition for law enforcement, and manipulation tactics.

Provider

Company that builds/develops the AI

The organisation that creates or develops an AI system. If you're building your own AI or customising an off-the-shelf model – you have provider obligations.

Putting into service

First use of AI for its intended purpose

When an AI system is first actually used to perform its job in the real world. Differs from "placing on market" – you might place on market, but the deployer puts it into service.

R

Real-time remote biometric identification

The banned facial recognition

Real-time facial recognition systems that identify people in public spaces. Banned in most EU contexts due to fundamental rights risks. The Act allows very narrow exceptions for law enforcement only.

Regulatory sandbox

Free testing environment for SMEs

A safe space where SMEs can test innovative AI with lighter regulatory requirements. Great for startups and smaller businesses developing AI – ask your national authority about local schemes.

Risk management system

Article 9, systematic risk identification

Your documented process for identifying, assessing, and reducing AI-related risks. Required for high-risk systems – shows you've thought through what could go wrong.

S

Significant modification

When a deployer becomes a provider

When you make substantial changes to how you use or modify an AI system, you may shift from deployer to provider. This triggers new obligations – important for SMEs customising AI.

T

Technical documentation

What providers must maintain

Detailed records of how your AI was built, trained, and tested. Includes data used, algorithms, testing results, and performance metrics. Needed to prove compliance.

Transparency obligation

Article 50, telling people about AI

For limited-risk AI systems: you must disclose that AI is involved and explain how it works. Builds trust and meets legal requirements for honesty.

U

Unacceptable risk

Synonym for prohibited

AI uses the Act classifies as too dangerous for any compliance pathway – they're simply banned. Includes certain surveillance, manipulation, and discrimination tactics.