

SME READINESS GUIDE | 2026

The EU AI Act

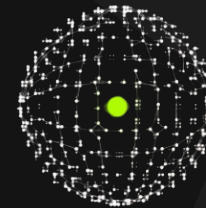
What your business needs to know

A practical guide for business owners to the EU's landmark AI regulation — focused on commercial impact, risk reduction and the actions to take now.

● AI literacy now live

● Fines up to EUR 35 million / 7%

● High-risk rules from 2026



AGS

AUTOMATED GOVERNANCE SYSTEMS

THE COMMERCIAL REALITY

The AI Act is now a board-level business issue

The EU Artificial Intelligence Act is the world's first comprehensive legal framework for AI. Its provisions have applied in phases since 1 August 2024 and can affect organisations outside the EU when AI outputs are used in the EU.

Global

reach

If an AI system's output is used in the EU, the Act can apply regardless of where your business is headquartered.

All

sectors

Finance, HR, healthcare, education, infrastructure and general operations can all be in scope.

Now

phased duties

Prohibited practices and AI literacy requirements are already live, with further deadlines approaching.

EUR 35 million

Non-compliance with prohibited practices can lead to a fine of EUR 35 million or 7% of global annual turnover.

SME owner question:

Do you know which AI tools your people use, what risk category they fall into, and what evidence you would show a regulator?

AT A GLANCE

What is live now, and what comes next

Different parts of the Act apply at different times. Build in lead time for classification, documentation, staff training and supplier assurance.



Important: Systems already on the market have specific transition rules. Significant design changes or changes of intended purpose can trigger earlier compliance obligations.

DEFINITION AND BOUNDARIES

Broad enough to capture modern AI — not simple automation

tion.

An AI system must infer

It generates outputs that can influence physical or virtual environments — rather than merely executing predefined rules.

Operate on machines

It is a machine-based system that works with data, models or logic to produce predictions, content, recommendations or decisions.

Have some autonomy

It functions with a degree of independence from direct human involvement.

General-purpose AI models

GPAI models such as large language models display significant generality and can perform a wide variety of tasks across domains. They have a dedicated framework under the Act.

Out of scope

AI used exclusively for military or national security purposes, or solely for scientific research and development, falls outside the Act's reach.

ROLES DETERMINE DUTIES

You may hold more than one role at the same time

The most stringent obligations apply to providers, but deployers, importers, distributors and upstream suppliers also need clear accountability.

Providers

Develop or place AI systems on the market. They face the most stringent duties, including risk management, data governance, documentation, conformity assessments and registration.

Deployers

Use AI systems in operations. They must follow instructions, ensure human oversight, monitor systems and inform affected individuals where required.

Importers & distributors

Must ensure the AI systems they handle comply before placing them on the market or making them available.

Upstream suppliers

Providers of tools, services or components integrated into high-risk AI systems can also face requirements.

Watch out

Deployers, distributors and importers can be reclassified as providers if they rebrand, substantially modify or change the intended purpose of an AI system to make it high-risk.

BANNED OUTRIGHT

Practices enforceable since 2 February 2025

These are the Act's red lines, where risks to fundamental rights are deemed unacceptable.

Social scoring

Scoring individuals based on social behaviour or personal characteristics.

Emotion inference

Inferring emotions in workplace or educational settings.

Facial recognition scraping

Building databases by untargeted scraping of internet or CCTV images.

Predictive criminal profiling

Assessing criminal risk based solely on profiling or personality traits.

Biometric categorisation

Inferring sensitive traits such as race, political opinions, religion or sexuality.

Subliminal manipulation

Exploiting subconscious vulnerabilities to influence behaviour.

Exploitation of vulnerabilities

Targeting people based on age, disability or socioeconomic disadvantage.

Real-time public biometrics

Remote biometric identification for law enforcement in public spaces, with narrow exceptions.

ARE YOUR SYSTEMS IN SCOPE?

High-risk AI systems face the most demanding requirements

There are two broad categories and a filter system that may allow some standalone systems to avoid high-risk classification.

Category 1: product-embedded AI

AI systems that are products or safety components of products subject to EU sectoral legislation requiring third-party conformity assessment. Examples include cars, aircraft, medical devices, machinery, toys, lifts, radio equipment and in vitro diagnostic devices.

The filter system

A standalone high-risk AI system may avoid classification if it poses no significant risk of harm, based on documented self-assessment and prior registration in the EU database. Profiling in a high-risk use case is automatically high-risk.

Category 2: standalone high-risk AI (Annex III)

HR & employment

Recruitment screening, performance monitoring

Finance

Credit scoring and creditworthiness assessment

Insurance

Life and health insurance risk pricing

Education

Admissions and learning outcome evaluation

Infrastructure

Critical digital infrastructure safety components

Biometrics

Remote identification and emotion recognition

WHAT HIGH-RISK AI COMPLIANCE LOOKS LIKE

Provider and deployer duties in practice

If your AI system is classified as high-risk, you need repeatable controls, documentation and oversight across the system lifecycle.

For providers

- Risk and quality management throughout the AI system lifecycle, including regular review and testing.
- Data governance for relevant, representative and error-controlled training, validation and testing datasets.
- Human oversight, including effective supervision and the ability to halt operations where needed.
- Technical documentation, logs, EU database registration and conformity assessments before market placement.

Follow instructions

Use the system as instructed; ensure input data quality and maintain qualified human oversight.

Monitor & report

Monitor operation, report incidents to relevant authorities and suspend use where necessary.

Inform individuals

Notify affected individuals that they are subject to an AI system, including workers in HR contexts, before deployment.

SME takeaway: create evidence as you go. Policies, logs, training records and supplier due diligence are easier to build before a deadline than after a regulatory request.

A REQUIREMENT, NOT A NICE-TO-HAVE

AI literacy applies to all providers and deployers

From 2 February 2025, organisations must take measures to ensure sufficient AI literacy for staff and others involved in the operation and use of AI systems on their behalf.

What it means

Appropriate skills, knowledge and understanding of AI, including opportunities, risks and potential harms.

Who it covers

Not just technical teams. Governance, legal, HR and operational staff who interact with AI systems are in scope.

In practice

Awareness campaigns, structured training and ongoing upskilling are the primary tools for compliance.

Uncertainty remains

Precise scope is still being clarified, but the obligation to act is clear.

AGS can help design and deliver AI literacy programmes tailored to your organisation's AI footprint, roles and risk profile.

GPAI MODELS HAVE THEIR OWN FRAMEWORK

Large language models and generative AI need specific attention

All GPAI model providers have obligations, with additional requirements for models deemed to carry systemic risk.

All GPAI providers must

- 01 Maintain technical documentation**
Share information with downstream AI system providers.
- 02 Implement copyright compliance**
Respect EU text and data mining rules.
- 03 Publish training data summary**
Disclose a summary of training data content.
- 04 Cooperate with the AI Office**
Engage with the European Commission's dedicated enforcement body for GPAI.

Systemic risk

A model is presumed to have systemic risk if training computation exceeds 10^{26} floating point operations, a threshold covering the most powerful frontier models.

Additional duties

Adversarial testing, systemic risk assessment and mitigation, incident reporting and robust cybersecurity measures. The European Commission has exclusive enforcement powers over GPAI models.

TRANSPARENCY REQUIREMENTS

People need to know when AI is involved

Specific obligations apply to AI systems that interact with people or generate synthetic content, covering providers and deployers.

Chatbots & AI interactions

Users must be informed they are interacting with an AI system, not a human.

Synthetic content

Providers generating synthetic audio, image, video or text must mark outputs in machine-readable format as artificially generated.

AI-generated public information

Deployers publishing AI-generated text on matters of public interest must disclose its artificial origin.

Emotion recognition & biometric categorisation

Deployers must ensure individuals are aware when these systems are operating on them.

Exceptions exist for law enforcement contexts and for artistic or satirical works in the case of deepfakes, but they are narrow and should be carefully assessed.

PENALTIES ARE DESIGNED TO BE A REAL DETERRENT

Fines are calculated against global annual turnover

Group-level turnover may be the reference point, with penalties determined according to the severity of the infringement.

Prohibited AI practices

EUR 35 million or 7% of global annual turnover

High-risk AI & transparency violations

EUR 15 million or 3% of global annual turnover

GPAI model violations

EUR 15 million or 3% of global annual turnover

Incorrect or misleading information

EUR 7.5 million or 1% of global annual turnover

SME provision

For SMEs and start-ups, fines are capped at the lower of the relevant percentage or fixed amount.

Enforcement split

Member States enforce most provisions; the Commission, via the AI Office, enforces GPAI models.

Clock is ticking

Penalty provisions for most requirements have applied since August 2025.

YOUR THREE IMMEDIATE PRIORITIES**Focus effort where it reduces risk fastest**

Organisations that act now will be better placed to innovate confidently and avoid the reputational and financial costs of non-compliance.

1**Ramp up AI literacy**

This obligation is already enforceable. Audit who interacts with AI systems and launch structured awareness and training programmes without delay.

2**Map your AI footprint**

Identify every AI system your organisation develops, uses, imports or distributes. Classify each by risk level and determine your role.

3**Build your implementation plan**

Prioritise high-risk and GPAI systems. Establish governance, risk management and documentation practices. Onboard legal, compliance, IT, HR and leadership.

ARE YOU ON TRACK?

Use this checklist against the Act's phased obligations

Each area corresponds to a live or approaching requirement. Treat it as a management checklist, not a one-off legal review.

Now

AI literacy & prohibited practices

Banned AI practices must be off your radar. AI literacy programmes should be underway for staff interacting with AI systems.

Aug 2025

GPAI readiness

If you develop or use large language models or generative AI, prepare technical documentation, copyright policies and training data summaries.

Aug 2026

High-risk AI systems

Risk management, data governance, conformity assessments and EU database registrations must be complete for standalone high-risk AI systems.

Aug 2027

Sectoral & legacy systems

Embedded AI in regulated products and pre-existing GPAI models must be fully compliant.

Do not wait for a deadline. Conformity assessments, data governance reviews and supplier assurance can take months to complete.

AGS SUPPORT FOR PRACTICAL AI GOVERNANCE

Compliance is about trust, not just avoiding fines

Automated Governance Systems helps organisations navigate the intersection of AI, automation and governance, drawing on over 30 years of experience in highly regulated environments.

AI governance & compliance

Assess systems against the Act, establish risk management frameworks and build documentation and processes to demonstrate compliance.

AI literacy programmes

Tailored training and awareness campaigns for your teams, from board level to operational staff.

AI orchestration & architecture

Design and implement AI systems with governance built in from the ground up, not bolted on afterwards.

Ongoing support

Monitor secondary legislation, guidelines and enforcement developments so you do not have to.

A SIMPLE 90-DAY SME ACTION PLAN

Turn regulatory uncertainty into a manageable workstream

Start with visibility, training and prioritisation. Then build the controls needed for your highest-risk systems.

Days 1-30**Inventory and ownership**

- Create an AI register
- Confirm provider/deployer roles
- Remove any prohibited practices
- Identify staff groups needing AI literacy

Days 31-60**Classify and prioritise**

- Risk-classify systems
- Flag GPAI and high-risk uses
- Assess supplier evidence
- Agree business owners and controls

Days 61-90**Evidence and implementation**

- Launch training records
- Draft policies and logs
- Plan conformity work where needed
- Prepare board-level reporting

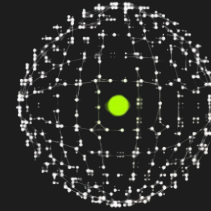
READY TO TAKE THE NEXT STEP?

Make AI Act readiness a business advantage

Whether you are just starting your AI Act journey or need expert support to accelerate your compliance programme, AGS is here to help.

Governance & Support Services

contact@automatedgovernancesystems.com



AGS

AUTOMATED GOVERNANCE SYSTEMS