

AURVALD · EU AI ACT TOOLKIT · V1.1 · OCT 2026

EU AI Act Readiness

Updated for the Digital Omnibus on AI — Regulation (EU) 2026/1744

Methodology, risk-classification framework, obligations mapping and a 16-question readiness checklist — for mid-market organisations using AI in the EU without a dedicated regulatory team.

Fractional Leadership · Data · AI · FinOps

PURPOSE

This toolkit gives you the AurVald method for EU AI Act readiness, the frameworks we use in a Rapid Review, and a 16-question self-assessment checklist. Use it as a shared starting point for scoping the work, or as a briefing for your board and audit committee.

Important: This toolkit is general information on Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744, reviewed on 2 October 2026. It is not legal advice. AurVald provides technical and governance expertise; confirm legal interpretations with qualified counsel.

1. The market moment

The Digital Omnibus on AI, in force since 27 July 2026, postponed the EU AI Act's high-risk obligations: to 2 December 2027 for stand-alone systems listed in Annex III, and to 2 August 2028 for AI embedded in products covered by Annex I. Prohibitions, general-purpose AI (GPAI) rules and the Article 50 transparency obligations were not postponed.

Most mid-market organisations meet the Act first through vendor contracts or customers' due-diligence questionnaires rather than through a planned programme. The extra time is best used to design compliance into the AI systems being built now, rather than retrofitting it in late 2027.

The AurVald view: EU AI Act compliance is an architecture problem, not just a legal problem. What you build determines what you must document. What you monitor determines what you can prove. The organisations that treat this as a checklist exercise separate from their AI architecture end up rebuilding both. The organisations that treat it as a lens applied while designing end up shipping faster with less rework.

2. Timeline of applicability

The Act entered into force on 1 August 2024 with staged application, amended by the Digital Omnibus on AI in July 2026. As at 2 October 2026:

Date	Milestone	Status
1 Aug 2024	AI Act (Reg. (EU) 2024/1689) enters into force	Complete
2 Feb 2025	Prohibited practices banned; AI literacy duty (Art. 4)	In force
2 Aug 2025	GPAI model obligations; governance; penalties framework	In force
27 Jul 2026	Digital Omnibus on AI (Reg. (EU) 2026/1744) enters into force	In force
2 Aug 2026	Transparency obligations (Art. 50); AI Office enforcement powers for GPAI	In force — grace period to 2 Dec 2026 for marking AI-generated content from systems already on the market
2 Dec 2027	HIGH-RISK obligations for stand-alone systems listed in Annex III	NEXT DEADLINE
2 Aug 2028	High-risk obligations for AI embedded in products under Annex I product legislation	Upcoming

What the Omnibus changed

- High-risk deadlines moved to 2 December 2027 (Annex III) and 2 August 2028 (Annex I).
- Article 4 AI literacy softened: organisations must take measures to support a sufficient level of AI literacy among staff, rather than ensure it.
- SME relief measures extended to small mid-cap companies.
- Registration requirements simplified.
- Two prohibited practices added: AI used to generate child sexual abuse material, and AI used to generate non-consensual intimate or sexually explicit content of identifiable people.
- GPAI model obligations, applicable since 2 August 2025, are unchanged.

3. Risk classification

The Act classifies AI systems into four tiers by risk. Classification determines the obligations. Getting the classification right is Step Zero — everything else follows from it.

Classification mistake to avoid: Many organisations classify a system as "limited-risk" because it interacts with people and produces content, when in fact it materially informs a decision in an Annex III area (e.g. shortlisting CVs, or assessing creditworthiness). Article 6(3) allows narrow exceptions — for example purely preparatory or procedural tasks — but a system that profiles individuals is always high-risk, and any exception you rely on must be documented.

Tier	Definition	Examples	Obligation Level
Prohibited	Unacceptable-risk AI. Cannot be placed on market or used in the EU.	Social scoring · Real-time remote biometric ID in public spaces (narrow exceptions) · Workplace/school emotion recognition · Untargeted face scraping · Added 2026: generating CSAM or non-consensual intimate imagery of real people	BAN — must be removed
High-risk	AI in listed critical sectors or as safety components of regulated products.	Annex III: HR (CV screening, promotion, termination) · Credit scoring (not fraud detection) · Life & health insurance pricing · Essential services · Education · Critical infrastructure · Biometrics · Law enforcement, migration, justice. Annex I: AI in regulated products	Full regime (Ch. III) from 2 Dec 2027 (Annex III) / 2 Aug 2028 (Annex I)
Limited-risk	AI interacting with natural persons, generating content, or deepfakes.	Chatbots · GenAI assistants · Emotion-recognition systems (non-workplace) · Biometric categorisation · Deepfakes	Transparency obligations (Art. 50) from 2 Aug 2026
Minimal-risk	Everything else.	Spam filters · AI-enabled video games · Inventory management	Voluntary codes only
GPAI models	General-purpose AI models — separate regime.	Foundation LLMs used across many use cases · Multi-purpose vision or speech models	Transparency, copyright, downstream info; more for systemic-risk models

4. Role determination

Once each AI system is classified, the next step is establishing your role. Obligations differ substantially between providers, deployers, importers and distributors — and an organisation is often several roles simultaneously across different systems.

Role	Definition	Primary obligations (high-risk)
Provider	Develops an AI system or has one developed and places it on the market or puts it into service under its own name.	Full Chapter III regime; risk management; data governance; technical documentation; conformity assessment; CE marking; registration; post-market monitoring; incident reporting
Deployer	Uses an AI system under its authority in a professional context.	Follow provider's instructions; human oversight; input-data quality; monitor operation; log-keeping; DPIA where relevant; notify serious incidents to provider and market surveillance
Importer	Places on the EU market an AI system bearing the name/trademark of a third-country natural or legal person.	Verify provider has done conformity assessment; ensure technical documentation and CE marking; keep records; support market surveillance authorities
Distributor	Any other party in the supply chain (other than provider or importer) that makes an AI system available on the EU market.	Verify CE marking and documentation before distributing; conditions of storage/transport preserve conformity
Product mfr.	Manufacturer that places on the market a product covered by Annex I product law together with an AI system.	Same obligations as provider for the AI system it embeds
Authorised rep.	Person in the EU with written mandate from a non-EU provider to perform tasks on their behalf.	Maintain technical documentation; keep EU Declaration of Conformity; provide info to authorities; cooperate on corrective action

The provider trap: Many organisations that consider themselves "just users" of a third-party AI system become PROVIDERS under the Act the moment they substantially modify the system, put it on the market under their own brand, or use a general-purpose AI model for a high-risk purpose. Provider obligations are an order of magnitude heavier than deployer obligations — this determination is worth doing carefully.

5. The three-stage readiness engagement

AurVald delivers EU AI Act compliance work in three progressive workstreams — each stands alone commercially and each produces evidence you can use directly.

Stage 1 — AI System Inventory & Risk Classification

Duration: 2 weeks. Fixed scope and fee. This is the Rapid Review variant we recommend as the entry point.

Discovery

- Catalogue every AI system in use or planned across the organisation
- For each: purpose, users, data inputs, decisions supported, vendor stack
- Interview each system's business owner to understand actual (not intended) use

Assessment framework

- Classify each system against the four Act tiers
- Establish organisational role per system (provider / deployer / importer / distributor)
- Identify GPAI-model dependencies and their compliance implications
- Flag any systems in prohibited-use categories — these are Stage-Zero problems

Deliverables

- AI System Register (one row per system, all classifications and roles recorded)
- Gap analysis: obligations vs. current-state per system
- Prioritised remediation roadmap for Stage 2
- Board-ready summary of exposure and required next steps

Stage 2 — Readiness Build

Duration: 4–8 weeks depending on system count and complexity. Designs the controls for high-risk systems identified in Stage 1 into their architecture, ahead of the December 2027 / August 2028 deadlines.

Components delivered

- Risk management system template and rollout per high-risk system (Art. 9)
- Data governance policy: training, validation and testing data quality (Art. 10)
- Technical documentation template to Annex IV standard (Art. 11)
- Record-keeping: automatic event logging (Art. 12), with deployer log retention of at least six months (Art. 26(6))
- Transparency artefacts for downstream deployers (Art. 13)
- Human-oversight design — measures, roles, procedures (Art. 14)
- Accuracy, robustness and cybersecurity target levels (Art. 15)
- Post-market monitoring plan (Art. 72)
- Serious-incident reporting procedure (Art. 73)
- Quality management system for providers (Art. 17)
- AI literacy measures for staff who use or oversee AI (Art. 4)
- Transparency notices and AI-generated content marking (Art. 50)

Stage 3 — Ongoing Assurance

Ongoing engagement. Delivered as a light retainer once Stage 2 is in place.

- Evidence pack maintenance per system
- EU declaration of conformity preparation where you are the provider (Art. 47)
- Notified Body engagement coordination (for systems requiring third-party conformity assessment)
- Post-market monitoring cycle facilitation
- Regulatory-change monitoring — new guidance, delegated acts, national authority interpretations
- Audit preparation and support

6. The 16-question readiness checklist

The questions every organisation using AI in the EU should be able to answer before the December 2027 deadline. Run it before commissioning external help — it shows where the gaps are and how urgent they are.

Inventory & classification

- ☐ We have an inventory of every AI system we develop, buy or embed in our products
- ☐ For each system we know our role: provider, deployer, importer or distributor
- ☐ Each system is classified by risk: prohibited, high-risk, transparency-only or minimal (Art. 5, 6, 50)
- ☐ We have confirmed that none of our systems falls under a prohibited practice (Art. 5)

Governance — applies to everyone

- ☐ A named person is accountable for AI Act readiness
- ☐ We have taken measures to build AI literacy among staff who use or oversee AI (Art. 4)
- ☐ People are told when they interact with an AI system, and AI-generated content is labelled where required (Art. 50)
- ☐ Contracts with AI suppliers give us the information we need to meet our own obligations

High-risk systems — if you have any

- ☐ A risk management process is documented for each high-risk system (Art. 9)
- ☐ Training and input data are governed for quality, relevance and bias (Art. 10)
- ☐ Technical documentation follows the structure in Annex IV (Art. 11)
- ☐ Systems record events automatically (Art. 12), and as a deployer we keep logs for at least six months (Art. 26(6))
- ☐ Human oversight is designed in, and the people doing it are trained and able to intervene (Art. 14, 26)
- ☐ Post-market monitoring and serious-incident reporting are in place (Art. 72, 73)
- ☐ Where we are the provider, conformity assessment, declaration of conformity, CE marking and registration are planned (Art. 43, 47, 48, 49)
- ☐ Our plan is aligned to the 2 December 2027 and 2 August 2028 deadlines

7. Penalties for non-compliance

Fines are set as the higher of a fixed amount or a percentage of worldwide annual turnover for the preceding year — except for smaller companies, where the lower applies.

- Prohibited practices: up to €35 million or 7% of worldwide turnover
- Most other obligations, including high-risk and transparency duties: up to €15 million or 3% of worldwide turnover
- Supplying incorrect or misleading information to authorities: up to €7.5 million or 1% of worldwide turnover
- SMEs (including start-ups) and, since the Omnibus, small mid-caps: the LOWER of the two amounts applies — which reduces, but does not remove, exposure

Enforcement is by national market surveillance authorities in each Member State. The AI Office at the European Commission supervises GPAI models, with enforcement powers from 2 August 2026.

The commercial-risk view: Fines are one dimension. For mid-market organisations the larger cost often arrives earlier and indirectly: enterprise customers asking for evidence during procurement, investor due-diligence findings, and insurer questions. An up-to-date AI register and classification is increasingly a sales asset, not just a compliance artefact.

8. Working with AurVald on AI Act readiness

Our readiness work follows the AurVald model: senior-led, fixed-scope entry point, AI Act controls designed into the architecture, and delivery through our London implementation partner where build capacity is needed. We provide technical and governance expertise, not legal advice — we work alongside your legal counsel or DPO.

How to start

- Contact info@aurvald.ee with a short description of your AI footprint
- We reply within two business days with a few scoping questions
- A 30-minute intro call scopes the Rapid Review — no obligation
- Stage 1 (2-week Rapid Review) can start the following week

What this toolkit gives you

- The framework and vocabulary you need to have this conversation productively
- A 16-question self-assessment you can run before engaging any external help
- A board-and-audit-ready reference document — annotate and share directly

Sources

Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 12 July 2024. Regulation (EU) 2026/1744 (Digital Omnibus on AI), OJ, 24 July 2026. European Commission, AI Act policy pages (digital-strategy.ec.europa.eu).

AurVald OÜ · Registered in Estonia · Fractional FinOps | Data | AI · info@aurvald.ee · aurvald.ee